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)

Територіально-розподілена корпоративна комп'ютерна мережа страхової компанії 'ВУСО ГРУП'

(тема)

Виконав:
здобувач 4 року навчання,
групи КІУКІ-21-2
Павло КЕЛЕБЕРДА
(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 Келеберді Павлу Олександровичу
(прізвище, ім’я, по батькові)

1. Тема роботи Територіально-розподілена корпоративна комп'ютерна мережа страхової компанії 'ВУСО ГРУП'

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 БАЗОВІ ПОНЯТТЯ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ
2 АРХІТЕКТУРА ТА ТЕХНОЛОГІЇ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ
3 ОПИС ОБ’ЄКТА ВПРОВАДЖЕННЯ
4 ТЕХНІЧНЕ РІШЕННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій 14 слайдів

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: 66 с., 15 рис., 0 табл., 1 дод., 12 джерел.

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

Метою кваліфікаційної роботи є розробка проекту територіально-розподіленої корпоративної комп’ютерної мережі страхової компанії «ВУСО ГРУП», яка забезпечить ефективний, безпечний та безперервний обмін інформацією між усіма структурними підрозділами компанії, а також відповідатиме сучасним вимогам щодо масштабованості, інформаційної безпеки та стійкості до збоїв.

У ході виконання кваліфікаційної роботи проведено аналіз існуючих мережевих технологій, обґрунтовано вибір архітектури корпоративної мережі, підібрано оптимальне мережеве обладнання та програмне забезпечення, розроблено структурну та функціональну схему мережі, а також визначено основні заходи із забезпечення інформаційної безпеки та стійкості до збоїв. Запропоноване рішення дозволяє централізовано керувати інформаційними потоками, забезпечити відмовостійкість системи та організувати ефективний захист корпоративних даних.

ABSTRACT

Bachelor’s thesis: 66 pages, 15 figures, 0 tables, 1 appendix, 12 sources.

COMPUTER NETWORK, INTERNET, ROUTER, PROTOCOL, SERVER, GATEWAY, FIREWALL, WI-FI, WLAN.

The purpose of this qualification thesis is to develop a project for a geographically distributed corporate computer network for the insurance company "VUSO GROUP," which will provide efficient, secure, and uninterrupted information exchange between all structural divisions of the company, as well as comply with modern requirements for scalability, information security, and fault tolerance.

During the execution of the thesis, an analysis of existing network technologies was carried out, the choice of corporate network architecture was substantiated, optimal network equipment and software were selected, a structural and functional network diagram was developed, and key measures for ensuring information security and system resilience were defined. The proposed solution allows for centralized management of information flows, ensures the system’s fault tolerance, and organizes effective protection of corporate data.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

AES – Advanced Encryption Standard (стандарт симетричного шифрування)

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

DNS – Domain Name System (система доменних імен)

IPS – Intrusion Prevention System (система запобігання вторгненням)

LAN – Local Area Network (локальна мережа)

VPN – Virtual Private Network (віртуальна приватна мережа)

WAN – Wide Area Network (глобальна мережа)

Wi-Fi – Wireless Fidelity (бездротова мережа)

WLAN – Wireless Local Area Network (бездротова локальна мережа)

ВСТУП

Сучасний розвиток інформаційних технологій та цифрова трансформація бізнес-процесів кардинально змінили підходи до організації діяльності великих корпоративних структур. Страхові компанії, які традиційно працювали з великими масивами даних та потребували надійного інформаційного обміну між різними підрозділами, стали одними з перших, хто активно впроваджував сучасні мережеві рішення. Особливо актуальним це питання стає для компаній з територіально розподіленою структурою, де необхідність забезпечення стабільного та безпечного зв'язку між віддаленими офісами є критично важливою для ефективного функціонування бізнесу.

Страхова компанія "ВУСО ГРУП" представляє собою типовий приклад сучасної корпоративної структури з широкою мережею філій та представництв, розташованих у різних регіонах України[1]. Забезпечення ефективної взаємодії між головним офісом, регіональними центрами та локальними підрозділами вимагає створення надійної, масштабованої та безпечної корпоративної комп'ютерної мережі. Така мережа повинна не лише забезпечувати швидкий доступ до корпоративних ресурсів та баз даних, але й гарантувати високий рівень інформаційної безпеки, що є особливо критичним для страхової галузі з огляду на необхідність захисту персональних даних клієнтів.

Проектування територіально-розподіленої корпоративної мережі для страхової компанії передбачає вирішення комплексу складних технічних завдань. До них належать вибір оптимальної топології мережі, забезпечення відмовостійкості системи, організація централізованого управління мережевими ресурсами, впровадження ефективних механізмів резервного копіювання та відновлення даних. Особливу увагу необхідно приділити питанням масштабованості системи, оскільки страхові компанії часто розширюють свою мережу представництв, що вимагає гнучкості

архітектурних рішень.

Актуальність даної кваліфікаційної роботи обумовлена зростаючими вимогами до якості та надійності корпоративних мережевих рішень у страховій галузі. Сучасні регуляторні вимоги щодо захисту персональних даних, необхідність забезпечення безперервності бізнес-процесів та підвищення ефективності роботи співробітників створюють потребу в комплексному підході до проектування мережевої інфраструктури. Крім того, пандемія COVID-19 та пов'язані з нею обмеження актуалізували питання організації віддаленої роботи співробітників, що додатково підкреслює важливість створення гнучких та адаптивних мережевих рішень.

Метою даної кваліфікаційної роботи є розробка проекту територіально-розподіленої корпоративної комп'ютерної мережі для страхової компанії "ВУСО ГРУП", яка забезпечуватиме ефективну взаємодію між усіма підрозділами компанії, високий рівень інформаційної безпеки та можливість масштабування системи відповідно до потреб бізнесу. У рамках роботи планується провести аналіз існуючих технологічних рішень, розробити оптимальну архітектуру мережі, обґрунтувати вибір обладнання та програмного забезпечення, а також розрахувати економічну ефективність запропонованого рішення.

Практична значущість дослідження полягає в можливості використання розроблених рекомендацій та проектних рішень не лише для страхової компанії "ВУСО ГРУП", але й для інших організацій аналогічного профілю та масштабу. Запропоновані в роботі підходи до проектування територіально-розподілених мереж можуть стати основою для створення типових рішень у страховій галузі, що сприятиме підвищенню загального рівня технологічного розвитку галузі та покращенню якості обслуговування клієнтів.

1 БАЗОВІ ПОНЯТТЯ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ

1.1 Основні поняття та сутність комп'ютерних мереж

Комп'ютерна мережа являє собою сукупність взаємопов'язаних комп'ютерів та периферійних пристроїв, які з'єднані каналами зв'язку для обміну інформацією та спільного використання ресурсів. Основною метою створення комп'ютерних мереж є забезпечення ефективного обміну даними між користувачами, розташованими на різних робочих станціях, та надання доступу до спільних ресурсів системи.

Ключовими компонентами комп'ютерної мережі є кінцеві вузли (робочі станції, сервери), мережеве обладнання (комутатори, маршрутизатори, концентратори), канали зв'язку (кабельні та бездротові з'єднання) та мережеве програмне забезпечення[2]. Кожен компонент виконує специфічні функції, які в сукупності забезпечують надійне функціонування мережевої інфраструктури.

Основними принципами організації комп'ютерних мереж є модульність, масштабованість, надійність та безпека. Модульність передбачає можливість поетапного нарощування мережі шляхом додавання нових компонентів. Масштабованість забезпечує здатність мережі розширюватися без суттєвого зниження продуктивності. Надійність гарантує стабільне функціонування системи навіть при виході з ладу окремих компонентів. Безпека передбачає захист даних від несанкціонованого доступу та втрати інформації.

