Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти перший (бакалаврський)

Високошвидкісна корпоративна комп'ютерна мережа компанії "OsabizUA"

(тема)

Виконав:
здобувач 4 року навчання,
групи КІУКІ-21-2
Максим МИРОНЕНКО
(власне ім’я, прізвище)

Спеціальність
123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма
Комп’ютерна інженерія
(повна назва освітньої програми)

Керівник: ас. Артем МОРОЗ
(посада, власне ім’я, прізвище)

Допускається до захисту

Завідувач кафедри ЕОМ _____ Андрій КОВАЛЕНКО
(підпис) (власне ім’я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти перший (бакалаврський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп’ютерна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Мироненку Максиму Володимировичу
(прізвище, ім’я, по батькові)

1. Тема роботи Високошвидкісна корпоративна комп'ютерна мережа компанії "OsabizUA"

затверджена наказом по університету від “ 26 ” травня 2025 р. № 424 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 17 червня 2025 р.

3. Вхідні дані до роботи

1. Розробка комп'ютерної мережі підприємства
2. Опис організаційної структури підприємства
3. Вимоги до швидкості передачі інформації в мережі
4. Перелік використаних програмних засобів: ОС Windows 11

4. Перелік питань, що потрібно опрацювати у роботі

1. Аналіз предметної області та сучасного стану корпоративних мереж
2. Теоретичні основи побудови корпоративних комп'ютерних мереж
3. Проектування високошвидкісної корпоративної мережі
4. Реалізація проєкту корпоративної мережі

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій Слайди презентації – 15 сторінок

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Аналіз проблеми та огляд існуючих рішень	27.05.25 – 30.05.25	
2	Вибір технології розробки та інструментальних	31.05.25 – 02.06.25	
	засобів		
3	Розробка алгоритмічного забезпечення	03.06.25 – 05.06.25	
4	Розробка та відлагодження програмного	06.06.25 – 09.06.25	
5	Оформлення матеріалів кваліфікаційної роботи	10.06.25 – 11.06.25	
6	Подання кваліфікаційної роботи керівникові	12.06.25 – 13.06.25	
	та її попередній захист		
7	Подання кваліфікаційної роботи на	14.06.25 – 16.06.25	
	рецензування		

Дата видачі завдання " 26 " травня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ ас. Артем МОРОЗ
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 64 с., 11 рис., 0 табл., 1 дод., 15 джерел.

КОМП’ЮТЕРНА МЕРЕЖА, ІНТЕРНЕТ, МАРШРУТИЗАТОР, ПРОТОКОЛ, СЕРВЕР, ШЛЮЗ, FIREWALL, WI-FI, WLAN.

Метою кваліфікаційної роботи є розробка проєкту високошвидкісної корпоративної комп’ютерної мережі, яка забезпечить ефективну підтримку бізнес-процесів, оптимальну продуктивність, масштабованість та високий рівень інформаційної безпеки для підприємства.

У ході виконання кваліфікаційної роботи проаналізовано сучасний стан корпоративних мереж, досліджено актуальні технології побудови мережевої інфраструктури, визначено технічні вимоги до проєкту, обґрунтовано вибір обладнання та програмного забезпечення, а також розроблено й описано практичні рішення щодо реалізації проєкту корпоративної мережі.

ABSTRACT

Bachelor’s thesis: 64 pages, 11 figures, 0 tables, 1 appendix, 15 sources.

FIREWALL, GATE, INTERNET, PROTOCOL, ROUTER, SERVER, WI-FI, WIRELESS NETWORK, WLAN.

The major goal of this thesis is to develop a project of a high-speed corporate computer network that will provide efficient support for business processes, optimal performance, scalability, and a high level of information security for the enterprise.

During the preparation of this thesis, the current state of corporate networks was analyzed, relevant technologies for building network infrastructure were studied, technical requirements for the project were defined, and the selection of hardware and software was substantiated. In addition, practical solutions for implementing the corporate network project were developed and described.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ACL — Access Control List (список контролю доступу)

CAN — Campus Area Network (кампусна мережа)

DHCP — Dynamic Host Configuration Protocol (протокол динамічного налаштування хоста)

DNS — Domain Name System (система доменних імен)

IDS — Intrusion Detection System (система виявлення вторгнень)

IPS — Intrusion Prevention System (система запобігання вторгнень)

IP — Internet Protocol (інтернет-протокол)

LAN — Local Area Network (локальна мережа)

MAN — Metropolitan Area Network (міська мережа)

NAS — Network Attached Storage (мережеве сховище даних)

NAT — Network Address Translation (трансляція мережевих адрес)

NGFW — Next Generation Firewall (міжмережевий екран нового покоління)

PoE — Power over Ethernet (живлення через Ethernet)

QoS — Quality of Service (якість обслуговування)

RAID — Redundant Array of Independent Disks (надлишковий масив незалежних дисків)

SDN — Software-Defined Networking (програмно-конфігурована мережа)

SFP — Small Form-factor Pluggable (компактний оптичний/електричний модуль)

TCP — Transmission Control Protocol (протокол керування передачею)

VLAN — Virtual Local Area Network (віртуальна локальна мережа)

WAN — Wide Area Network (глобальна мережа)

ВСТУП

У парадигмі розвитку інформаційних технологій корпоративні комп'ютерні мережі становлять фундаментальну основу для забезпечення стабільного й ефективного функціонування бізнес-процесів підприємств різних масштабів. Висока швидкість передачі даних, надійність комунікаційних каналів і якість наданих мережевих сервісів визначають продуктивність діяльності персоналу та суттєво впливають на конкурентоспроможність організації в умовах динамічного ринку. Для компанії "OsabizUA", яка демонструє сталий розвиток та адаптується до цифрових викликів сучасності, постає гостра необхідність упровадження інноваційної високошвидкісної мережевої інфраструктури. Така інфраструктура повинна забезпечувати безперебійний обмін інформацією між структурними підрозділами, надійний доступ до корпоративних ресурсів, а також підтримувати впровадження новітніх цифрових рішень. Збільшення обсягу даних, розширення штату користувачів та інтеграція ресурсомістких сервісів, таких як хмарні технології й відеоконференцзв’язок, зумовлюють потребу у модернізації існуючої мережі відповідно до сучасних стандартів і вимог щодо пропускної здатності, мінімізації затримок і підвищення рівня інформаційної безпеки [1].

Актуальність роботи визначається тим, що ефективність цифрових бізнес-процесів безпосередньо залежить від характеристик корпоративної мережі, зокрема її швидкодії, надійності та стійкості до зовнішніх загроз. Будь-які затримки чи перебої у функціонуванні мережі здатні призвести до фінансових втрат, зниження продуктивності персоналу та ризиків для безпеки даних. Окрім цього, впровадження сучасних інформаційних технологій — таких як хмарні сервіси, системи для колективної роботи та інструменти захисту інформації — потребує якісної і масштабованої мережевої архітектури, яка відповідатиме перспективним завданням

компанії.

Метою даної роботи є розробка проекту високошвидкісної корпоративної комп'ютерної мережі для компанії "OsabizUA", яка відповідатиме актуальним потребам організації та забезпечить оптимальні показники продуктивності, надійності, масштабованості та інформаційної безпеки. Для досягнення цієї мети передбачено аналіз існуючої інфраструктури, вивчення сучасних технологій побудови корпоративних мереж, визначення технічних вимог до нової архітектури, вибір оптимального мережевого обладнання та рішень щодо організації передачі даних, а також обґрунтування економічної ефективності запропонованих заходів.

Об'єктом дослідження виступає корпоративна комп'ютерна мережа компанії "OsabizUA", а предметом — методи й технології створення високошвидкісних корпоративних мереж, що забезпечують ефективну підтримку бізнес-процесів організації. У процесі роботи використовуються методи аналізу науково-технічної літератури, нормативних документів, системний аналіз існуючих рішень, порівняльний аналіз мережевих технологій, математичне моделювання мережевого трафіку та техніко-економічне обґрунтування проєктних рішень.

Практична значущість проєкту полягає у можливості впровадження розробленої мережевої інфраструктури для оптимізації діяльності компанії "OsabizUA", що сприятиме підвищенню ефективності роботи персоналу, поліпшенню якості обслуговування клієнтів і посиленню ринкових позицій підприємства. Запропоновані рішення можуть бути також використані іншими організаціями для створення та модернізації власних корпоративних мереж, а також у навчальному процесі при підготовці спеціалістів з мережевих технологій.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА СУЧАСНОГО СТАНУ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Аналіз сучасних вимог до корпоративних комп'ютерних мереж

Корпоративні комп'ютерні мережі є фундаментальною складовою інфраструктури сучасних підприємств, які прагнуть досягти високого рівня ефективності внутрішньої та зовнішньої комунікації, оптимізації бізнес-процесів і забезпечення стабільного доступу до корпоративних ресурсів. У зв’язку з безперервним розвитком цифрових технологій, впровадженням новітніх інформаційних систем і стрімким зростанням обсягів даних, вимоги до корпоративних мереж постійно ускладнюються. Передусім сучасна корпоративна мережа повинна забезпечувати не лише надійну та безперебійну передачу даних між усіма вузлами інфраструктури, але й підтримувати високу масштабованість, що дозволяє одночасно працювати сотням чи навіть тисячам користувачів, які взаємодіють із файловими серверами, базами даних, корпоративними додатками та зовнішніми сервісами через Інтернет. Мережа має бути готова до роботи із широким спектром інформаційних потоків: окрім традиційного трафіку даних, усе більшого значення набувають мультимедійні потоки, що включають передачу аудіо та відео в режимі реального часу, відеоконференції, IP-телефонію, стрімінгове відео та інші ресурсоємні застосунки [2]. Це зумовлює необхідність реалізації комплексних механізмів керування смугою пропускання, застосування методів пріоритизації трафіку, а також запровадження інструментів моніторингу та управління якістю обслуговування (QoS), щоб гарантувати дотримання параметрів пропускної здатності, мінімізації затримок, запобігання втратам пакетів і стабільності джитера навіть при пікових навантаженнях.

Якість обслуговування (QoS) набуває ключового значення, оскільки саме цей параметр визначає здатність мережі відповідати суворим вимогам критично важливих бізнес-додатків. До основних показників QoS належать пропускна здатність каналів, затримки при передачі даних, стабільність часових характеристик (джитер) і рівень втрат пакетів. Наприклад, для голосового трафіку та IP-телефонії встановлені жорсткі обмеження на затримку (не більше 150 мс в одному напрямку) та втрати пакетів (не вище 1%), а для відеоконференцій ці вимоги ще суворіші — допустима затримка має бути не більшою за 100 мс, а джитер не перевищувати 30 мс. Корпоративні інформаційні системи, такі як ERP та CRM, вимагають гарантованої пропускної здатності та максимальної надійності, оскільки навіть короткочасні перебої можуть призвести до фінансових втрат, погіршення обслуговування клієнтів та зниження ефективності управління підприємством.

Водночас, під впливом зростання обсягів даних і інтеграції новітніх технологій, зокрема хмарних сервісів, систем відеоспостереження високої роздільної здатності, штучного інтелекту, машинного навчання, а також масового впровадження Інтернету речей (IoT), вимоги до пропускної здатності та швидкодії корпоративних мереж невпинно зростають. Типова сучасна корпоративна мережа середнього підприємства повинна забезпечувати сукупну пропускну здатність не менше 1-10 Гбіт/с на рівні мережевого ядра, тоді як для великих компаній цей показник може досягати 40-100 Гбіт/с і більше, що дозволяє обробляти масиви даних у реальному часі, забезпечувати роботу систем відеонагляду у форматі 4K і вище, а також ефективно підтримувати роботу десятків або сотень різноманітних корпоративних додатків. З урахуванням сучасних тенденцій, до числа критичних характеристик корпоративної мережі входять також адаптивність до змінних навантажень, можливість швидкої модернізації, інтеграція з глобальними мережами та хмарними платформами, а також впровадження ефективних заходів із забезпечення інформаційної безпеки на всіх рівнях.