Переваги використання комп'ютерних мереж включають спільне використання дорогого обладнання, централізоване зберігання та резервне копіювання даних, підвищення продуктивності праці завдяки автоматизації бізнес-процесів, а також забезпечення оперативного обміну інформацією між співробітниками. Для страхових компаній особливо важливими є можливості

централізованого управління клієнтською базою, автоматизації процесів оформлення полісів та врегулювання страхових випадків.

1.2 Класифікація та види мережевих систем

Комп'ютерні мережі класифікуються (рисунок 1.1) за різними критеріями, що дозволяє обрати оптимальне рішення для конкретних потреб організації. Основними критеріями класифікації є географічна поширеність, топологія, метод доступу до середовища передачі, тип використовуваного обладнання, спосіб організації, тип передачі даних та функціональне призначення мережі.

За географічною поширеністю розрізняють[4] персональні мережі (PAN), локальні мережі (LAN), мережі кампусу (CAN), міські мережі (MAN) та глобальні мережі (WAN). Персональні мережі (PAN) охоплюють простір навколо окремого користувача, зазвичай до 10 метрів, і забезпечують взаємодію між пристроями однієї особи. Локальні мережі (LAN) об'єднують пристрої в межах одного приміщення або будівлі на відстані до декількох кілометрів, що є типовим для офісів і підприємств. Мережі кампусу (CAN) з’єднують декілька будівель на обмеженій території, наприклад, кампус університету чи офісний комплекс. Міські мережі (MAN) покривають територію міста, забезпечуючи зв'язок між окремими організаціями, а глобальні мережі (WAN) можуть охоплювати необмежені географічні території, з’єднуючи офіси, філії та дата-центри по всьому світу.

За способом організації розрізняють однорангові (peer-to-peer) мережі та мережі з виділеним сервером (client-server). В однорангових мережах всі комп'ютери мають рівні права і можуть функціонувати як клієнти і як сервери одночасно. Така організація підходить для невеликих робочих груп до 10-15 користувачів, оскільки проста в налаштуванні, проте має обмеження щодо безпеки та продуктивності[3]. Мережі з виділеним сервером мають централізовану архітектуру, де один або кілька серверів надають сервіси

клієнтським станціям. Цей тип оптимальний для середніх та великих корпоративних мереж, забезпечує централізоване управління, масштабованість і підвищену безпеку.

За типом передачі даних мережі поділяються на провідні та бездротові. Провідні мережі використовують фізичні канали зв'язку — мідні кабелі (виті пари, коаксіальні кабелі) та оптоволоконні кабелі. Вони відзначаються високою швидкістю передачі даних, стабільністю і захищеністю від зовнішніх впливів. Бездротові мережі базуються на радіохвилях, інфрачервоному випромінюванні або супутникових каналах зв'язку. Основними перевагами є мобільність і простота розгортання, а недоліками — схильність до перешкод і обмежена пропускна здатність.

За функціональним призначенням виділяють обчислювальні мережі (Data Networks)[5,6], мережі зберігання даних (SAN), телекомунікаційні мережі (Telecommunication Networks) та мультимедійні мережі (Multimedia Networks). Для страхових компаній найбільш актуальними є обчислювальні мережі та мережі зберігання даних, оскільки вони забезпечують ефективну обробку великих обсягів інформації та надійне зберігання критично важливих даних, що сприяє підвищенню рівня обслуговування клієнтів і захисту інформації.

Класифікація комп'ютерних мереж

Систематизація мережевих технологій за основними критеріями

КРИТЕРІЙ	ТИП МЕРЕЖІ	ОПИС	ДАЛЬНІСТЬ / КОРИСТУВАЧІ	ПРИКЛАДИ ВИКОРИСТАННЯ
ГЕОГРАФІЧНА ЗОНА	PAN	Персональна мережа	до 10 м / 1–2 користувачі	Bluetooth-пристрої, носимі гаджети
	LAN	Локальна мережа	до 1–2 км / 10–1000 користувачів	Офіс, школа, підприємство
	CAN	Мережа кампусу	до 10 км / 100–10000 користувачів	Університет, бізнес-кампус
	MAN	Міська мережа	до 50 км / багато користувачів	Зв'язок між філіями у місті
	WAN	Глобальна мережа	необмежено / тисячі користувачів	Корпоративна мережа з філіями
ОРГАНІЗАЦІЯ	Одноранговa	Всі пристрої рівноправні	до 15	Невелика робоча група
	З сервером	Сервер надає сервіси	15+ більше	Корпоративна мережа
ТИП ПЕРЕДАЧІ	Провідна	Кабелі (мідь, оптика)	—	Стаціонарні мережі
	Бездротова	Радіо, ІЧ, супутник	—	Wi-Fi, мобільні мережі
ПРИЗНАЧЕННЯ	Обчислювальна	Передача, обробка даних	—	Офісні додатки-центри
	Зберігання даних	Централізоване зберігання	—	SAN, резервне копіювання
	Телекомунікаційна	Передача голосу, відео, сигналів	—	IP-телефонія, відеоконференції
	Мультимедійна	Передача мультимедійного контенту	—	Стримінг, цифрове телебачення

Рисунок 1.1 – Класифікація комп'ютерних мереж

1.3 Структурна організація та топологічні рішення мереж

Топологія комп’ютерної мережі (рисунок 1.2) — це спосіб фізичного або логічного з’єднання всіх її компонентів. Саме від вибору топології значною мірою залежать такі характеристики мережі, як продуктивність, надійність, масштабованість, а також вартість створення й обслуговування інфраструктури. Серед найпоширеніших топологій виділяють шину, зірку, кільце, сітку та ієрархічну структуру.

У топології "шина" всі пристрої підключаються до одного спільного кабелю, який слугує магістраллю для передавання даних. Це рішення відрізняється простотою і економічністю, дозволяє швидко підключати нові пристрої та зменшує витрати на кабелі. Водночас головними недоліками є

низька відмовостійкість (адже пошкодження магістрального кабелю паралізує всю мережу), складність діагностики несправностей і зниження пропускної здатності при збільшенні кількості учасників.

У разі топології "зірка" всі пристрої під’єднуються до центрального вузла — це може бути комутатор, концентратор або маршрутизатор. Така схема забезпечує високу надійність: вихід з ладу одного пристрою не впливає на інші, адміністрування стає простішим, а несправності легко виявляються. Проте єдиний центральний вузол стає точкою відмови всієї мережі, а витрати на прокладання кабелів зростають.

Топологія "кільце" ґрунтується на послідовному з’єднанні пристроїв у замкнене коло. Дані рухаються по кільцю в одному напрямку, що виключає колізії та гарантує пропускну здатність для кожного пристрою, а також дає змогу охоплювати великі відстані. Однак така мережа не відрізняється відмовостійкістю, її конфігурація ускладнюється зі зростанням кількості вузлів, а будь-яка несправність або додавання нового пристрою впливає на роботу всієї мережі.

Сітчаста топологія вирізняється тим, що кожен пристрій може бути з’єднаний одразу з кількома іншими, створюючи численні альтернативні шляхи для передавання даних. Повна сітка передбачає наявність з’єднань між усіма можливими парами пристроїв, що забезпечує максимальну надійність, оскільки у разі збою одного з каналів дані проходять іншими маршрутами. Однак така структура складна в реалізації та потребує значних витрат на кабелі й обладнання.

У корпоративних мережах страхових компаній, які мають багаторівневу організацію, найчастіше використовується ієрархічна топологія, яка поєднує елементи декількох базових схем. Вона охоплює рівень доступу для кінцевих пристроїв, рівень розподілу для агрегації трафіку та основний рівень, що забезпечує швидкісний обмін між різними сегментами мережі. Такий підхід дозволяє досягти гнучкості, масштабованості та централізованого адміністрування, що особливо важливо

для організацій із великою кількістю підрозділів і високими вимогами до надійності мережі.