1.2 Тенденції розвитку високошвидкісних мережевих технологій

Розвиток мережевих технологій у корпоративному сегменті відзначається постійним зростанням швидкості передачі даних, впровадженням інноваційних стандартів, а також активною модернізацією протоколів і апаратних рішень, що дозволяють підприємствам ефективно адаптуватися до зростаючих вимог цифрової економіки. Аналіз сучасних тенденцій вказує на те, що ключовими векторами еволюції є впровадження високошвидкісних стандартів Ethernet і стрімке вдосконалення бездротових технологій. Еволюція технології Ethernet ілюструє значне зростання швидкостей: якщо раніше базовим стандартом у корпоративних мережах був Fast Ethernet із пропускною здатністю до 100 Мбіт/с, то нині Gigabit Ethernet із швидкістю 1 Гбіт/с став мінімальною нормою для мережевого доступу. Для магістральних з’єднань дедалі частіше застосовуються 10 Gigabit Ethernet та ще більш сучасні рішення, які базуються на стандартах IEEE 802.3ae (10 Гбіт/с), IEEE 802.3ba (40 Гбіт/с) та IEEE 802.3bj (100 Гбіт/с), що дозволяє об’єднувати сервери, комутатори верхнього рівня й забезпечувати надійний зв’язок із зовнішніми мережами та інтернет-провайдерами. У сегменті бездротового зв’язку домінує технологія Wi-Fi шостого покоління (IEEE 802.11ax), яка не лише забезпечує теоретичну швидкість до 9,6 Гбіт/с, а й підвищує ефективність роботи в умовах високої щільності підключень та складної радіообстановки. На етапі активної розробки перебуває стандарт Wi-Fi 7[3,4]. (IEEE 802.11be), що обіцяє ще більшу пропускну здатність, до 30 Гбіт/с, і впровадження передових алгоритмів оптимізації.

Сучасний розвиток мережевих технологій не обмежується підвищенням швидкості. Велику увагу сьогодні приділено концепціям програмно-конфігурованих мереж (Software-Defined Networking, SDN) і мережевої функціональної віртуалізації (Network Function Virtualization, NFV). Програмно-конфігуровані мережі дозволяють централізовано управляти мережею, забезпечуючи динамічну маршрутизацію трафіку,

оптимізацію розподілу ресурсів та гнучке впровадження політик безпеки. SDN значно спрощує адміністрування великих, розгалужених мереж із багаторівневою структурою та дозволяє оперативно реагувати на зміну вимог до мережевого середовища. Мережева функціональна віртуалізація, у свою чергу, сприяє впровадженню більшої гнучкості за рахунок перенесення традиційних мережевих функцій (таких як маршрутизація, міжмережеві екрани, балансування навантаження) у програмне середовище, що працює на універсальному апаратному забезпеченні. Це не лише знижує витрати на обладнання, а й полегшує масштабування та модернізацію мережі.

Окремо слід відзначити швидкий прогрес у застосуванні технологій штучного інтелекту в мережевому менеджменті. Сучасні корпоративні мережі перетворюються на інтелектуальні системи, здатні до самостійної оптимізації, автоматичного виявлення аномалій, загроз безпеці та прогнозування навантажень. Такі "розумні" мережі дозволяють підвищити рівень автоматизації, забезпечити максимальну ефективність використання ресурсів, а також своєчасно реагувати на появу нових загроз.

Ринок корпоративних мережевих рішень, відповідно, характеризується інтенсивною конкуренцією та постійним технологічним оновленням. Лідерами галузі залишаються такі компанії, як Cisco Systems, Juniper Networks, Arista Networks, Huawei, HPE (Aruba Networks) та інші глобальні виробники, які пропонують повний спектр рішень — від пристроїв доступу до обладнання для центрів обробки даних та інфраструктур хмарних дата-центрів. Cisco Systems утримує провідні позиції, зокрема у сегменті комутаторів і маршрутизаторів для корпоративних мереж, пропонуючи надійні й масштабовані системи, які відповідають вимогам підприємств різного розміру. Водночас, все більшу популярність здобувають рішення на базі відкритих стандартів і так званого white-box обладнання, що дає змогу підприємствам скоротити витрати, уникнути прив’язки до одного постачальника та збільшити гнучкість під час побудови і модернізації інфраструктури. Однією з ключових тенденцій є також перехід до хмарних

моделей управління: провідні виробники дедалі частіше впроваджують системи централізованого адміністрування та моніторингу мережевого обладнання через хмарні платформи, що суттєво спрощує процеси експлуатації, підвищує рівень безпеки й дає змогу більш гнучко реагувати на зміни у корпоративному середовищі.

Таким чином, розвиток корпоративних мереж визначається сукупністю інноваційних технологій, підвищенням швидкостей, переходом до програмно-орієнтованих архітектур, впровадженням елементів штучного інтелекту, а також адаптацією до гібридних і хмарних моделей управління, що забезпечує ефективність, безпеку та масштабованість сучасної цифрової інфраструктури підприємств.

1.3 Характеристика компанії та аналіз її потреб у мережевій інфраструктурі

Для розробки ефективної корпоративної комп’ютерної мережі першочергово важливо здійснити ґрунтовний аналіз діяльності організації, оцінити поточний стан її інформаційно-телекомунікаційної інфраструктури та врахувати довгострокові стратегії розвитку. Компанія, що надає консалтингові послуги у сфері інформаційних технологій і має чисельність персоналу близько 150 осіб, функціонує у головному офісі та двох віддалених філіях, при цьому охоплює напрями розробки програмного забезпечення, системної інтеграції, технічної підтримки й консалтингу. Така спеціалізація компанії визначає підвищені вимоги до швидкості обміну інформацією, надійності комунікацій, стабільного функціонування критичних сервісів, а також до безпеки і масштабованості інфраструктури. Зокрема, ефективна робота з великими масивами програмного коду вимагає швидкодійного доступу до серверів з системами контролю версій і файловими сховищами, а проведення відеоконференцій та співпраця з клієнтами чи віддаленими працівниками потребує високої якості інтернет-

з’єднання, здатного забезпечити гарантовану пропускну здатність і відсутність критичних затримок. Використання хмарних платформ для зберігання даних, організації електронної пошти, колективної роботи над проєктами формує значний обсяг зовнішнього трафіку, який повинен бути підтриманий сучасними каналами зв’язку із високою надійністю та швидкістю.

Детальний аналіз існуючої мережевої інфраструктури виявив низку серйозних недоліків, характерних для багатьох організацій, що експлуатують обладнання минулих поколінь. Так, ядро мережі побудоване на центральному комутаторі Cisco Catalyst 2960[5], який підтримує лише Gigabit Ethernet, а до сегментів доступу підключені пристрої, що мають порти Fast Ethernet, обмежуючи швидкість роботи з корпоративними ресурсами. Для доступу до інтернету використовується єдиний маршрутизатор, а бездротове покриття забезпечується двома точками доступу стандарту 802.11n, чого недостатньо для повноцінної підтримки сучасних мобільних пристроїв, особливо у конференц-залах та зонах спільної роботи. Продуктивність мережі часто не відповідає потребам – особливо це помітно у пікові години, коли навантаження на магістральні канали досягає критичних значень, що призводить до затримок при доступі до файлових серверів, періодичних обривів з’єднання з хмарними платформами й погіршення якості відеоконференцій. Система централізованого моніторингу відсутня, що не дозволяє своєчасно реагувати на збої та локалізувати проблеми, а процес налаштування та обслуговування обладнання ускладнений через брак єдиного інтерфейсу управління.

Аналіз мережевого трафіку показує, що під час інтенсивної роботи значна частка пропускної здатності інтернет-каналу використовується на підтримку хмарних сервісів, синхронізацію даних, роботу поштових клієнтів і організацію відеоконференцій, при цьому у години пік завантаженість інтернет-каналу наближається до 90% від номінальної пропускної здатності, що негативно впливає на доступність та якість сервісів. Застарілі комутатори

та обмежена кількість точок доступу не дозволяють забезпечити необхідну швидкість передачі даних у всіх робочих зонах, а покриття бездротової мережі є недостатнім. Відсутність резервування критичних компонентів створює додаткові ризики для безперебійності роботи компанії, а використання єдиного провайдера підвищує ймовірність простою у разі аварійної ситуації.

Усі ці фактори зумовлюють необхідність комплексної модернізації мережевої інфраструктури компанії, що передбачає як технічне оновлення, так і впровадження сучасних методів управління. Ключовим напрямом є підвищення пропускної здатності магістральних з'єднань до 10 Гбіт/с, що дозволить суттєво знизити затримки при роботі з великими обсягами даних і забезпечити високий рівень продуктивності при масштабуванні організації. Безпровідна інфраструктура повинна бути повністю оновлена шляхом впровадження точок доступу стандарту Wi-Fi 6, які забезпечать високошвидкісний доступ усім мобільним пристроям, нададуть можливість ефективного роумінгу та покриття усіх офісних приміщень. Кількість точок доступу визначається виходячи з площі та архітектури будівлі, але має забезпечувати рівномірне покриття, що відповідає сучасним вимогам до мобільності працівників.

Особливу увагу необхідно приділити впровадженню системи централізованого моніторингу й управління мережею, що забезпечить виявлення й аналіз проблем у реальному часі, оптимізацію розподілу навантаження та своєчасну ідентифікацію аномалій. Для забезпечення стійкості та безпеки функціонування передбачено резервування каналів зв'язку шляхом підключення до двох інтернет-провайдерів, дублювання критично важливих серверів, а також використання систем безперебійного живлення, що мінімізує ризики втрати даних та простоїв у разі технічних збоїв. Безпека корпоративної мережі підвищується завдяки впровадженню сучасних засобів захисту: міжмережевих екранів нового покоління (NGFW), систем виявлення та запобігання вторгненням, технологій сегментації мережі

й організації контролю доступу до ресурсів на основі ролей користувачів.

Модернізація корпоративної мережі має не лише технологічне, а й економічне підґрунтя: інвестиції в оновлення інфраструктури здатні окупитися протягом двох років завдяки підвищенню продуктивності персоналу, зниженню витрат на підтримку застарілого обладнання, зменшенню кількості збоїв та забезпеченню можливості впровадження нових сервісів, які сприятимуть подальшому розвитку компанії. З урахуванням зростання чисельності співробітників і потенційного відкриття нових філій необхідно орієнтуватися на гнучку, масштабовану архітектуру мережі, яка дозволить швидко інтегрувати нові сегменти без радикальної перебудови всієї інфраструктури.

Отже, аналіз предметної області свідчить про нагальну необхідність проведення комплексної модернізації корпоративної мережі із застосуванням найсучасніших технологій передачі даних, управління та захисту, що стане надійною основою для ефективного функціонування організації, підвищення її конкурентоспроможності та реалізації стратегічних цілей. Це створює передумови для розробки високопродуктивного проекту корпоративної мережі, який буде представлено та обґрунтовано у наступних розділах дослідження.

2 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1 Класифікація та характеристики комп'ютерних мереж

Класифікація комп’ютерних мереж здійснюється за різними критеріями, що дозволяє глибоко аналізувати їхню архітектуру, принципи функціонування та можливості подальшого масштабування. Розуміння базових типів мереж і їхніх особливостей має принципове значення для побудови ефективної корпоративної інфраструктури, адже саме це визначає підхід до вибору топології, протоколів та засобів захисту. За масштабом і призначенням виділяють персональні, локальні, кампусні, міські та глобальні мережі, кожна з яких має власне технічне і функціональне призначення.

Персональні мережі (PAN) (рисунок 2.1) охоплюють невелику область — радіус до 10 метрів, і здебільшого використовуються для об'єднання пристроїв однієї особи, наприклад, смартфонів, планшетів, ноутбуків, гарнітур і розумних годинників. Застосування Bluetooth, Zigbee чи NFC уможливлює організацію бездротового обміну даними, причому швидкість передачі для Bluetooth 5.0 становить до 24 Мбіт/с. Локальні мережі (LAN) формують основу цифрової інфраструктури офісів, університетів і підприємств, забезпечуючи високошвидкісний обмін інформацією між пристроями в межах однієї будівлі або комплексу будівель. За сучасних вимог LAN базуються на технологіях Ethernet і Wi-Fi, що забезпечують пропускну здатність від 100 Мбіт/с до 100 Гбіт/с, з використанням комутаторів, маршрутизаторів і точок доступу. Мережі кампусу (CAN) поєднують декілька локальних мереж у межах навчального закладу чи великого підприємства, що дозволяє організувати високошвидкісну магістраль із загальною пропускною здатністю до 100 Гбіт/с, найчастіше за допомогою оптоволоконних каналів. Міські мережі (MAN) охоплюють цілі

міста або великі адміністративні регіони, часто розгортаються операторами зв'язку та використовують як традиційні кабельні системи, так і сучасні оптоволоконні та бездротові технології для з’єднання численних об’єктів інфраструктури. Глобальні мережі (WAN) забезпечують взаємодію географічно віддалених офісів і філій підприємства, а також вихід до Інтернету, використовуючи орендовані лінії, MPLS, VPN-тунелі, SD-WAN та інші інженерні рішення для забезпечення надійності й безпеки міжрегіональних і міжнародних з'єднань.