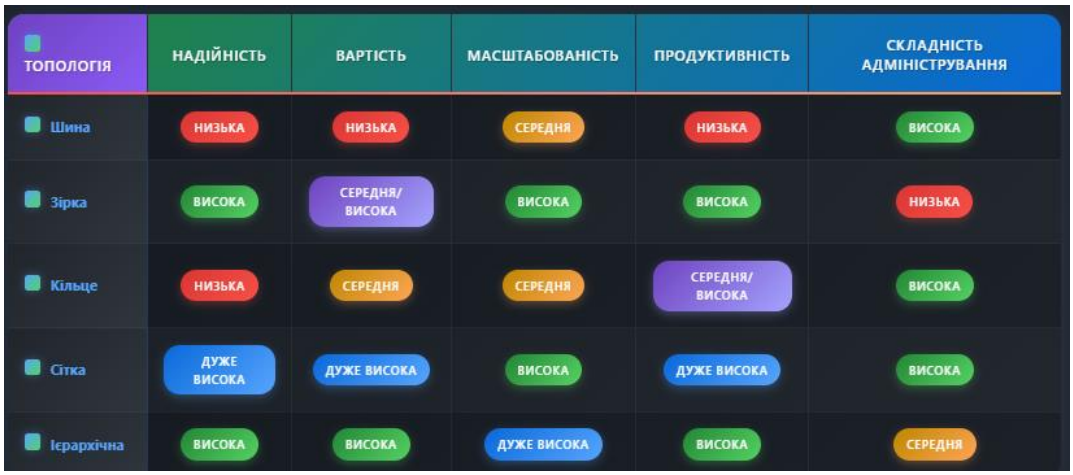


Рисунок 1.2 – Аналіз характеристик основних топологічних рішень

1.4 Стек протоколів TCP/IP та його компоненти

Стек протоколів TCP/IP (рисунок 1.3) – це комплекс взаємопов’язаних мережевих протоколів, які утворюють основу сучасних комп’ютерних мереж. Його ключова перевага полягає в універсальності: рішення, розроблені на базі TCP/IP, здатні ефективно функціонувати у гетерогенному середовищі, що складається з пристроїв різних виробників, різних типів операційних систем та різних фізичних середовищ передачі. В основі архітектури TCP/IP лежить чотиришарова модель, кожен рівень якої має чітко визначені завдання та забезпечує розмежування функцій. На фізичному рівні реалізується передача бітових потоків через різноманітні фізичні носії: мідні або оптичні кабелі, бездротові технології, електричні сигнали або світлові імпульси. Саме цей рівень визначає тип використовуваних роз’ємів, особливості кодування даних, а також швидкість передачі. Типовими прикладами технологій фізичного рівня є Ethernet[7], Wi-Fi, DSL і оптоволоконні інтерфейси, що часто зустрічаються у корпоративних мережах.

Мережевий рівень відповідає за логічну адресацію пристроїв у мережі та організацію маршрутизації пакетів. Ключовим протоколом цього рівня є IP (Internet Protocol), який формує унікальні IP-адреси для кожного пристрою та керує доставкою пакетів від джерела до отримувача, навіть якщо вони знаходяться у різних фізичних або логічних сегментах мережі. Додатково на цьому рівні функціонують такі протоколи, як ICMP (використовується для передачі повідомлень про помилки та діагностики), ARP (відповідає за визначення фізичних MAC-адрес у локальних мережах) і IGMP (застосовується для організації групових багатоадресних розсилок, що важливо для мультимедійних сервісів).

Транспортний рівень дозволяє забезпечити надійність передачі та контроль якості зв’язку між програмними застосунками на різних пристроях. Він визначає способи сегментації даних, їх повторної збірки та обробки втрат або помилок під час передачі. Найпоширенішими протоколами є TCP (Transmission Control Protocol), що гарантує встановлення з’єднання, контроль послідовності, повторну передачу втрачених пакетів і контроль потоку, та UDP (User Datagram Protocol), який забезпечує мінімальну затримку і використовується там, де критичні швидкість і низькі накладні витрати – наприклад, у VoIP чи потоковому відео.

Прикладний рівень охоплює велику кількість протоколів, які реалізують різні сервіси для кінцевого користувача. Це протоколи для організації веб-доступу (HTTP/HTTPS), передачі файлів (FTP, SFTP), електронної пошти (SMTP, POP3, IMAP), доменних імен (DNS), автоматичної конфігурації мережі (DHCP)[8], а також протоколи моніторингу та управління мережевим обладнанням (SNMP)[9]. Окрему увагу в корпоративному середовищі, особливо для фінансових і страхових компаній, приділяють питанням безпеки: для шифрування трафіку використовують SSL/TLS, для побудови захищених VPN – IPSec, а протоколи аутентифікації забезпечують контроль доступу до внутрішніх ресурсів. Завдяки такому підходу, стек TCP/IP дозволяє створювати гнучкі,

масштабовані та захищені мережі, що відповідають сучасним вимогам бізнесу.

Рисунок 1.3 – Стек протоколів TCP/IP. Чотирирівнева архітектура мережевих протоколів

Таким чином, TCP/IP-стек виступає фундаментом для надійної, масштабованої й захищеної мережевої взаємодії в будь-якому сучасному корпоративному або глобальному середовищі

1.5 Технологія Ethernet та принципи функціонування та застосування

Технологія Ethernet є основою сучасних локальних комп'ютерних мереж, і її популярність пояснюється простотою впровадження, надійністю, економічною ефективністю та гнучкістю масштабування під потреби бізнесу.

Ethernet виник у 1970-х роках і з тих пір пройшов значний шлях еволюції – від перших реалізацій на коаксіальному кабелі з швидкістю передачі 10 Мбіт/с до сучасних високошвидкісних рішень, які дозволяють передавати дані зі швидкістю понад 100 Гбіт/с. Принцип роботи Ethernet (рисунок 1.4) заснований на методі доступу до середовища передачі CSMA/CD, який дозволяє кільком пристроям використовувати одне й те саме середовище для обміну даними, визначаючи моменти, коли канал зайнятий, та уникаючи колізій. З появою комутованих мереж Ethernet (switching Ethernet) колізії стали практично неможливими, адже кожен пристрій отримав виділений канал до комутатора, що забезпечило повнодуплексний режим роботи й суттєве зростання пропускної здатності.

Ethernet стандартизується (рисунок 1.4) організацією IEEE у рамках специфікацій серії 802.3, які регламентують технічні параметри, типи кабелів, протоколи фізичного і канального рівнів. До основних сучасних стандартів належать Fast Ethernet (100 Мбіт/с), Gigabit Ethernet (1 Гбіт/с), 10 Gigabit Ethernet і стандарти для ще вищих швидкостей. Для різних завдань і сегментів мережі використовуються різні фізичні середовища передачі даних: виту пару (UTP, STP) найчастіше застосовують у корпоративних мережах через низьку вартість і простоту монтажу, а оптоволоконні кабелі використовують для магістральних ліній, де потрібна висока швидкість і велика довжина сегмента. У старих чи спеціалізованих системах ще можна зустріти коаксіальні кабелі.

Мережеві інтерфейси в Ethernet ідентифікуються за унікальними 48-бітовими MAC-адресами, що дозволяє чітко визначати джерело і призначення кадру в межах однієї локальної мережі. Підтримуються три типи адресації: одноадресна (unicast), багатоадресна (multicast) і широкомовна (broadcast). У корпоративних мережах все більшого значення набувають технології VLAN, які дозволяють логічно розділяти мережу на ізольовані сегменти незалежно від фізичної топології, підвищуючи безпеку й керованість трафіком. Важливою можливістю є також агрегація каналів (Link

Aggregation), яка забезпечує підвищення пропускної здатності й відмовостійкості магістральних з'єднань.

Сучасні тенденції розвитку Ethernet охоплюють впровадження технологій Power over Ethernet (PoE), які дозволяють одночасно передавати дані й електроживлення по одному кабелю, що особливо актуально для підключення IP-камер, точок доступу, VoIP-телефонів. Збільшення швидкості, зменшення затримок, підтримка центрів обробки даних та інтеграція з рішеннями програмно-конфігурованих мереж (SDN) відкривають нові можливості для побудови гнучких, масштабованих і захищених мережевих інфраструктур.

СТАНДАРТ	МАКСИМАЛЬНА ШВИДКІСТЬ	ТИП КАБЕЛЮ	МАКСИМАЛЬНА ДОВЖИНА СЕГМЕНТА	ТОПОЛОГІЯ	ОСНОВНЕ ЗАСТОСУВАННЯ
10BASE-T	10 Мбіт/с	Вита пара (Cat 3)	100 м	Зірка	*Старі офісні мережі*
100BASE-TX	100 Мбіт/с	Вита пара (Cat 5)	100 м	Зірка	*Офісні локальні мережі*
1000BASE-T	1 Гбіт/с	Вита пара (Cat 5e/6)	100 м	Зірка	*Сучасні офіси, дата-центри*
1000BASE-SX/LX	1 Гбіт/с	Оптоволокно	до 550 м / до 5 км	Зірка	*Магістральні та міжбудівельні канали*
10GBASE-T	10 Гбіт/с	Вита пара (Cat 6a)	100 м	Зірка	*Центри обробки даних, серверні ферми*
10GBASE-SR/LR	10 Гбіт/с	Оптоволокно	до 300 м / до 10 км	Зірка	*Високошвидкісні канали*
100GBASE-SR4/LR4	100 Гбіт/с	Оптоволокно	до 100 м / до 10 км	Зірка	*Дата-центри, суперкомп'ютерні мережі*

Рисунок 1.4 - Стандарти Ethernet. Технічні характеристики мережевих технологій

2 АРХІТЕКТУРА ТА ТЕХНОЛОГІЇ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

2.1 Фундаментальні принципи побудови VPN-інфраструктури

Віртуальні приватні мережі (VPN)[10] є одним із ключових інструментів захисту інформаційних ресурсів організації та забезпечення безпечної комунікації між її структурними підрозділами. Основна мета створення VPN полягає у формуванні захищеного віртуального каналу поверх відкритої або незахищеної мережі, наприклад Інтернету, що дозволяє передавати корпоративні дані із дотриманням вимог конфіденційності, цілісності та доступності.

VPN-інфраструктура ізолює трафік організації від сторонніх користувачів, забезпечуючи прозорий доступ до ресурсів, незалежно від фізичного розташування користувачів чи філій. Це досягається шляхом створення зашифрованих тунелів, у яких інформація інкапсулюється та передається в зашифрованому вигляді між вузлами мережі. Таким чином, навіть якщо трафік перехоплений у публічному середовищі, сторонній спостерігач не може прочитати чи модифікувати дані.

Базові моделі побудови VPN-інфраструктур включають кілька основних варіантів, серед яких найбільш поширені моделі «клієнт-сервер», «site-to-site» (міжсайтовий VPN) та хмарні VPN-рішення. У моделі клієнт-сервер віддалений користувач (клієнт) підключається до корпоративної мережі через спеціалізований VPN-сервер, отримуючи таким чином доступ до внутрішніх ресурсів компанії так, ніби він перебуває у локальній мережі. Цей підхід широко використовується для організації безпечної віддаленої роботи співробітників.

У моделі site-to-site організовується захищений тунель між двома або більше офісами компанії, які можуть знаходитись у різних містах чи країнах. Таке рішення дозволяє інтегрувати розподілені підрозділи в єдину

корпоративну мережу, підтримуючи прозору маршрутизацію внутрішнього трафіку, централізоване адміністрування та спрощену політику безпеки. У цьому випадку всі пристрої у філіях сприймають мережу як єдиний логічний простір, що підвищує зручність спільної роботи та обміну інформацією.

З появою хмарних технологій все більшої популярності набувають хмарні VPN-рішення. У такій архітектурі шифрування та управління VPN-з'єднаннями здійснюється у хмарному середовищі, а кінцеві точки можуть підключатись як до власних дата-центрів компанії, так і до хмарних ресурсів (наприклад, AWS, Azure, Google Cloud). Це дозволяє швидко масштабувати інфраструктуру, підвищити гнучкість, а також знизити витрати на підтримку фізичного обладнання.

Незалежно від обраної моделі, фундаментальними принципами побудови VPN-інфраструктури є:

- ізоляція трафіку — розмежування мережевих потоків, що запобігає несанкціонованому доступу до інформації;
- інкапсуляція даних — обгортання інформаційних пакетів у додаткові протокольні оболонки для транспортування;
- шифрування — перетворення даних у нечитабельну форму, захищаючи їх від перехоплення;
- автентифікація — перевірка справжності учасників з'єднання;
- контроль цілісності — забезпечення, що дані не були змінені під час передачі;
- масштабованість — можливість розширення мережі без втрати рівня безпеки та продуктивності.

Вибір конкретної архітектури та протоколів VPN здійснюється з урахуванням корпоративних політик безпеки, вимог до продуктивності, типу підключень (статичних чи динамічних), необхідності резервування та інтеграції з існуючими системами автентифікації.

У підсумку, грамотне проєктування VPN-інфраструктури дозволяє не лише захистити корпоративну інформацію, а й значно підвищити

мобільність, гнучкість та ефективність роботи сучасних організацій.

2.2 Таксономія VPN-технологій за критеріями застосування

Сучасний ринок віртуальних приватних мереж представлений широким спектром технологій, які розрізняються за цілями використання, архітектурними особливостями, підтримуваними протоколами та рівнем безпеки. Таксономія VPN-технологій дозволяє структурувати підходи до побудови захищених мереж і обрати оптимальне рішення для конкретного сценарію застосування.

За критерієм призначення VPN-технології поділяються на дві основні категорії: VPN для віддаленого доступу (Remote Access VPN) та мережеві VPN для з’єднання офісів (Site-to-site VPN). Перша група орієнтована на підключення окремих користувачів чи пристроїв до корпоративної мережі через захищений канал з будь-якого місця — найчастіше використовується для організації віддаленої роботи співробітників. Друга — для побудови єдиної мережі між відокремленими офісами, дата-центрами чи підрозділами, забезпечуючи прозорий і безпечний обмін даними.

Важливим є критерій мережевого рівня, на якому працює VPN-рішення. Залежно від цього технології поділяються на:

- мережевий рівень (Network Layer VPN) — працює на рівні IP (наприклад, IPSec), дозволяє прозоро тунелювати будь-який IP-трафік;
- транспортний рівень (Transport Layer VPN) — організовує захист на рівні TCP/UDP сесій (наприклад, SSL VPN, TLS VPN), дозволяючи шифрувати окремі сервіси, як-от доступ до веб-ресурсів чи віддалених робочих столів;
- канальний рівень (Data Link Layer VPN) — забезпечує захист протоколів нижчих рівнів, наприклад, через PPP, PPTP, L2TP.

За типом інфраструктури VPN бувають корпоративні (enterprise), екстранет-VPN (об'єднання з партнерами чи замовниками), мобільні VPN

(для забезпечення захисту даних у мобільних пристроях) і хмарні (cloud VPN). Останні дозволяють інтегрувати різноманітні фізичні, віртуальні й хмарні ресурси організації у спільний захищений простір.