Рисунок 2.1 – Порівняння основних характеристик

Локальні й корпоративні мережі мають свої характерні ознаки — вони відзначаються високою швидкістю передачі даних, мінімальними затримками, надійністю та відносно простою, або ж, навпаки, ієрархічно складною структурою. У якісно спроектованих LAN пропускна здатність для

робочих станцій становить не менше 1 Гбіт/с, а для серверів — 40–100 Гбіт/с, із коефіцієнтом помилок не вище 10^{-12}. Корпоративні мережі містять кілька рівнів ієрархії — рівень доступу, розподілу й ядра — та мають підвищені вимоги до масштабованості, керованості, захисту інформації та резервування критичних компонентів, що забезпечує відмовостійкість та безперервність бізнес-процесів. Безпека реалізується завдяки застосуванню механізмів автентифікації, шифрування, сегментації трафіку й централізованого моніторингу подій.

Крім масштабування, важливу роль відіграє вибір топології мережі, адже саме вона визначає ефективність обробки трафіку, стійкість до відмов і гнучкість при розширенні. Найбільш поширеною для корпоративних LAN є топологія «зірка», у якій усі пристрої під’єднані до центрального комутатора або концентратора, що спрощує адміністрування й дозволяє швидко локалізувати несправності [7]. Однак основним недоліком є залежність усієї мережі від центрального вузла. Для складних корпоративних мереж характерна топологія «дерево» або ієрархічна структура, яка складається з кількох рівнів — ядра, розподілу й доступу — та дає змогу досягти хорошого балансу між продуктивністю й масштабованістю. Топологія «кільце» використовується там, де критично важливі резервування й відновлення зв’язку у разі пошкодження магістрального кабелю; вона дозволяє організувати кільцеву передачу даних із протоколами швидкого відновлення, такими як ERPS. Для критично важливих об’єктів і систем, де максимальна надійність є пріоритетом, застосовується топологія «mesh» — сітка, яка забезпечує множинні резервні шляхи між усіма вузлами, хоча й потребує значних інвестицій. Часткова mesh-топологія дозволяє досягти компромісу між ціною й рівнем відмовостійкості.

Завдяки правильному розумінню властивостей і обмежень кожного типу мережі, особливостей їхньої топології й рівня масштабованості, можна обґрунтовано підходити до проектування корпоративних інфраструктур, забезпечуючи їхню ефективну роботу, безпеку й простоту адміністрування

навіть за умов динамічного розвитку організації.

2.2 Порівняльний аналіз архітектур корпоративних мереж

Архітектура корпоративної мережі формує основу для ефективного функціонування всієї цифрової інфраструктури організації. Від вибору архітектурної моделі залежить надійність, масштабованість, безпека та подальша гнучкість корпоративної мережі. Найпоширенішою є ієрархічна модель, яка структурує мережу за рівнями — доступу, розподілу та ядра. Такий підхід дає змогу ефективно організувати трафік, централізовано впроваджувати політики безпеки й якісно масштабувати мережу відповідно до зростання компанії. Рівень доступу є базовим для підключення кінцевих пристроїв: тут формуються правила доступу до ресурсів, маркується трафік, реалізується базова сегментація через VLAN і впроваджуються основні політики QoS та фільтрації. Наступний рівень — розподілу — відповідає за агрегацію трафіку, маршрутизацію між різними сегментами й інтеграцію механізмів безпеки: тут застосовуються ACL, політики безпеки, маршрутизатори та потужні комутатори 3-го рівня. На рівні ядра формується високошвидкісний магістральний канал для транспортування трафіку між різними частинами мережі, використовується обладнання з мінімальною затримкою й максимальною пропускною здатністю — це критично для великих компаній та організацій із розподіленою структурою.

Однією з базових концепцій у сучасній архітектурі корпоративних мереж є принцип сегментації — як фізичної, так і логічної. Фізична сегментація досягається шляхом виділення окремих комутаторів, портів чи фізичних каналів для певних груп пристроїв чи критичних систем. Це дозволяє досягти максимальної ізоляції, проте підвищує витрати та знижує гнучкість масштабування. Логічна сегментація, навпаки, базується на застосуванні VLAN, що дає змогу створювати ізольовані мережі всередині єдиної фізичної інфраструктури, ефективно розмежовуючи трафік,

формуючи групи доступу та спрощуючи адміністрування. Для підвищення рівня безпеки й адаптивності сьогодні широко впроваджується мікросегментація, яка дозволяє налаштовувати політики доступу на рівні окремих пристроїв, користувачів чи додатків із використанням можливостей SDN, — це підхід особливо цінний для захисту критичних застосунків та гнучкого управління корпоративною політикою доступу.

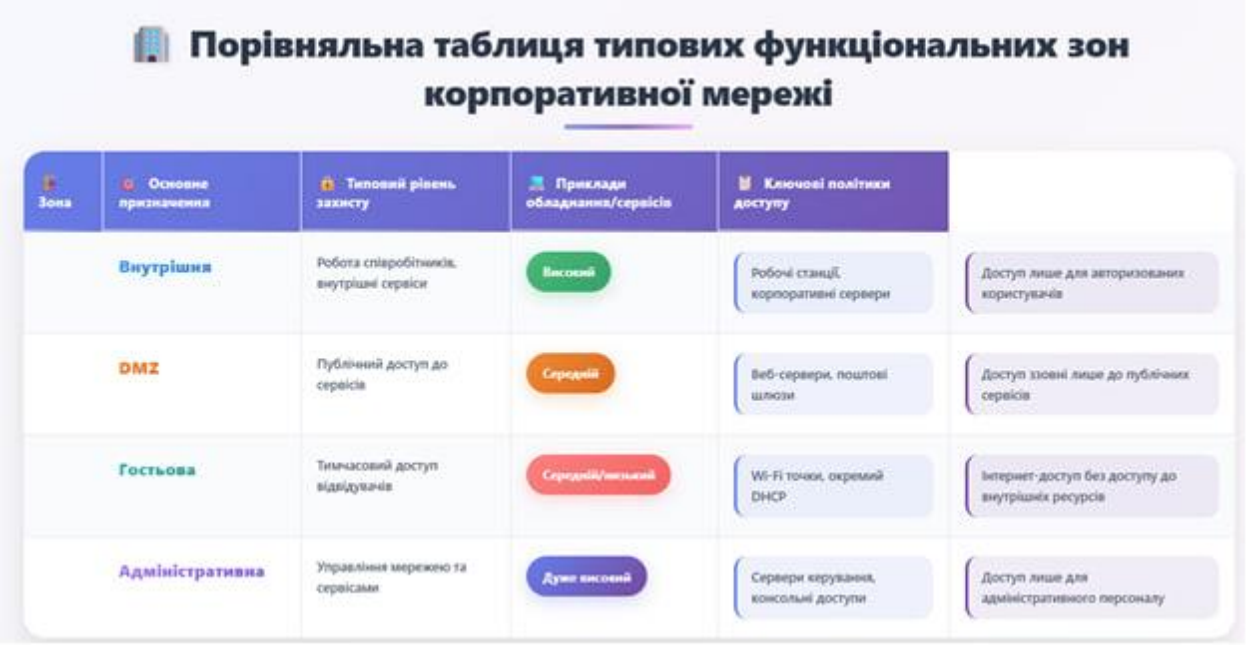
Зонування корпоративної мережі дозволяє вибудовувати різні рівні довіри, виділяючи окремі функціональні зони: внутрішню (internal zone), демілітаризовану (DMZ), гостьову (guest network), адміністративну (management network) тощо. Кожна зона має чітко визначені правила взаємодії із зовнішнім та внутрішнім трафіком, сувору політику безпеки та власні механізми моніторингу. Це дозволяє ізолювати критичні ресурси, мінімізувати ризики поширення атак та оперативно локалізувати потенційні загрози.

Окрім класичної ієрархічної моделі, сучасна мережна архітектура активно розвивається в напрямку застосування альтернативних підходів, що виникли у відповідь на нові технологічні вимоги бізнесу. Архітектура spine-and-leaf, яка стала стандартом для дата-центрів, дозволяє досягти однакової затримки між усіма вузлами мережі, відсутності вузьких місць і максимізації швидкості передачі east-west трафіку. У цій моделі кожен leaf-комутатор з’єднаний із усіма spine-комутаторами, утворюючи на логічному рівні mesh-топологію. Collapsed core-архітектура — спрощена версія ієрархії для невеликих організацій, де функції рівня ядра та розподілу поєднуються, що дозволяє знизити витрати, проте обмежує масштабованість. Гіперконвергентна архітектура інтегрує обчислювальні, мережеві та сховищні ресурси в єдині модулі, спрощуючи адміністрування та масштабування, проте створюючи ризик залежності від певного виробника й обмежуючи варіативність компонентів.

Порівняльна таблиця основних архітектур корпоративних мереж

Архітектура	Кількість рівнів	Масштабованість	Надійність	Складність адміністрування	Вартість реалізації	Переваги	Недоліки
Ієрархічна (3-tier)	3	Висока (до тисяч вузлів)	Висока	Середня	Середня	Чітка структуризація, ізоляція, простота масштабування	Вузькі місця на рівні ядра, обмеження горизонтального росту
Spine-and-leaf	2	Дуже висока	Дуже висока	Висока	Висока	Однакові затримки, відсутність bottleneck, гнучке розширення	Висока вартість, складність конфігурації
Collapsed core	2 (або 1 логічно)	Обмежена	Середня	Проста	Низька	Зменшення кількості обладнання, низька ціна	Обмежена масштабованість, потенційні проблеми продуктивності
Гіперконвергентна	1–2	Висока	Висока	Дуже проста	Висока	Інтеграція IT-ресурсів, швидке розгортання	Vendor lock-in, складності інтеграції з рішеннями інших виробників

Рисунок 2.2 – Порівняльна таблиця основних архітектур корпоративних мереж



Порівняльна таблиця типових функціональних зон корпоративної мережі

Зона	Основне призначення	Типовий рівень захисту	Приклади обладнання/сервісів	Ключові політики доступу	
Внутрішня	Робота співробітників, внутрішні сервіси	Високий	Робочі станції, корпоративні сервери	Доступ лише для авторизованих користувачів	
DMZ	Публічний доступ до сервісів	Середній	Веб-сервери, поштові шлюзи	Доступ ззовні лише до публічних сервісів	
Гостьова	Тимчасовий доступ відвідувачів	Середній/низький	Wi-Fi точки, окремий DHCP	Інтернет-доступ без доступу до внутрішніх ресурсів	
Адміністративна	Управління мережею та сервісами	Дуже високий	Сервери керування, консольні доступи	Доступ лише для адміністративного персоналу	

Рисунок 2.3 – Порівняльна таблиця типових функціональних зон корпоративної мережі

Завдяки такій деталізації й системному підходу до аналізу архітектурних моделей та зонування, можна прийняти обґрунтоване рішення

щодо проектування корпоративної мережі, орієнтуючись на конкретні потреби організації, її масштаб, вимоги до безпеки та бюджетні обмеження. Такий аналіз дозволяє визначити оптимальний баланс між продуктивністю, безпекою, масштабованістю і вартістю впровадження, що є запорукою успіху IT-інфраструктури сучасної компанії.

2.3 Сучасні технології та стандарти високошвидкісних мереж

Розвиток високошвидкісних мережевих технологій супроводжується багатовекторним зростанням: від збільшення пропускної здатності й зниження затримок до впровадження інтелектуальних механізмів управління ресурсами та адаптивних протоколів комутації і маршрутизації. Основою сучасної корпоративної інфраструктури залишаються технології Ethernet, які забезпечують масштабованість, надійність і гнучкість у поєднанні з високою швидкістю передачі даних. Сучасна архітектура мереж дедалі частіше орієнтується на інтеграцію різних поколінь Ethernet у єдиному інформаційному просторі. Gigabit Ethernet[8] залишається стандартом для підключення кінцевих пристроїв і серверів, пропонуючи швидкість до 1 Гбіт/с по мідному кабелю категорії 5e або вище, що оптимально для більшості сучасних офісів. 10 Gigabit Ethernet забезпечує необхідну швидкодію для серверних і магістральних з'єднань, особливо в умовах використання віртуалізації, хмарних сервісів і зростання відеотрафіку. 40 і 100 Gigabit Ethernet, а також перспективні 200 та 400 Gigabit Ethernet стандарти стають пріоритетом для великих дата-центрів, наукових інститутів, операторських і корпоративних магістральних мереж, забезпечуючи підтримку інтенсивного трафіку, резервування і відмовостійкість.

Наведений нижче рисунок 2.4 дозволяє порівняти ключові характеристики основних стандартів високошвидкісного Ethernet

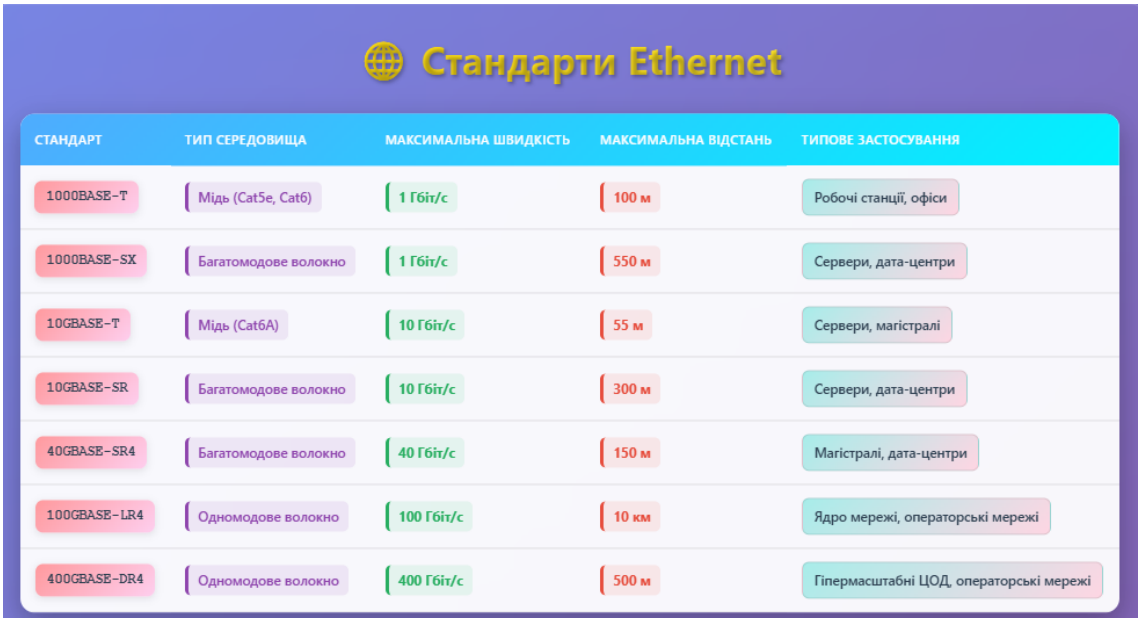


Рисунок 2.4 – Ключові характеристики основних стандартів високошвидкісного Ethernet

Паралельно з фізичними технологіями зростає роль протоколів (рисунок 2.5) комутації й маршрутизації, які відповідають за оптимізацію потоків даних, підвищення відмовостійкості і раціональне використання ресурсів. На канальному рівні для уникнення петель і резервування маршрутів довгий час використовувався STP (Spanning Tree Protocol) і його покращені версії RSTP, MSTP, однак вони характеризуються повільною конвергенцією і нераціональним використанням резервних каналів. Протоколи нового покоління — TRILL і SPB — дозволяють ефективно використовувати всі доступні шляхи, забезпечують швидку реакцію на зміни топології і суттєво підвищують ефективність east-west трафіку, що особливо важливо для дата-центрів.

На мережевому рівні стандартним для корпоративних мереж став OSPF, який використовує ієрархічну модель з розбиттям на області та швидкий алгоритм Дейкстри для пошуку найкоротших шляхів. Протокол BGP — основа глобальної маршрутизації Інтернету — також застосовується у великих корпоративних мережах для гнучкого управління маршрутами між філіями чи балансування трафіку на стику з Інтернет-провайдерами. Для

швидкої конвергенції й підвищення стійкості, особливо в інфраструктурах Cisco, широко використовується EIGRP, який забезпечує резервування маршрутів і оперативне перемикання при збої основного каналу.

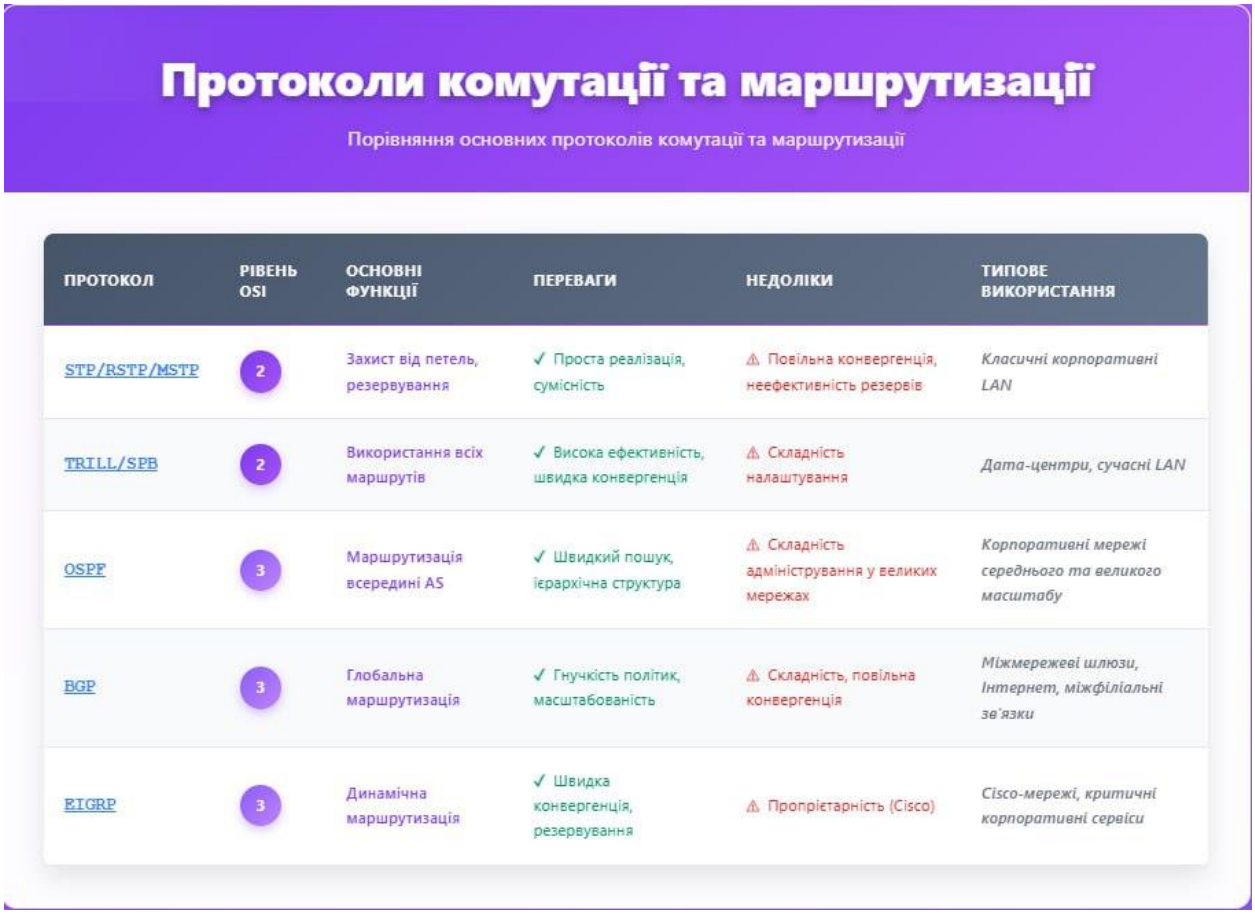


Рисунок 2.5 – Порівняння основних протоколів комутації та маршрутизації

Ще одним невід’ємним елементом сучасних мереж є підтримка QoS — системи управління якістю обслуговування. У корпоративному середовищі QoS забезпечує пріоритезацію трафіку, дозволяючи надавати гарантовану пропускну здатність додаткам із високими вимогами до затримок і втрат пакетів, наприклад, VoIP, відеоконференціям чи критичним корпоративним сервісам. Для цього застосовуються механізми диференціації, класифікації, пріоритетної обробки та керування чергами. Серед них — Priority Queuing, Weighted Fair Queuing, Class-Based Weighted Fair Queuing[9], а також алгоритми управління трафіком і формування черг, такі як Token Bucket, Leaky Bucket, Random Early Detection та Weighted Random Early Detection.

Завдяки цим технологіям, навіть у разі перевантаження каналів або пікових навантажень у мережі зберігається якість обслуговування найкритичніших сервісів, забезпечується гнучкість реагування на зміну трафіку і підвищується загальна ефективність використання ресурсів.

Таким чином, розвиток високошвидкісних мереж, впровадження нових стандартів Ethernet і протоколів маршрутизації, а також ускладнення механізмів забезпечення якості обслуговування формують багаторівневу, адаптивну і масштабовану архітектуру корпоративних мереж, здатну задовольнити сучасні вимоги цифрового бізнесу, індустрії 4.0 та гібридних хмарних середовищ.

2.4 Принципи забезпечення безпеки та надійності мереж

Безпека та надійність є фундаментальними вимогами до корпоративних мереж, оскільки сучасний бізнес дедалі більше залежить від стабільності та цілісності IT-інфраструктури. Кількість кіберзагроз постійно зростає, а атаки стають все більш складними, тому питання захисту мережі, забезпечення відмовостійкості та ефективного моніторингу виходять на перший план. Побудова сучасної корпоративної мережі неможлива без комплексного впровадження різних рівнів захисту та резервування.

На початковому рівні безпеки ключову роль відіграють мережеві екрани. Традиційні firewall виконують фільтрацію трафіку за адресами та портами, однак їх функціонал вже недостатній для протидії новим складним атакам. У відповідь на це використовуються Next Generation Firewall, які здатні виконувати глибоку інспекцію додатків, виявляти вторгнення, блокувати підозрілий трафік, інтегрувати антивірусну перевірку й обмеження доступу до шкідливих чи небажаних веб-ресурсів. Ці рішення надають більш гнучкі інструменти контролю і забезпечують детальні політики безпеки.

Велике значення мають системи виявлення та запобігання вторгненням (IDS/IPS), які аналізують потоки мережевого трафіку та дозволяють

ідентифікувати як відомі, так і невідомі типи атак завдяки використанню сигнатур та поведінкових алгоритмів. Розвиток таких платформ йде шляхом інтеграції із системами аналітики загроз, що дозволяє оперативно оновлювати бази атак і ефективно реагувати на нові виклики.

У корпоративних мережах все ширше впроваджується концепція Zero Trust, яка повністю виключає "довіру за замовчуванням" — кожен користувач, пристрій або додаток повинні проходити автентифікацію та авторизацію при кожному запиті до ресурсів. Для зменшення можливого розповсюдження загроз практикується мікросегментація мережі, завдяки якій адміністратори створюють детальні правила доступу для окремих зон і пристроїв.

Захист інформації під час передавання забезпечується широким використанням сучасних криптографічних протоколів. Для шифрування трафіку застосовуються TLS/SSL, IPSec, що гарантує конфіденційність даних навіть у разі їх перехоплення. В якості алгоритмів симетричного шифрування рекомендується використовувати AES-256, для асиметричного — RSA-2048 або еліптичні криві, що відповідає сучасним вимогам безпеки.

Надійність мережі формується за рахунок комплексного резервування та впровадження відмовостійких рішень. Для цього дублюються критично важливі компоненти, використовується кластеризація обладнання, впроваджуються технології високої доступності. Віртуальні маршрутизатори, створені на основі протоколів VRRP або HSRP, забезпечують автоматичне перемикання трафіку у разі відмови основного пристрою. Додатково, стекові технології дозволяють фізично об'єднувати декілька комутаторів в єдиний логічний пристрій — у разі виходу з ладу одного із них сесії користувачів залишаються активними, а пропускна здатність не втрачається.

Особливу увагу слід приділяти резервуванню каналів зв’язку та географічному дублюванню вузлів. Це дозволяє зберегти працездатність мережі навіть при аваріях чи катастрофах у конкретному регіоні. Швидке перемикання на резервні лінії забезпечують сучасні протоколи

маршрутизації з підтримкою швидкої конвергенції, такі як RSTP або відповідні алгоритми динамічної маршрутизації. Наступний рисунок 2.6 ілюструє основні технології забезпечення безпеки корпоративної мережі.