З точки зору технологій (рисунок 2.2) та протоколів (рисунок 2.1), найпоширенішими є такі рішення:

- PPTP (Point-to-Point Tunneling Protocol)[11,12] — історично один із перших VPN-протоколів, простий у налаштуванні, але має низький рівень безпеки й практично не використовується у сучасних корпоративних мережах.

- L2TP/IPSec (Layer 2 Tunneling Protocol з IPSec) — поєднує функції інкапсуляції та шифрування, підходить для організації тунелювання через незахищені мережі з високим рівнем захисту.

- IPSec (Internet Protocol Security) — стандарт корпоративного захисту на мережевому рівні, забезпечує шифрування, автентифікацію, контроль цілісності даних. Підтримується майже всіма виробниками мережевого обладнання.

- SSL VPN (Secure Sockets Layer VPN) — функціонує на транспортному рівні, зручно інтегрується з браузерами та забезпечує захист віддаленого доступу до корпоративних веб-додатків без складної клієнтської частини.

- OpenVPN — відкритий програмний комплекс із високою гнучкістю та підтримкою різних методів шифрування й автентифікації, використовується як для віддаленого доступу, так і для з’єднання офісів.

- MPLS VPN (Multiprotocol Label Switching VPN) — рішення для великих корпоративних мереж, що надається телекомунікаційними операторами і дозволяє будувати віртуальні мережі на основі технології MPLS.

Варто зазначити, що вибір конкретної VPN-технології залежить від багатьох факторів:

- масштабу організації (малий бізнес, середнє підприємство, велика корпорація);
- типу захищуваного трафіку (веб, файлові сервіси, VoIP, відеоконференції тощо);
- вимог до мобільності співробітників;
- рівня очікуваної безпеки;
- наявності власної або орендованої IT-інфраструктури.

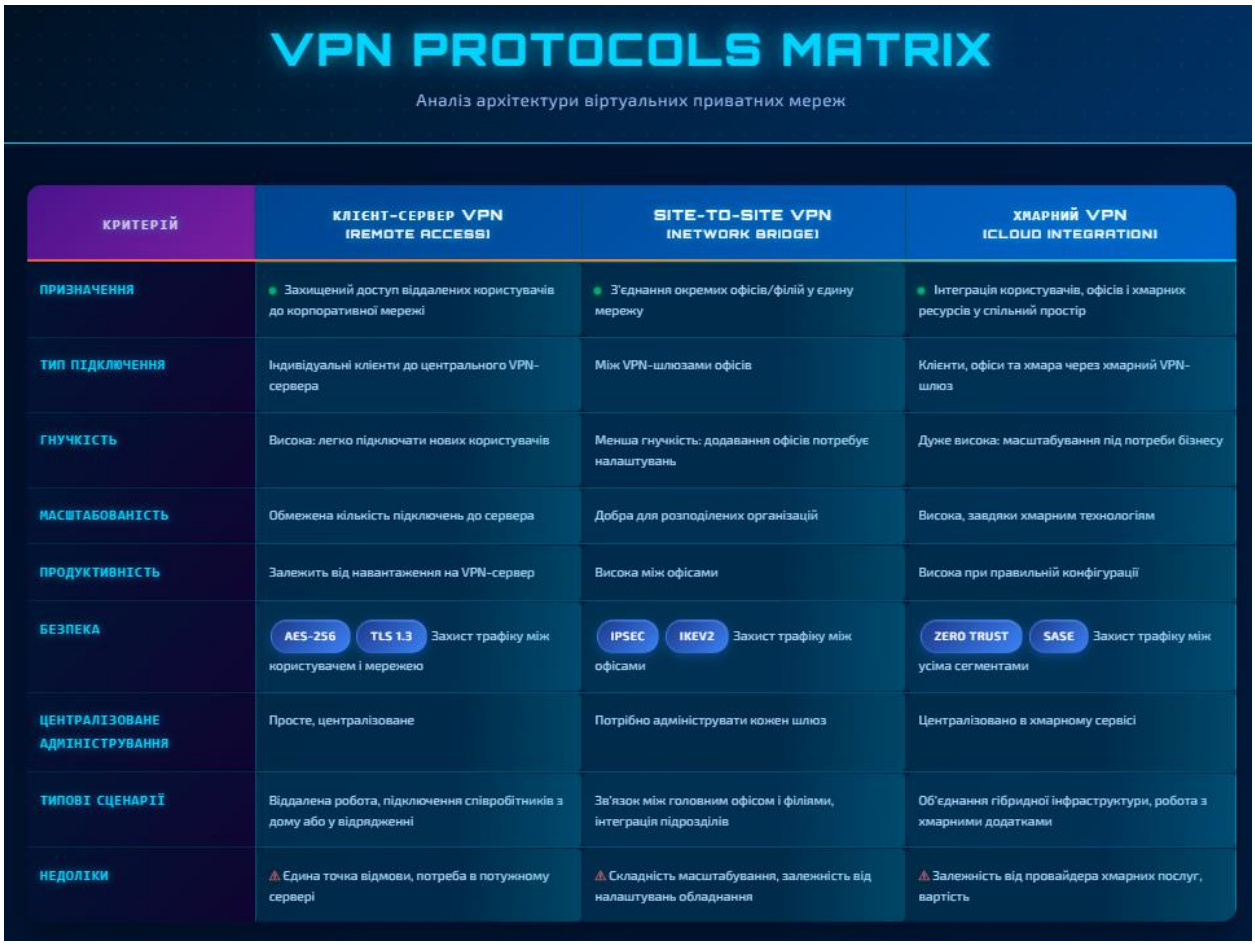


Рисунок 2.1 – Коротка характеристика найпоширеніших VPN-технологій

Сучасні організації нерідко використовують комбінації декількох VPN-технологій для досягнення оптимального балансу між безпекою, продуктивністю та зручністю адміністрування.

Рисунок 2.2 – Порівняльна діаграма VPN-технологій

Графічна візуалізація у вигляді "радарної" діаграми (Spider chart) дозволяє порівняти основні типи VPN-технологій за такими ключовими параметрами, як простота налаштування, рівень безпеки, швидкість роботи, гнучкість використання, масштабованість та надійність. Кожна технологія має свої сильні і слабкі сторони.

PPTP відрізняється максимальною простотою впровадження, але поступається іншим протоколам за рівнем безпеки. L2TP з IPSec забезпечує високий рівень захисту, однак вимагає складніших налаштувань. Протокол IPSec вважається промисловим стандартом для корпоративних мереж: він надає дуже високий рівень безпеки та хорошу швидкість роботи, але його розгортання є досить складним. Протоколи SSL VPN та OpenVPN відзначаються універсальністю та гнучкістю, забезпечуючи оптимальний баланс між простотою, безпекою і швидкістю. Для великих корпоративних структур використовується MPLS VPN — ця технологія забезпечує найвищий рівень надійності та масштабованості, але її впровадження є найбільш складним і дорогим серед усіх перерахованих рішень.

2.3 Механізми тунелювання та інкапсуляції даних

Механізми тунелювання та інкапсуляції даних є наріжним каменем побудови сучасних VPN-інфраструктур. Саме завдяки цим механізмам стає можливою передача корпоративних даних через відкриті, потенційно небезпечні мережі — зокрема, через Інтернет — у захищеному та надійному форматі. Суть тунелювання полягає у створенні віртуального каналу, який поєднує віддалені мережеві вузли або цілі підмережі та дозволяє передавати дані, ніби вони знаходяться у межах однієї локальної мережі. Інкапсуляція, в свою чергу, передбачає "обгортання" оригінальних даних додатковими заголовками протоколів, що забезпечує як коректну маршрутизацію у глобальній мережі, так і захист від несанкціонованого доступу або модифікації.

Процес побудови VPN-тунелю (рисунок 2.3) базується на принципі інкапсуляції даних, коли початкові пакети, сформовані у відправника, додатково пакуються у спеціальні тунельні протоколи. Це можуть бути як класичні протоколи нижнього рівня, наприклад, GRE (Generic Routing Encapsulation), так і більш сучасні рішення на основі L2TP, IPSec або SSL/TLS. Усі ці протоколи створюють додатковий захисний "шар" навколо даних, що транспортуються через загальнодоступну мережу. На практиці це означає, що під час передачі по Інтернету або іншій зовнішній мережі внутрішній вміст пакета недоступний для сторонніх, оскільки він захищений механізмами шифрування та автентифікації.

Різноманіття VPN-технологій дозволяє будувати тунелі між окремими комп’ютерами (віддалений доступ), між офісами чи дата-центрами (site-to-site), а також створювати гібридні інфраструктури для роботи з хмарними платформами. Усі ці рішення мають спільну ознаку — завдяки механізмам тунелювання та інкапсуляції корпоративний трафік ізольований від зовнішнього впливу, а дані не можуть бути прочитані або змінені у процесі пересилання. Зазвичай, після інкапсуляції на стороні відправника, дані

шифруються, потім транспортуються до вузла призначення, де тунель розшифровується та інкапсульований пакет розпаковується, після чого початковий трафік надходить до адресата у первинному вигляді.

Завдяки цим технологіям компанії можуть використовувати Інтернет для об'єднання своїх підрозділів і віддалених співробітників у єдиний корпоративний простір, не ризикуючи безпекою власних інформаційних ресурсів. Інкапсуляція також дозволяє транспортувати пакети одного протоколу всередині іншого, наприклад, передавати IP-пакети поверх UDP чи TCP у випадку з OpenVPN, або Ethernet-кадри у L2TP. Це робить VPN-інфраструктуру універсальною, сумісною із різними типами мереж і протоколів.

Особливо важливо, що тунелювання та інкапсуляція, крім захисту даних, забезпечують ще й цілісність і автентичність трафіку. Використання сучасних алгоритмів хешування та цифрових підписів гарантує, що інформація, передана через тунель, не була змінена в дорозі й дійсно походить від авторизованого відправника. Це критично для корпоративних мереж, у яких захист від атак типу "людина посередині" (Man-in-the-Middle) та від спроб підміни трафіку є пріоритетом.

Використання тунелювання і інкапсуляції стало стандартом для корпоративних VPN-рішень і забезпечило можливість гнучкого масштабування мережевої інфраструктури під сучасні вимоги. Такі підходи дозволяють не лише безпечно передавати дані між різними сегментами мережі, але й організовувати прозору маршрутизацію, сумісність із різними протоколами, а також оптимізувати витрати на побудову та обслуговування захищених каналів зв’язку. У підсумку, тунелювання та інкапсуляція є базовими механізмами, без яких не можна уявити ефективну й надійну роботу корпоративних VPN у сучасних умовах розвитку інформаційних технологій.

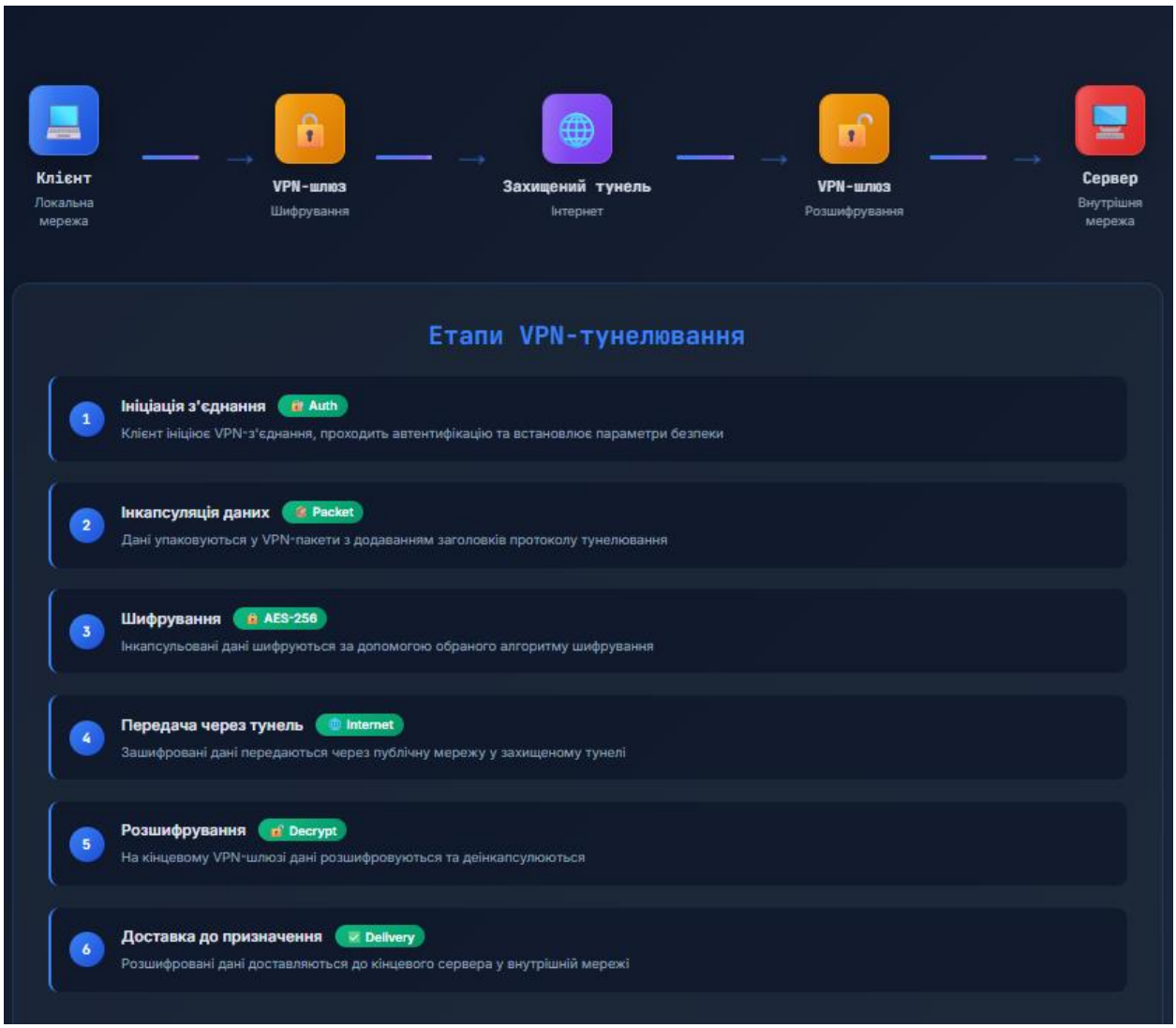


Рисунок 2.3 – Типова схема VPN-тунелювання

2.4 Алгоритми шифрування та автентифікації у VPN-системах

Сучасні VPN-системи забезпечують конфіденційність, цілісність і автентичність даних передусім за рахунок впровадження криптографічних алгоритмів шифрування й механізмів автентифікації. Захист інформації, яка передається по публічних чи незахищених каналах зв’язку, є одним із фундаментальних завдань корпоративних мереж, і саме тому вибір відповідних алгоритмів та методів ідентифікації користувачів відіграє ключову роль у проєктуванні VPN-інфраструктур.