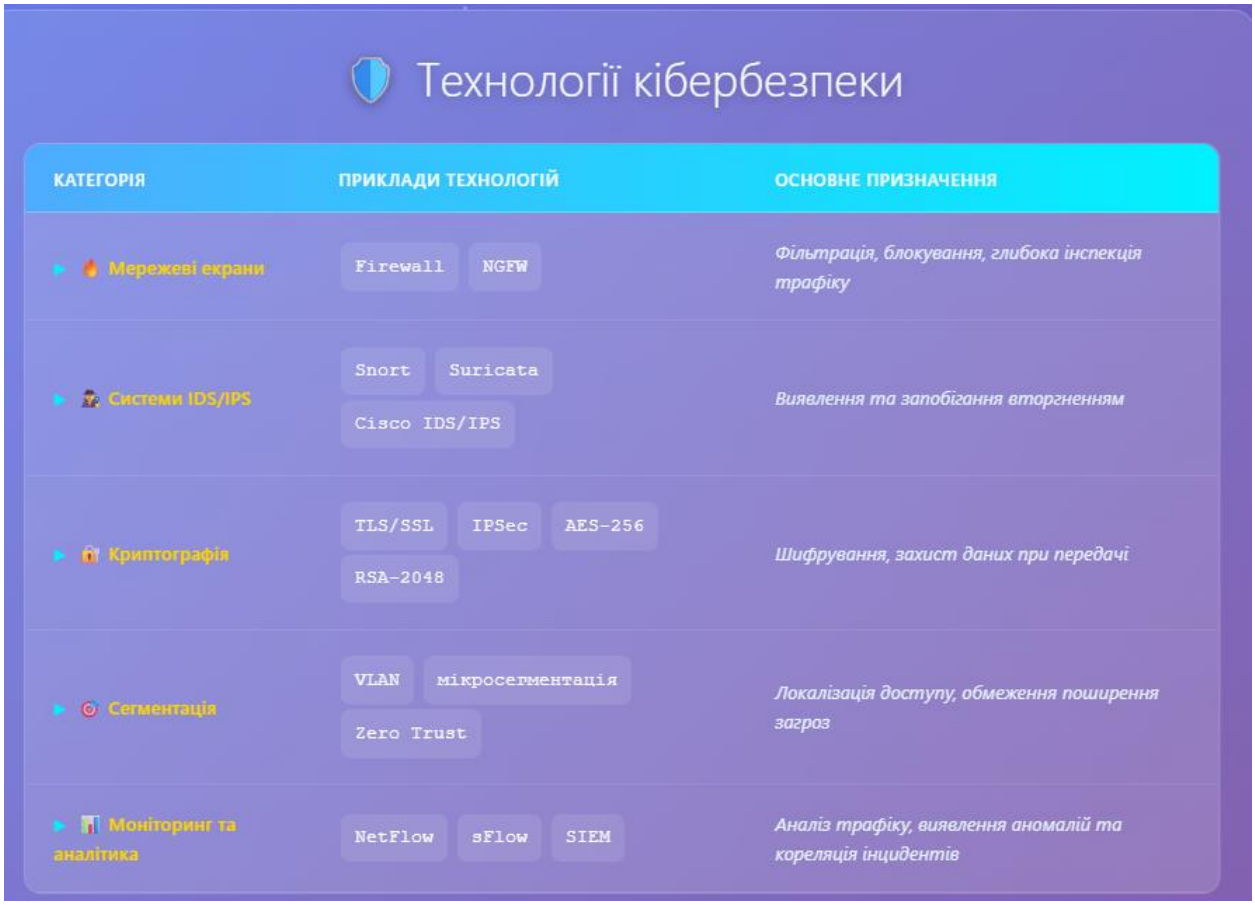
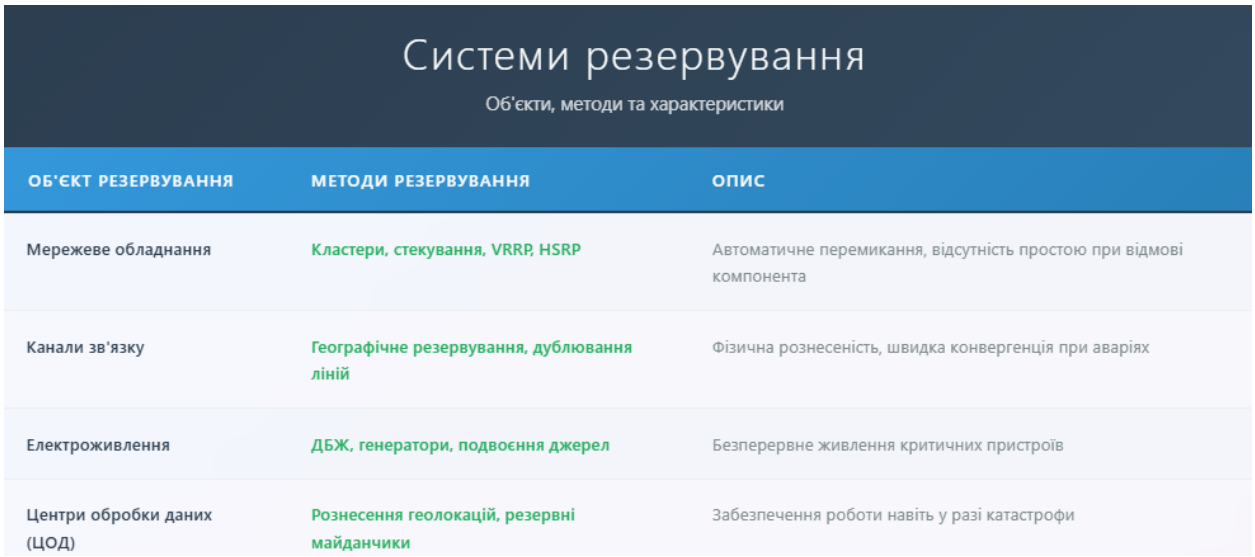


Рисунок 2.6 – Технології забезпечення безпеки корпоративної мережі

Високий рівень надійності мережі досягається лише за умови безперервного моніторингу та управління всіма її компонентами. SNMP дає змогу централізовано збирати та аналізувати інформацію про роботу мережевого обладнання, а потокові протоколи на кшталт NetFlow і sFlow дозволяють отримувати деталізовані дані про трафік. Це полегшує пошук вузьких місць, оптимізацію пропускної здатності та швидке реагування на підозрілу активність. Для централізації операцій із моніторингу й управління впроваджуються системи NMS, які інтегруються із helpdesk та дозволяють автоматизувати реагування на інциденти.

Велике значення має впровадження SIEM-систем, які дозволяють

корелювати журнали подій з різних джерел, формувати цілісну картину безпеки інфраструктури та своєчасно ідентифікувати складні багатоетапні атаки. Із розвитком технологій машинного навчання ці системи стають здатними до автоматичного виявлення аномалій навіть у раніше невідомих сценаріях. Нижче (рисунок 2.7) зведені ключові аспекти відмовостійкості корпоративної мережі.



Системи резервування

Об'єкти, методи та характеристики

ОБ'ЄКТ РЕЗЕРВУВАННЯ	МЕТОДИ РЕЗЕРВУВАННЯ	ОПИС
Мережеве обладнання	Кластери, стекування, VRRP, HSRP	Автоматичне перемикання, відсутність простою при відмові компонента
Канали зв'язку	Географічне резервування, дублювання ліній	Фізична рознесеність, швидка конвергенція при аваріях
Електроживлення	ДБЖ, генератори, подвоєння джерел	Безперервне живлення критичних пристроїв
Центри обробки даних (ЦОД)	Рознесення геолокацій, резервні майданчики	Забезпечення роботи навіть у разі катастрофи

Рисунок 2.7 – Системи резервування

Таким чином, сучасна корпоративна мережа будується на принципах багаторівневого захисту, резервування ключових компонентів і безперервного моніторингу. Тільки комплексний підхід дозволяє забезпечити її надійність, безпеку та готовність до непередбачуваних подій, що є запорукою стабільної роботи всієї організації як сьогодні, так і в майбутньому.

3 ПРОЕКТУВАННЯ ВИСОКОШВИДКІСНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Формування технічних вимог та завдань проектування

На початковому етапі проектування корпоративної мережі критично важливо провести детальний аналіз як функціональних, так і нефункціональних вимог, щоб забезпечити безперебійну і ефективну роботу всієї IT-інфраструктури компанії. Для цього необхідно врахувати специфіку кожного підрозділу (рисунок 3.1): IT, бухгалтерія, HR, маркетинг, продажі, логістика, виробництво та керівництво. Кожна структура організації має різний обсяг навантаження, кількість робочих місць, типи пристроїв (ПК, ноутбуки, мобільні пристрої), а також потреби у дротових і бездротових підключеннях, що напряму впливає на вимоги до пропускної здатності, відмовостійкості та безпеки мережі. Серед функціональних вимог ключовими є безперервний доступ користувачів до внутрішніх ресурсів, централізоване зберігання даних, висока швидкість обміну інформацією між підрозділами, резервне копіювання даних, а також стабільний доступ до сервісів дата-центру. До нефункціональних вимог відносяться вимоги до високої швидкості передачі даних, надійності системи (резервування каналів та вузлів), масштабованості архітектури для майбутнього розширення, а також підтримки сучасних протоколів і сервісів, зокрема VLAN, QoS, SDN.

Детальний розрахунок навантаження та трафіку проводиться на основі аналізу кількості користувачів у кожному підрозділі та типового сценарію їхньої роботи. Необхідно враховувати як середню, так і пікову інтенсивність трафіку, з урахуванням взаємодії з дата-центром, використанням хмарних сервісів, регулярного резервного копіювання, відеоконференцій, пересилання великих файлів і роботи критичних бізнес-застосунків (наприклад, ERP, CRM). Оцінюється загальна кількість пристроїв, максимальні одночасні з’єднання та вимоги до кожного типу підключення.

Визначення критеріїв ефективності мережі базується на потребі забезпечення мінімальних затримок при доступі до внутрішніх і зовнішніх сервісів, високої пропускної здатності (щонайменше 10 Gbps для access-рівня і від 40 до 100 Gbps для магістральних каналів), безперервної роботи мережі навіть у випадку аварійних ситуацій або виходу з ладу окремих елементів інфраструктури. Важливою є гнучкість управління та можливість швидкого масштабування системи під зростаючі потреби бізнесу, а також інтеграція з централізованими системами моніторингу і адміністрування.

Рисунок 3.1 – Аналіз відділів компанії

Таким чином, на етапі формування технічних вимог та завдань проектування розробляється повний перелік функціональних і нефункціональних критеріїв, аналізується поточне й прогнозоване навантаження на мережу, визначаються чіткі показники ефективності та умови для подальшого масштабування. Це дозволяє забезпечити відповідність проекту стратегічним і бізнес-цілям компанії, а також гнучкість і надійність IT-інфраструктури у довгостроковій перспективі.

3.2 Розробка архітектури та вибір топології мережі

Розробка сучасної корпоративної мережі передбачає вибір такої архітектури, яка дозволяє забезпечити максимальну ефективність, безпеку, відмовостійкість і масштабованість у динамічних умовах розвитку компанії. В даному проєкті обґрунтовано застосування ієрархічної трирівневої топології, що складається з основного (core), розподільчого (distribution) та доступового (access) рівнів. Такий підхід дозволяє раціонально організувати трафік між підрозділами, ізолювати різні логічні домени за допомогою VLAN, а також забезпечити резервування та балансування навантаження на кожному рівні. Застосування ієрархії допомагає чітко розмежувати функції: магістральні комутатори забезпечують високу пропускну здатність і швидкий обмін даними між головними сегментами, розподільчі пристрої відповідають за підключення підрозділів, а комутатори рівня доступу гарантують безпосередню роботу з робочими місцями користувачів.

Проектування логічної структури мережі базується на принципах централізації критичних сервісів у дата-центрі, чіткого розподілу трафіку між підрозділами та впровадження гнучкої системи VLAN. Кожен підрозділ отримує власний віртуальний сегмент для підвищення безпеки, ізоляції трафіку та оптимізації внутрішньої взаємодії. Всі основні сервіси — бази даних, додатки, файлові сховища — розміщуються у захищеному сегменті дата-центру, а доступ до них контролюється централізовано. Завдяки такому підходу забезпечується прозора маршрутизація, легкість адміністрування та швидка локалізація можливих збоїв.

Вибір протоколів передачі даних базується на потребі досягнення максимальної пропускної здатності та стійкості до збоїв. На фізичному рівні впроваджуються стандарти Ethernet (10/40/100 Gbps), що відповідає вимогам до сучасних високошвидкісних корпоративних мереж. Для маршрутизації та балансування навантаження застосовуються протоколи OSPF або BGP на рівні core і distribution, що дозволяє автоматично знаходити оптимальні

шляхи передачі трафіку та динамічно реагувати на зміни в мережевій топології. Для підвищення безпеки впроваджується 802.1X для контролю доступу до мережі, а IPSec використовується для тунелювання даних та захисту з'єднань між віддаленими сегментами. Пріоритезація критичного трафіку досягається завдяки впровадженню QoS, що дає змогу виділяти ресурси для ключових сервісів, таких як відеоконференції чи резервне копіювання, не знижуючи продуктивність решти системи.