Шифрування у VPN відбувається за допомогою симетричних і асиметричних криптоалгоритмів. Симетричні алгоритми (наприклад, AES,

3DES, Blowfish, RC4) використовують один і той самий секретний ключ для шифрування й дешифрування даних, що забезпечує високу швидкість обробки інформації та ефективність у випадках великого трафіку. Особливо широке застосування в сучасних VPN знайшов алгоритм AES (Advanced Encryption Standard), який має оптимальне співвідношення між рівнем безпеки, продуктивністю та гнучкістю вибору довжини ключа. Для застарілих систем може зустрічатися DES, проте його використання поступово зводиться нанівець через відносно низький рівень захисту.

Асиметричне шифрування (RSA, Diffie-Hellman, ECC) ґрунтується на використанні пари ключів — відкритого та закритого. Цей підхід зазвичай застосовується на етапі встановлення VPN-з’єднання для обміну ключами, автентифікації сторін та формування спільного секрету для подальшого симетричного шифрування сесії. Найбільш поширеним протоколом обміну ключами є алгоритм Диффі-Геллмана (DH), що дозволяє двом сторонам безпечно узгодити загальний секрет навіть через незахищений канал. Для підпису й підтвердження автентичності часто використовується RSA, а для сучасних високопродуктивних систем — криптографія на еліптичних кривих (ECC).

Крім шифрування, VPN-системи впроваджують механізми автентифікації для підтвердження особи користувача або пристрою, який підключається до мережі. Найпростіший спосіб — це автентифікація за паролем або спільним ключем, однак у корпоративному середовищі дедалі частіше використовуються сертифікатні системи на основі PKI (Public Key Infrastructure), коли доступ до VPN отримують лише власники цифрових сертифікатів, виданих авторитетним центром сертифікації. Також застосовуються багатоетапні або багатофакторні підходи (наприклад, пароль + одноразовий код із токена чи SMS, апаратні ключі), які значно підвищують рівень захисту.

Для забезпечення цілісності й невід’ємності даних використовуються хеш-функції та алгоритми створення цифрових підписів (SHA-2, SHA-3,

HMAC, MD5), які дозволяють визначити, чи були дані змінені в процесі передачі. Хеш-контроль використовується як на етапі встановлення з’єднання, так і під час передавання кожного пакету даних у VPN-тунелі.

Таким чином, сучасні VPN-системи поєднують різні методи шифрування, обміну ключами, автентифікації та контролю цілісності для створення комплексного багаторівневого захисту даних. Поєднання симетричних і асиметричних алгоритмів дозволяє одночасно досягти високої продуктивності та максимального рівня безпеки, а впровадження сучасних багатофакторних методів автентифікації мінімізує ризик несанкціонованого доступу до корпоративної мережі. Завдяки цим механізмам VPN залишається одним із найнадійніших інструментів захисту інформації у сучасних розподілених і гібридних IT-інфраструктурах.

2.5 Технічна специфікація протоколу OpenVPN

OpenVPN є одним із найпопулярніших і найгнучкіших протоколів для організації віртуальних приватних мереж у сучасних корпоративних інфраструктурах. Його популярність обумовлена відкритим вихідним кодом, високим рівнем захисту, широкими можливостями конфігурації, а також підтримкою різноманітних операційних систем і апаратних платформ. OpenVPN забезпечує створення зашифрованих тунелів поверх TCP або UDP, дозволяючи захищено передавати дані між віддаленими користувачами, філіями, дата-центрами та хмарними ресурсами через незахищене середовище, таке як Інтернет.

Технічна архітектура OpenVPN ґрунтується на клієнт-серверній моделі, де спеціальний OpenVPN-сервер приймає підключення від одного або декількох клієнтів. Для передачі даних OpenVPN може інкапсулювати IP-трафік у SSL/TLS тунелі, що забезпечує захист від прослуховування та модифікації інформації. В основі механізмів безпеки протоколу лежить використання SSL/TLS для аутентифікації і обміну ключами, а також

сучасних алгоритмів шифрування (AES, Blowfish, Camellia тощо) для захисту інформації під час передачі.

OpenVPN підтримує автентифікацію користувачів за допомогою імені й пароля, статичних або динамічних ключів, X.509-сертифікатів, а також багатофакторні методи автентифікації з інтеграцією зовнішніх систем (наприклад, LDAP, RADIUS, PAM). Для підвищення рівня безпеки в OpenVPN впроваджено механізми Perfect Forward Secrecy (PFS), які забезпечують, що компрометація одного сеансового ключа не призведе до розкриття всього зашифрованого трафіку.

Важливою особливістю OpenVPN є можливість використання як точка-точка (P2P), так і багатокористувацьких (multiclient) конфігурацій, що дозволяє створювати як класичні тунелі між двома вузлами, так і масштабовані VPN-сервіси для великої кількості клієнтів. Завдяки підтримці віртуальних мережевих інтерфейсів (TUN/TAP), OpenVPN може працювати як у режимі маршрутизації IP-пакетів, так і у режимі передачі Ethernet-кадрів, що забезпечує гнучкість у налаштуванні корпоративної мережевої інфраструктури.

OpenVPN відзначається високою продуктивністю і стабільністю роботи. Він ефективно справляється з NAT, підтримує динамічну маршрутизацію, розподілення навантаження, балансування каналів, а також автоматичне перепідключення клієнтів у разі тимчасових збоїв з’єднання. Протокол має розвинуті інструменти логування й моніторингу, що дозволяє адміністраторам оперативно відстежувати стан мережі та забезпечувати відповідність корпоративним політикам безпеки.

OpenVPN легко інтегрується у хмарні та гібридні IT-інфраструктури, підтримує масштабування, використання кластерів серверів і побудову складних сценаріїв доступу для різних категорій користувачів. Відкрита архітектура протоколу і велика спільнота розробників забезпечують постійну підтримку та оновлення функціоналу, що робить OpenVPN надійним вибором для організацій будь-якого розміру.

У результаті, OpenVPN поєднує у собі простоту налаштування, високу гнучкість, безпечну архітектуру й широкі можливості масштабування, забезпечуючи захищений доступ до корпоративних ресурсів незалежно від фізичного розташування користувачів чи підрозділів компанії. Саме завдяки цим властивостям OpenVPN є провідним рішенням для створення сучасних VPN у приватному, корпоративному та хмарному середовищі.

3 ОПИС ОБ’ЄКТА ВПРОВАДЖЕННЯ

3.1 Характеристика і структура об’єкта впровадження

Об’єктом впровадження є сучасна корпоративна комп’ютерна мережа страхової компанії «ТОВ ВУСО ГРУП», що функціонує як ключова ланка підтримки всіх бізнес-процесів організації. Компанія відрізняється складною організаційною структурою: до її складу входить центральний офіс, де розміщується керівництво та основні сервісні потужності, а також широка мережа регіональних представництв і філій, розташованих у різних містах країни. Така розподіленість вимагає від інформаційної інфраструктури високої гнучкості, стійкості до збоїв і здатності до швидкого масштабування відповідно до динамічних потреб бізнесу.

Визначальною особливістю об’єкта є побудова територіально-розподіленої мережі, яка поєднує всі офіси й підрозділи в єдиний інформаційний простір. Це дозволяє забезпечити прозорий і захищений обмін даними між центральним офісом і регіональними філіями, централізоване управління мережевими ресурсами та оперативний доступ співробітників до корпоративних сервісів незалежно від їхнього місцезнаходження. Таке рішення формує фундамент для впровадження єдиних політик інформаційної безпеки та забезпечення стабільної роботи критично важливих сервісів у будь-який час.

До складу інформаційної інфраструктури компанії входять сервери різного призначення (файлові, додаткові сервісні, сервери віддаленого доступу), мережеві пристрої (маршрутизатори, комутатори, міжмережеві екрани — firewall, системи виявлення та запобігання вторгненням — IPS), а також патч-панелі, які дозволяють організовувати гнучку систему підключень у серверних кімнатах. На робочих місцях співробітників використовуються сучасні клієнтські пристрої — комп’ютери, ноутбуки,

термінали, що мають можливість захищеного підключення до корпоративної мережі.