Для ілюстрації наведемо типову структуру логічних сегментів та розподілу функцій обладнання (рисунок 3.2)

Політика мережевого доступу

ПІДРОЗДІЛ	VLAN ID	ДОСТУП ДО ДАТА-ЦЕНТРУ	ПРІОРИТЕТ ТРАФІКУ	ДОДАТКОВІ ВИМОГИ
IT-відділ	10	ПОВНИЙ	ВИСОКИЙ	*Підвищена безпека, WiFi 6E*
Бухгалтерія	20	ЧАСТКОВИЙ	СЕРЕДНІЙ	*Шифрування*
HR	30	ПОВНИЙ	СЕРЕДНІЙ	*Захист персональних даних*
Маркетинг	40	ПОВНИЙ	СЕРЕДНІЙ	*Відеоконференції*
Продажі	50	ПОВНИЙ	ВИСОКИЙ	*Мобільний доступ*
Логістика	60	ЧАСТКОВИЙ	СЕРЕДНІЙ	*Доступ 24/7*
Виробництво	70	ПОВНИЙ	ВИСОКИЙ	*Резервування каналів*
Керівництво	80	ПОВНИЙ	НАЙВИЩИЙ	*Безперебійний доступ*

Рисунок 3.2 – Політика мережевого доступу

Таким чином, впровадження ієрархічної архітектури, логічної сегментації та сучасних мережевих протоколів дозволяє створити надійну, гнучку й масштабовану інфраструктуру, здатну ефективно підтримувати всі бізнес-процеси компанії, оперативно адаптуватися до зростаючих вимог і забезпечувати найвищий рівень інформаційної безпеки.

3.3 Розрахунок параметрів мережі та планування масштабування

В процесі розрахунку параметрів мережі та планування масштабування особлива увага приділяється забезпеченню достатньої пропускної здатності каналів для різних сегментів інфраструктури, а також моделюванню майбутніх навантажень і побудові стратегії, що дозволяє оперативно реагувати на зростання потреб компанії. На першому етапі аналізується поточний та прогнозований обсяг трафіку з урахуванням кількості користувачів, пристроїв та інтенсивності обміну даними у всіх підрозділах. Для кожної ділянки мережі обирається така ширина смуги пропускання, яка дозволяє не лише покривати сучасні потреби, а й мати резерв для пікових навантажень, резервування або зростання обсягів трафіку у майбутньому. Особливо це актуально для магістральних каналів між ядром мережі (Core Switch) та розподільчими вузлами (Distribution Switch), де швидкість з'єднань сягає 100 Gbps, а між розподільчими та доступовими рівнями — 40 Gbps, що забезпечує стабільність та уникнення перевантажень навіть у випадку надзвичайних ситуацій.

Важливою складовою процесу є моделювання навантаження мережі із застосуванням спеціалізованих програмних інструментів, які дозволяють прогнозувати, як змінюватиметься трафік у різні години доби, при запуску нових бізнес-процесів, впровадженні хмарних сервісів чи зростанні кількості співробітників. На основі отриманих результатів визначаються потенційні “вузькі місця” у топології, розробляються сценарії резервування каналів, дублювання критичних сегментів, щоб запобігти втратам даних або зниженню продуктивності у разі збою. Завдяки цьому мережа отримує властивість самовідновлення та стійкості до навантажень.

Стратегія масштабування передбачає постійний моніторинг використання ресурсів, оцінку тенденцій зростання бізнесу й кількості пристроїв, що підключаються до мережі. Впровадження модульних комутаторів дозволяє легко додавати нові порти для підключення пристроїв

чи цілих підрозділів без повної перебудови інфраструктури. Гнучкість архітектури гарантує, що нові сегменти можуть інтегруватися без втрат продуктивності, а резервування портів на ключових комутаторах мінімізує простої під час розширення. Такий підхід дозволяє забезпечити стійкий розвиток мережі у відповідності до бізнес-потреб, а також підвищує ефективність інвестицій в IT-інфраструктуру.

Таким чином, завдяки грамотному розрахунку параметрів, використанню сучасних комутаторів з можливістю масштабування, а також моделюванню навантаження та закладанню значного резерву, корпоративна мережа може ефективно функціонувати сьогодні та бути готовою до майбутнього розширення, зберігаючи стабільність, надійність і продуктивність у будь-яких умовах.

3.4 Рішення щодо підвищення ефективності та захисту мережі

У сучасних корпоративних мережах питання підвищення ефективності та забезпечення комплексного захисту мають пріоритетне значення, оскільки саме вони визначають стійкість бізнесу до внутрішніх та зовнішніх викликів. Для оптимізації трафіку впроваджується політика управління смугою пропускання, заснована на сучасних механізмах QoS (Quality of Service)[11], які дозволяють розподіляти ресурси мережі відповідно до важливості різних сервісів. Критичні бізнес-додатки, системи відеоконференцій та резервного копіювання отримують підвищений пріоритет, що мінімізує затримки та втрати даних навіть при пікових навантаженнях. Додатково використовується балансування навантаження між серверами дата-центру, що дозволяє ефективно розподіляти трафік і запобігати перевантаженням окремих вузлів. У разі виявлення “вузьких місць” чи аномального збільшення навантаження впроваджується моніторинг та автоматичне перенаправлення трафіку, що забезпечує безперервність і стабільність сервісів.

З метою підвищення рівня безпеки всі ключові сегменти мережі

оснащуються багаторівневими міжмережевими екранами (firewall), які реалізують політики доступу відповідно до функціональних обов’язків підрозділів та окремих користувачів. Додатково інтегруються системи виявлення та запобігання вторгненням (IDS/IPS)[12], що дозволяють оперативно реагувати на спроби несанкціонованого доступу, атаки або підозрілу активність. Для захисту даних застосовується наскрізне шифрування трафіку як у внутрішньому периметрі, так і на стику з зовнішніми мережами. Контроль доступу до інфраструктури здійснюється через впровадження систем NAC (Network Access Control)[13], які забезпечують перевірку автентичності користувачів і пристроїв, а також протоколу 802.1X, що дозволяє обмежити доступ лише для авторизованих користувачів.

Реалізація сучасних рекомендацій щодо підвищення продуктивності передбачає впровадження новітніх стандартів бездротового зв’язку, таких як WiFi 6E, що дозволяє значно збільшити пропускну здатність та стабільність покриття у високонавантажених офісах. Важливо також проводити регулярний аудит мережевої інфраструктури (рисунок 3.3) для своєчасного оновлення обладнання, виявлення слабких місць та ліквідації застарілих технологій, які можуть бути вразливими до нових кіберзагроз. Ефективність функціонування мережі підтримується за рахунок організації централізованої системи моніторингу, що дозволяє в реальному часі відслідковувати всі ключові параметри, фіксувати інциденти і оперативно реагувати на потенційні загрози або збої.

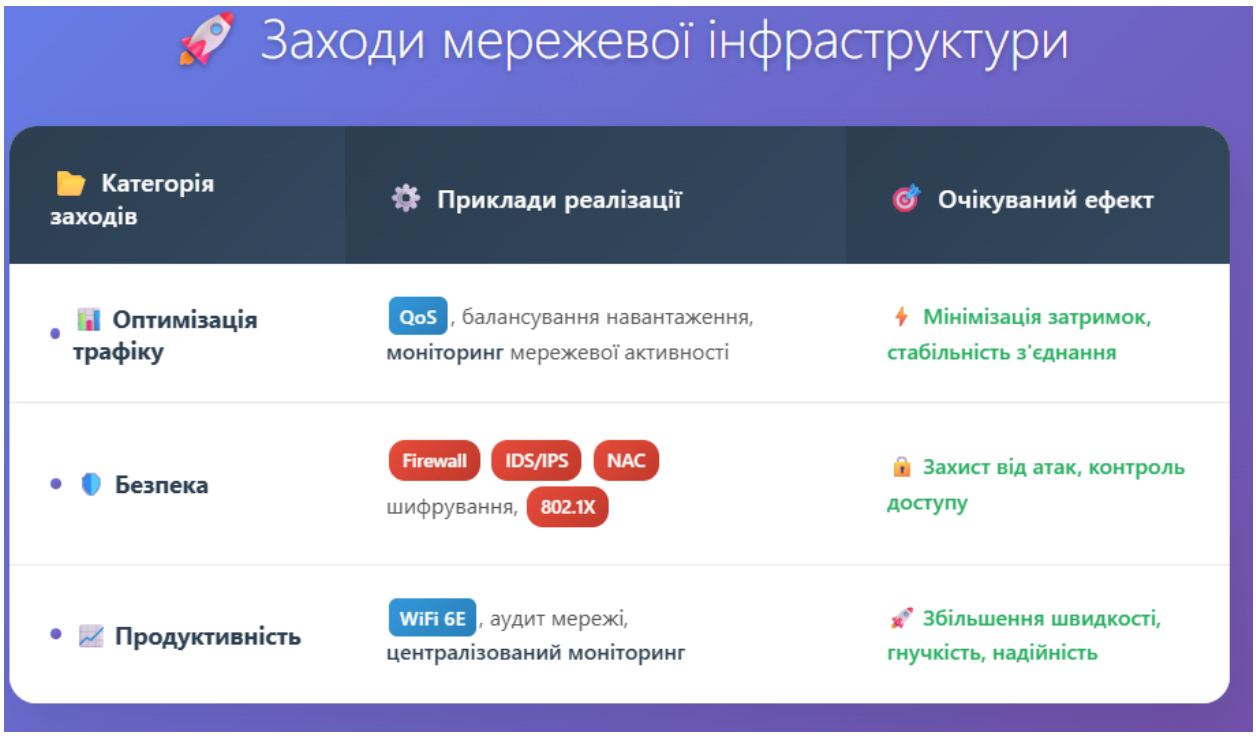


Рисунок 3.3 – Заходи мережної інфраструктури

Завдяки інтеграції описаних рішень корпоративна мережа не лише відповідає сучасним вимогам до продуктивності, але й гарантує максимальний рівень інформаційної безпеки та готовність до оперативної адаптації в умовах динамічного розвитку бізнесу.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ КОРПОРАТИВНОЇ МЕРЕЖІ

Дана схема (рисунок 4.1) представляє комплексну корпоративну мережевую архітектуру компанії "Osabizua", яка побудована за принципами високошвидкісної передачі даних та забезпечує надійне функціонування всіх підрозділів організації.

На самому верхньому рівні архітектури розташовано підключення до глобальної мережі Інтернет, яке проходить через потужний мережевий екран (Firewall). Цей компонент служить першою лінією захисту від зовнішніх загроз та контролює весь вхідний і вихідний трафік. Firewall забезпечує фільтрацію пакетів, захист від DDoS-атак та інших видів кібернетичних загроз, що може зіткнутися корпоративна мережа.

Безпосередньо за файрволом розташована двокомпонентна система ядрових комутаторів (Core Switch), кожен з яких забезпечує пропускну здатність 100 Гігабіт на секунду. Ці пристрої формують хребет всієї мережевої інфраструктури та забезпечують високошвидкісну комутацію між різними сегментами мережі. Використання двох ядрових комутаторів створює резервування на найвищому рівні, що гарантує безперервну роботу мережі навіть у випадку відмови одного з пристроїв.

Наступний рівень представлений чотирма розподільними комутаторами (Distribution Switch), позначеними як Dist. SW1, Dist. SW2, Dist. SW3 та Dist. SW4. Кожен з цих пристроїв має пропускну здатність 40 Гігабіт на секунду та виконує функції агрегації трафіку від підключених сегментів мережі. Розподільні комутатори забезпечують оптимальний розподіл навантаження та створюють додатковий рівень резервування для критично важливих з'єднань.

Центральною частиною інфраструктури є дата-центр (Data Center), який містить ключові серверні компоненти. До складу дата-центру входять сервер баз даних (DB Server), що зберігає всю корпоративну інформацію,

сервер додатків (App Server), який забезпечує роботу бізнес-логіки та корпоративних програм, а також веб-сервер (Web Server) для обслуговування веб-додатків та корпоративного порталу. Додатково дата-центр включає системи резервного копіювання (Backup), сховища даних (Storage) та засоби моніторингу (Monitor), які забезпечують надійність збереження даних та контроль за станом всієї інфраструктури.

На рівні доступу розташовані вісім комутаторів доступу (Access SW), кожен з яких забезпечує пропускну здатність 10 Гігабіт на секунду. Ці пристрої безпосередньо підключають кінцеві пристрої користувачів та забезпечують останню милю високошвидкісного з'єднання до корпоративної мережі.

Схема демонструє організаційну структуру компанії через вісім основних департаментів. IT відділ відповідає за технічну підтримку та розвиток інформаційних систем. Відділ бухгалтерії забезпечує фінансовий облік та звітність. HR департамент займається управлінням людськими ресурсами та кадровою політикою. Відділ маркетингу розробляє та реалізує стратегії просування продукції. Департамент продажів безпосередньо взаємодіє з клієнтами та забезпечує комерційну діяльність. Логістичний відділ координує постачання та розподіл товарів. Виробничий департамент контролює процеси створення продукції. Керівництво здійснює стратегічне управління всією організацією.

Кожен департамент має власну локальну інфраструктуру, що включає файловий сервер (FS) для зберігання відділових документів та даних, персональні комп'ютери (PC) для співробітників, а також точки бездротового доступу (WiFi 6E) для забезпечення мобільного доступу до мережевих ресурсів.

Технічні характеристики мережі вражають своїми показниками. Загальна пропускна здатність перевищує 200 Гігабіт на секунду, що забезпечує швидку передачу великих обсягів даних між різними сегментами мережі. Архітектура підтримує сучасні технології віртуалізації мереж,

включаючи VLAN для сегментації трафіку, QoS для пріоритизації критично важливих додатків та SDN для програмного управління мережевими ресурсами. Резервування реалізовано на всіх рівнях інфраструктури, що гарантує високу доступність сервісів. Цілодобовий моніторинг та управління забезпечують своєчасне виявлення та усунення потенційних проблем.

Система безпеки побудована за принципом багаторівневого захисту. Окрім основного файрволу, використовуються системи виявлення та запобігання вторгненням (IDS/IPS), які аналізують мережевий трафік на предмет підозрілої активності. Весь критично важливий трафік шифрується для захисту від перехоплення. Система контролю доступу до мережі (NAC) забезпечує автентифікацію та авторизацію всіх пристроїв, які намагаються підключитися до корпоративної інфраструктури.

Ця архітектура представляє сучасний підхід до побудови корпоративних мереж, який забезпечує високу продуктивність, надійність та безпеку для всіх бізнес-процесів організації.

Рисунок 4.1 – схема корпоративної мережі «OsabizUA»

4.1 Детальна архітектура корпоративної мережі "Osabizua"

4.1.1 Структурна схема мережі

Корпоративна мережа компанії "Osabizua"[10]. побудована за принципом класичної ієрархічної архітектури з використанням адресного простору 192.168.0.0/16, що забезпечує чітку логічну структуру та ефективне управління мережевими ресурсами. Основою цієї архітектури є трирівнева модель, де кожен рівень виконує специфічні функції та взаємодіє з суміжними рівнями для забезпечення безперебійної роботи всієї інфраструктури.

Точкою входу до корпоративної мережі служить мережевий екран з IP-адресою 192.168.1.1, який забезпечує контроль доступу до внутрішніх ресурсів з глобальної мережі Інтернет. Цей пристрій виконує функції глибокої фільтрації пакетів, захисту від мережевих атак та забезпечення безпечного NAT-перетворення для внутрішніх адрес.

Ядровий рівень представлений двома високопродуктивними комутаторами третього рівня з пропускною здатністю 100 Гігабіт на секунду кожен. Перший ядровий комутатор отримав адресу 192.168.1.10, а другий 192.168.1.11. Ці пристрої формують відмовостійкий xrebbet мережі з повним резервуванням критичних з'єднань. Вони забезпечують високошвидкісну комутацію між різними сегментами мережі та реалізують складні алгоритми балансування навантаження.

Розподільний рівень складається з чотирьох комутаторів з пропускною здатністю 40 Гігабіт на секунду кожен. Перший розподільний комутатор Dist SW1 має адресу 192.168.1.20, другий Dist SW2 адресу 192.168.1.21, третій Dist SW3 адресу 192.168.1.22, а четвертий Dist SW4 адресу 192.168.1.23. Ці пристрої агрегують трафік від комутаторів доступу та реалізують політики VLAN сегментації для різних департаментів організації.

Рівень доступу представлений вісьмома комутаторами з пропускною

здатністю 10 Гігабіт на секунду кожен. Кожен комутатор доступу обслуговує окремий департамент та має відповідну IP-адресу в діапазоні від 192.168.20.1 до 192.168.90.1 з кроком 10 для кожного наступного відділу. Така організація адресації забезпечує логічну відповідність між фізичним розташуванням обладнання та логічною структурою мережі.

Центральною частиною інфраструктури є дата-центр, який займає окрему підмережу 192.168.10.0/24. У складі дата-центру функціонують шість ключових серверів з чітко визначеними ролями та IP-адресами. Сервер баз даних з адресою 192.168.10.10 забезпечує централізоване зберігання та управління всією корпоративною інформацією. Сервер додатків з адресою 192.168.10.20 виконує бізнес-логіку та забезпечує роботу корпоративних програм. Веб-сервер з адресою 192.168.10.30 обслуговує внутрішні веб-додатки та корпоративний портал. Сервер резервного копіювання з адресою 192.168.10.40 забезпечує регулярне створення резервних копій критичних даних. Сервер зберігання з адресою 192.168.10.50 надає централізовані файлові сервіси для всіх департаментів. Сервер моніторингу з адресою 192.168.10.60 здійснює цілодобовий контроль за станом всієї інфраструктури.

Департаментська структура мережі відображає організаційну будову компанії та включає вісім основних підрозділів, кожен з яких має власну підмережу та VLAN. IT відділ займає VLAN 20 з адресним простором 192.168.20.0/24 та обслуговується комутатором доступу з адресою 192.168.20.1. Відділ бухгалтерії використовує VLAN 30 з підмережею 192.168.30.0/24 та комутатором 192.168.30.1. HR департамент працює в VLAN 40 з адресним простором 192.168.40.0/24 через комутатор 192.168.40.1. Відділ маркетингу розташований в VLAN 50 з підмережею 192.168.50.0/24 та комутатором 192.168.50.1. Департамент продажів використовує VLAN 60 з адресами 192.168.60.0/24 через комутатор 192.168.60.1. Логістичний відділ працює в VLAN 70 з підмережею 192.168.70.0/24 та комутатором 192.168.70.1. Виробничий департамент займає VLAN 80 з адресним простором 192.168.80.0/24 через комутатор

192.168.80.1. Керівництво компанії розташоване в VLAN 90 з підмережею 192.168.90.0/24 та комутатором доступу 192.168.90.1.

4.1.2 Схема фізичного підключення

Фізична архітектура корпоративної мережі побудована з використанням сучасних технологій структурованих кабельних систем та принципів ієрархічного з'єднання мережевого обладнання. Магістральні з'єднання між ядровими комутаторами та розподільними комутаторами реалізовані за допомогою оптоволоконних кабелів багатомодового типу OM4, що забезпечує передачу даних на високих швидкостях без втрат сигналу на відстанях до 400 метрів.

Фізичне з'єднання починається від мережевого екрану, який розташований в периметрі мережі та має двосистемне підключення до обох ядрових комутаторів для забезпечення відмовостійкості. Кожен ядровий комутатор з'єднаний з усіма чотирма розподільними комутаторами за допомогою окремих оптоволоконних ліній, що створює повнозв'язну топологію на рівні розподілу та забезпечує множинні шляхи для проходження трафіку.

Комутатори доступу підключені до розподільних комутаторів за принципом подвійного підключення, де кожен комутатор доступу має з'єднання з двома різними розподільними комутаторами. Такий підхід забезпечує резервування каналів зв'язку та можливість автоматичного перемикання на резервний шлях у випадку відмови основного з'єднання. З'єднання між розподільними комутаторами та комутаторами доступу реалізовані за допомогою оптоволоконних кабелів з роз'ємами SFP+ для забезпечення швидкості 10 Гігабіт на секунду.

Дата-центр має окреме високошвидкісне підключення безпосередньо до обох ядрових комутаторів за допомогою оптоволоконних каналів з пропускною здатністю 40 Гігабіт на секунду. Всі сервери в дата-центрі

підключені до спеціального серверного комутатора, який має агреговані порти до ядрових комутаторів. Кожен сервер обладнаний мережевими картами з підтримкою швидкості 10 Гігабіт на секунду та резервними портами для забезпечення відмовостійкості.

Горизонтальна кабельна система в кожному департаменті побудована на основі кабелів категорії 6A з екрануванням, що забезпечує передачу даних на швидкості до 10 Гігабіт на секунду на відстані до 100 метрів. Кожне робоче місце обладнане двома мережевими розетками для підключення комп'ютера та додаткових пристроїв, таких як IP-телефони або настільні комутатори.

Кожен департамент має власну комунікаційну шафу з комутатором доступу, patch-панелями, системами кабель-менеджменту та блоками безперебійного живлення. Шафи з'єднані між собою магістральними кабелями, що прокладені в спеціальних кабельних лотках з можливістю легкого доступу для обслуговування та модернізації.

Система електроживлення включає центральну UPS систему в дата-центрі потужністю достатньою для живлення всього критичного обладнання протягом щонайменше 30 хвилин, а також локальні UPS блоки в кожній комунікаційній шафі. Резервний дизель-генератор забезпечує довготривалу автономну роботу всієї інфраструктури у випадку тривалого відключення основного електроживлення.

4.1.3 Логічна схема адресації та маршрутизації

Логічна архітектура мережі побудована на основі класичної IP-адресації з використанням приватного адресного простору 192.168.0.0/16, що забезпечує достатню кількість адрес для всіх поточних та майбутніх потреб організації. Така схема адресації дозволяє легко ідентифікувати приналежність пристроїв до конкретних підрозділів та функціональних груп за третім октетом IP-адреси.

Управлінська підмережа займає діапазон 192.168.1.0/24 та включає всі критичні компоненти мережевої інфраструктури. Мережевий екран з адресою 192.168.1.1 служить default gateway для всіх внутрішніх підмереж та забезпечує маршрутизацію трафіку до зовнішніх мереж. Ядрові комутатори з адресами 192.168.1.10 та 192.168.1.11 реалізують внутрішню маршрутизацію між VLAN та забезпечують високошвидкісну комутацію трафіку. Розподільні комутатори з адресами від 192.168.1.20 до 192.168.1.23 виконують функції агрегації трафіку та реалізації політик якості обслуговування.

Серверна підмережа 192.168.10.0/24 консолідує всі серверні ресурси організації в єдиному логічному сегменті з підвищеними вимогами до безпеки та продуктивності. Сервер баз даних 192.168.10.10 зберігає критичну корпоративну інформацію та має пріоритетний доступ до мережевих ресурсів. Сервер додатків 192.168.10.20 забезпечує виконання бізнес-логіки та потребує стабільного з'єднання з сервером баз даних. Веб-сервер 192.168.10.30 обслуговує HTTP та HTTPS запити від користувачів всіх департаментів. Сервер резервного копіювання 192.168.10.40 працює переважно в нічні години для створення резервних копій. Сервер зберігання 192.168.10.50 надає файлові сервіси через протоколи SMB та NFS. Сервер моніторингу 192.168.10.60 збирає telemetry дані від всього мережевого обладнання та серверів.

Департаментські підмережі організовані за принципом десятків у третьому октеті, що створює логічну відповідність між номером VLAN та адресним простором. IT відділ в VLAN 20 використовує підмережу 192.168.20.0/24 з комутатором доступу 192.168.20.1. Робочі станції IT співробітників займають адреси від 192.168.20.10 до 192.168.20.13 для чотирьох комп'ютерів PC-IT-01 до PC-IT-04. Принтер IT відділу має статичну адресу 192.168.20.100, а точка бездротового доступу WiFi IT розташована за адресою 192.168.20.200.

Відділ бухгалтерії в VLAN 30 займає підмережу 192.168.30.0/24 з

комутатором доступу 192.168.30.1. Три робочі станції бухгалтерів PC-ACC-01, PC-ACC-02 та PC-ACC-03 мають адреси відповідно 192.168.30.10, 192.168.30.11 та 192.168.30.12. Ці комп'ютери потребують стабільного з'єднання з ERP системою на сервері додатків для обробки фінансових операцій.

HR департамент в VLAN 40 використовує підмережу 192.168.40.0/24 з комутатором доступу 192.168.40.1. Робоча станція PC-HR-01 з адресою 192.168.40.10 забезпечує доступ до систем управління персоналом. Принтер HR відділу за адресою 192.168.40.100 використовується для друку кадрових документів, а точка доступу WiFi HR з адресою 192.168.40.200 забезпечує бездротовий доступ для мобільних пристроїв.

Відділ маркетингу в VLAN 50 займає підмережу 192.168.50.0/24 з комутатором 192.168.50.1. Робоча станція PC-MKT-01 з адресою 192.168.50.10 використовується для роботи з CRM системами та маркетинговими додатками, що потребують значної пропускної здатності для обробки мультимедійного контенту.

Департамент продажів в VLAN 60 використовує підмережу 192.168.60.0/24 з комутатором доступу 192.168.60.1. Робоча станція PC-SALES-01 з адресою 192.168.60.10 забезпечує доступ до систем управління продажами. Принтер відділу продажів за адресою 192.168.60.100 використовується для друку комерційних пропозицій та договорів, а точка доступу WiFi Sales з адресою 192.168.60.200 дозволяє менеджерам з продажів працювати з мобільними пристроями.

Логістичний відділ в VLAN 70 займає підмережу 192.168.70.0/24 з комутатором 192.168.70.1. Робоча станція PC-LOG-01 з адресою 192.168.70.10 підключена до систем управління складом та відстеження вантажів.

Виробничий департамент в VLAN 80 використовує підмережу 192.168.80.0/24 з комутатором доступу 192.168.80.1. Робоча станція PC-PROD-01 з адресою 192.168.80.10 забезпечує управління виробничими

процесами. Принтер виробничого відділу за адресою 192.168.80.100 друкує технічну документацію, а точка доступу WiFi Prod з адресою 192.168.80.200 забезпечує бездротовий доступ для планшетів та мобільних сканерів на виробництві.

Керівництво компанії в VLAN 90 займає підмережу 192.168.90.0/24 з комутатором 192.168.90.1. Робоча станція PC-MGMT-01 з адресою 192.168.90.10 має привілейований доступ до всіх корпоративних систем та бізнес-аналітики.

Маршрутизація в мережі реалізована за допомогою статичних маршрутів на ядрових комутаторах з резервуванням через протокол VRRP. Кожна департаментська підмережа має default gateway на відповідному комутаторі доступу, який перенаправляє міжмережевий трафік до ядрових комутаторів. Ядрові комутатори обмінюються маршрутною інформацією та забезпечують оптимальні шляхи до всіх призначень.

Політики безпеки реалізовані через Access Control Lists на ядрових комутаторах, які контролюють трафік між різними VLAN. Серверна підмережа має підвищений рівень захисту з обмеженим доступом тільки для авторизованих користувачів. Міждепартаментський трафік фільтрується відповідно до корпоративних політик безпеки, а весь зовнішній трафік проходить через мережевий екран з глибокою інспекцією пакетів.

4.2 Специфікація мережевого обладнання та програмного забезпечення

4.2.1 Обґрунтування вибору маршрутизаторів та комутаторів

У корпоративній мережі реалізовано сучасний набір активного мережевого обладнання, серверної інфраструктури й програмних засобів керування та безпеки, які відповідають вимогам до продуктивності, масштабованості й захищеності.

Ядро мережі побудовано на базі двох високопродуктивних комутаторів

рівня Core, кожен з яких має пропускну здатність 100 Гбіт/с і підтримує функції L3-маршрутизації, стекування, резервування модулів живлення та вентиляції. Такі комутатори забезпечують швидкісний обмін даними між усіма сегментами мережі та резервування каналів у разі відмови одного з пристроїв. Для підключення зовнішніх мереж і захисту периметра використовується апаратний міжмережевий екран із підтримкою інтелектуальної фільтрації, контролю доступу, NAT, VPN та захисту від атак (наприклад, серії Cisco ASA, Fortinet FortiGate або MikroTik CCR).

Розподільний рівень реалізовано на чотирьох комутаторах із пропускною здатністю 40 Гбіт/с, які мають достатню кількість SFP+/QSFP+ портів для підключення access-комутаторів і серверного обладнання. Ці пристрої підтримують VLAN, ACL, маршрутизацію на третьому рівні, стекування, а також політики QoS для ефективного розподілу мережевого навантаження.

Для підключення кінцевих пристроїв у підрозділах використано керовані комутатори доступу з портами 10 Гбіт/с, підтримкою Power over Ethernet Plus (802.3at), VLAN, 802.1X, SNMP та можливістю централізованого адміністрування. Завдяки PoE+ забезпечується живлення IP-телефонів, точок WiFi та мережевих камер без додаткових блоків живлення.

Серверне обладнання розташоване у виділеному дата-центрі й представлено окремими фізичними або віртуалізованими серверами, кожен із яких виконує власну роль: сервер баз даних, сервер додатків, веб-сервер, сервер резервного копіювання, сховище та сервер моніторингу. Для високої доступності використовуються багатопроцесорні сервери із підтримкою RAID, гарячої заміни дисків і мережевих інтерфейсів 10GBase-T або SFP+. Для організації централізованого сховища даних доцільно використовувати NAS-систему із підтримкою багаторівневого RAID і резервного копіювання.

Для організації бездротового доступу в офісі впроваджені точки доступу стандарту WiFi 6E з підтримкою роботи у всіх актуальних

діапазонах, централізованим адмініструванням, роумінгом і WPA3-Enterprise. Це дозволяє створити окремі сегментовані SSID для співробітників, гостей і IoT-пристроїв, ізоляцію трафіку через VLAN і гарантувати безперебійний доступ у будь-якій частині офісу.

Адміністрування та моніторинг мережевої інфраструктури здійснюється за допомогою спеціалізованого програмного забезпечення: систем моніторингу стану обладнання (наприклад, Zabbix, PRTG, SolarWinds), SIEM-платформ для аналізу подій безпеки, контролерів бездротової мережі (UniFi Controller, Aruba Central)[14]. та систем для управління резервним копіюванням (Veeam, Nakivo). Для віртуалізації серверів використовуються платформи VMware vSphere або Microsoft Hyper-V, що дозволяє забезпечити гнучке розподілення ресурсів і швидке відновлення у разі збоїв.

Завдяки такій специфікації обладнання й програмного забезпечення мережа підтримує високу пропускну здатність, захищеність даних, централізоване адміністрування та гнучкість масштабування відповідно до потреб організації.

4.2.2 Вибір серверного обладнання

Для побудови корпоративної мережі такого рівня доцільно використовувати потужний міжмережевий екран, наприклад, Fortinet FortiGate 100F із підтримкою інтегрованого VPN, систем IDS/IPS, web-фільтрації та розширених засобів аналітики безпеки. Ядро мережі доцільно організувати на базі L3-комутаторів Cisco Catalyst 9500-32C з портами 40/100GbE, підтримкою стекування, розширеними функціями маршрутизації, високою надійністю та відмовостійкістю. Розподільний рівень оптимально будувати на Cisco Catalyst 9300-48UB, який є стекованим L3-комутатором із PoE+, підтримкою 10GbE uplinks і чудово підходить для агрегації трафіку між відділами й доступу до серверної. Хорошим вибором також буде HPE

Aruba 2930M 48G 1-slot1, що підтримує стекування, VLAN, PoE+ і 10GbE uplinks через SFP+.

Для рівня доступу найкраще підійде Cisco Catalyst 9200-24P-E із 24 портами 1GbE, підтримкою PoE+ для точок WiFi, IP-телефонів, принтерів і комп'ютерів. Для малих підрозділів практичним вибором стане Aruba 2530-24G-PoE+ як базовий керований комутатор, а для сегментів із підвищеними швидкісними вимогами економічним варіантом є MikroTik CRS326-24S+2Q+RM із великою кількістю SFP+ портів. Система бездротового доступу базується на сучасних точках доступу Ubiquiti UniFi U6 Enterprise із підтримкою WiFi 6E, діапазонів 2.4/5/6 GHz, технологіями MU-MIMO та централізованим керуванням через UniFi Network Controller.

Серверна частина побудована на універсальних двопроцесорних серверах HPE ProLiant DL380 Gen11, які підходять для розміщення баз даних і віртуалізації, мають підтримку до 8/12 SSD/HDD, вбудований RAID-контролер і масштабування до 2 ТБ оперативної пам'яті.. Для менш навантажених сервісів, додаткових ролей або резервування можна застосувати HPE ProLiant DL360 Gen11. Функції централізованого зберігання даних і резервного копіювання виконує а, який має два джерела живлення, підтримку RAID 5/6/10 і можливість гарячої заміни дисків.

Джерела безперебійного живлення, такі як APC Smart-UPS SRT2200XLI, використовуються для захисту серверної та мережевого обладнання від перебоїв електропостачання. Для організації централізованого керування електроживленням комутаційних шаф застосовуються керовані розетки типу APC AP7921B. Моніторинг і адміністрування інфраструктури здійснюється за допомогою систем Zabbix або PRTG Network Monitor[15], а для WiFi-сегменту — через UniFi Controller.

Усі запропоновані моделі обладнання відповідають сучасному корпоративному рівню, відзначаються масштабованістю, підтримкою необхідних протоколів маршрутизації, VLAN, QoS, 802.1X, PoE+, мають високу надійність і широке ком'юніті підтримки. Ubiquiti UniFi ідеально

підходить для малого та середнього бізнесу, тоді як Cisco, Juniper, HPE й Aruba — це класичний вибір для enterprise-мереж будь-якої складності. Конфігурацію можна адаптувати відповідно до бюджету, технічних завдань чи вподобань, а також деталізувати під потреби конкретних ділянок мережі — наприклад, підібрати SFP+/QSFP+ модулі для аплінків, оптимізувати компонування для стійкового монтажу або розширити функціонал за рахунок програмних ліцензій і додаткових аксесуарів.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було встановлено, що сучасна високошвидкісна корпоративна комп’ютерна мережа є критично важливою складовою інфраструктури компанії "OsabizUA" у контексті цифрової трансформації та зростаючих вимог до продуктивності й безпеки бізнес-процесів. У результаті проведених етапів роботи було проаналізовано вихідний стан мережевої інфраструктури, досліджено провідні тенденції й технології побудови корпоративних мереж, визначено технічні вимоги, підібрано оптимальне мережеве обладнання та обґрунтовано економічну доцільність запропонованих рішень.

Розроблений проєкт мережевої інфраструктури забезпечує стабільний, захищений і високопродуктивний обмін даними між усіма підрозділами компанії, підтримує впровадження сучасних інформаційних сервісів, таких як хмарні технології, відеоконференції та інструменти для колективної роботи. Запропонована архітектура дозволяє масштабувати мережу у разі зростання компанії, забезпечує мінімізацію затримок, підвищує рівень інформаційної безпеки й стійкості до зовнішніх загроз.

Практична значущість проєкту полягає в можливості реального впровадження нової мережевої інфраструктури для оптимізації діяльності "OsabizUA", підвищення ефективності роботи персоналу та покращення якості сервісу для клієнтів. Водночас запропоновані рішення можуть стати корисною основою для інших підприємств, що прагнуть модернізувати власні корпоративні мережі відповідно до сучасних вимог цифрової економіки.

Загалом результати цієї роботи підтверджують, що інвестування у розвиток високошвидкісних і надійних корпоративних мереж є стратегічно виправданим кроком для забезпечення конкурентоспроможності, інноваційності та сталого розвитку компаній на сучасному ринку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Кузьменко Н.В., Горбанський В.М. Комп'ютерні мережі та телекомунікації: підручник. – К.: Професіонал, 2007. – 672 с.

2. Петренко А.І., Семенов Ю.А. Основи мережевих технологій. – К.: Техніка, 2008. – 544 с.

3. Дорошенко А.Ю., Яременко О.А. Адміністрування мереж TCP/IP: навчальний посібник. – Х.: НТУ «ХПІ», 2010. – 280 с.

4. Костров Б.В., Ручкін В.Н. Комп'ютерні мережі: архітектура, протоколи, безпека. – М.: Кудіц-Образ, 2006. – 336 с.

5. Максимов Н.В., Попов І.І. Комп'ютерні мережі: навчальний посібник. – 3-тє вид. – М.: Форум, 2010. – 448 с.

6. Новіков Ю.В., Кондратенко С.В. Локальні мережі: архітектура, алгоритми, проектування. – М.: ЕКОМ, 2004. – 312 с.

7. Гриценко В.І., Жукова Г.В. Теорія телетрафіку та її застосування: монографія. – К.: Наукова думка, 2005. – 452 с.

8. Стіллінгс В. Криптографія та захист мереж: принципи та практика. – 4-те вид. – М.: Вільямс, 2007. – 672 с.

9. Поляк-Брагінський О.В. Локальні обчислювальні мережі: навчальний посібник. – К.: Університет «Україна», 2009. – 368 с.

10. Шиндер Д.Л., Шиндер Т.В. Комп'ютерні мережі Microsoft: технічний довідник. – К.: Російська редакція, 2003. – 736 с.

11. Бабенко В.П., Маслов О.М. Структуровані кабельні системи // Зв'язок. – 2008, №3. – С. 28–32.

12. Кириченко Л.О., Радченко В.Г. Методи оптимізації мережевого трафіку в корпоративних мережах // Проблеми програмування. – 2007, №2-3. – С. 156–164.

13. IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—

Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2020.

14. RFC 791 Internet Protocol - DARPA Internet Program Protocol Specification [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc791

15. RFC 2616 Hypertext Transfer Protocol -- HTTP/1.1 [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2616