Усі компоненти інфраструктури взаємодіють між собою відповідно до заздалегідь визначеної архітектури й топології, що передбачає багаторівневу систему резервування, балансування навантаження та централізоване адміністрування. Комплекс технічних і програмних засобів, реалізований у компанії, спрямований на підвищення надійності роботи, швидке виявлення й усунення можливих несправностей, а також дотримання сучасних стандартів захисту інформації.

Таким чином, корпоративна мережа «ТОВ ВУСО ГРУП» є не лише каналом для передачі даних, а й цілісною системою, що забезпечує надійну роботу всіх бізнес-підрозділів, підтримує цифрову трансформацію компанії та слугує фундаментом для подальшого розвитку її інформаційних сервісів.

3.2 Завдання і мета роботи, що виконується

Головною метою впровадження проєкту є створення сучасної, високонадійної та масштабованої корпоративної комп’ютерної мережі страхової компанії «ТОВ ВУСО ГРУП». Запропонована мережа повинна забезпечити ефективний і безперебійний обмін даними між центральним офісом та всіма регіональними підрозділами, підтримувати централізований доступ до критично важливих бізнес-ресурсів, а також гарантувати високий рівень інформаційної безпеки для всіх користувачів і служб компанії.

До ключових завдань проєкту належить комплексна розробка архітектури мережі з урахуванням розгалуженої структури компанії та її територіальної розподіленості. Особлива увага приділяється впровадженню сучасних механізмів резервування і відмовостійкості для основних мережевих компонентів, що дозволить мінімізувати ризики простоїв і втрати даних у разі технічних збоїв або кібератак. Передбачено оптимізацію роботи серверної інфраструктури — налаштування й масштабування RDP-сервера

для організації віддаленого доступу, розгортання файлового сервера для централізованого зберігання і обміну корпоративною інформацією.

Важливим аспектом є впровадження багаторівневої системи захисту корпоративної мережі. Це включає встановлення міжмережевого екрану (firewall) для контролю зовнішнього та внутрішнього трафіку, використання систем виявлення і запобігання вторгненням (IPS) для моніторингу підозрілої активності та своєчасного реагування на спроби несанкціонованого доступу. Крім того, проєктом передбачено впровадження зручних і безпечних механізмів адміністрування мережі — централізований моніторинг, аудит дій користувачів і адміністраторів, розмежування прав доступу відповідно до політик інформаційної безпеки компанії.

Завдяки реалізації цих завдань нова корпоративна мережа дозволить «ТОВ ВУСО ГРУП» підвищити продуктивність бізнес-процесів, забезпечити надійний захист від внутрішніх і зовнішніх загроз, а також створити гнучку платформу для подальшого розвитку та впровадження сучасних цифрових сервісів і технологій.

3.3 Архітектура та топологія мережі

Корпоративна мережа «ТОВ ВУСО ГРУП» спроєктована на основі ієрархічної багаторівневої архітектури, що об'єднує структурні переваги топологій зірки та дерева. Такий підхід дозволяє досягти високого рівня масштабованості, централізованого управління, гнучкості та резервування ключових ресурсів. У центрі мережі знаходиться ядро (core layer), розташоване у головному офісі компанії, яке забезпечує взаємодію між основними сервісами та захищений вихід до глобальної мережі Інтернет.

Ядро мережі об'єднує ключові сервери компанії — файловий сервер, RDP-сервер для організації віддаленого доступу, а також вузли засобів інформаційної безпеки, включаючи міжмережевий екран (firewall) і системи виявлення та запобігання вторгненням (IPS). Центральний маршрутизатор

виконує роль основного шлюзу, контролюючи маршрутизацію внутрішнього й зовнішнього трафіку та забезпечуючи сегментування мережі для розмежування доступу й підвищення захищеності.

Взаємодія між структурними підрозділами та центральним офісом реалізується через захищені VPN-канали, що дозволяє надійно передавати дані незалежно від фізичного розташування користувачів чи філій. Кожен регіональний офіс оснащений локальним маршрутизатором та комутатором доступу, які під'єднані до корпоративної мережі за допомогою VPN-тунелю. Це забезпечує цілісність і конфіденційність інформаційних потоків та виключає можливість перехоплення критичних даних у зовнішньому середовищі.

В основі фізичної інфраструктури лежать сучасні комутатори та патч-панелі, що забезпечують ефективне адміністрування, просте масштабування та оперативне підключення нових пристроїв у разі зростання компанії. Таке рішення дозволяє швидко нарощувати кількість робочих місць, організовувати окремі сегменти для різних служб або тимчасових проєктних груп без значних перебудов фізичної топології.

Для забезпечення відмовостійкості та балансування навантаження у мережі впроваджено кілька IPS-систем, розташованих на різних рівнях архітектури. Вони виконують функції активного моніторингу, аналізу та блокування підозрілих дій, що дозволяє ефективно реагувати на зовнішні та внутрішні загрози, запобігати атакам і зберігати безперервність бізнес-процесів.

Таким чином, побудована архітектура корпоративної мережі не лише гарантує надійність та захищеність інформаційного простору компанії, а й створює гнучку платформу для подальшого розширення та впровадження сучасних цифрових сервісів у масштабах всієї організації.

3.4 Модель OSI для “ТОВ ВУСО ГРУП”

Функціонування корпоративної мережі страхової компанії «ТОВ ВУСО ГРУП» організовано з урахуванням суворого дотримання багаторівневої еталонної моделі OSI (рисунок 3.1), що дозволяє забезпечити ефективну, захищену та керовану інформаційну інфраструктуру.

На фізичному рівні мережі використовуються сучасні структуровані кабельні системи, патч-панелі, маршрутизатори, комутатори, сервери та робочі станції співробітників. Саме тут здійснюється передача електричних або оптичних сигналів, що забезпечують фізичне з’єднання всіх елементів мережі у центральному офісі та регіональних підрозділах.

Канальний рівень відповідає за надійну доставку даних у межах одного сегменту, виявлення та виправлення помилок на фізичному носії, а також за логічне розмежування доступу. У корпоративній мережі це реалізовано через функціонал комутаторів, організацію VLAN для відділення трафіку різних служб і підвищення рівня безпеки за рахунок ізоляції підрозділів компанії.

На мережевому рівні відбувається маршрутизація даних між окремими сегментами мережі, реалізована за допомогою маршрутизаторів, які підтримують динамічні протоколи маршрутизації та політики контролю доступу. Саме тут здійснюється підключення корпоративної мережі до Інтернету через захищений шлюз (firewall) із додатковими модулями IPS для виявлення та блокування потенційних атак.

Транспортний рівень гарантує цілісність та надійність доставки даних між окремими сервісами мережі. У структурі «ТОВ ВУСО ГРУП» широко використовуються стандартні транспортні протоколи TCP і UDP для обслуговування таких сервісів, як RDP (віддалений доступ), файловий сервер, корпоративна пошта та інші бізнес-додатки.

На сеансовому рівні підтримується встановлення, керування та завершення стійких сеансів зв’язку між клієнтськими пристроями та серверними службами. Це важливо для гарантії безперервності роботи

користувачів із критичними сервісами компанії, зокрема під час віддаленої роботи через VPN.

Рівень представлення виконує функції шифрування й кодування даних, перетворення інформації у формат, зрозумілий різним програмам. Тут впроваджуються механізми захисту інформації — шифрування трафіку між вузлами, кодування переданих даних для сумісності між гетерогенними системами.

На прикладному рівні працюють основні бізнес-сервіси й додатки: сервери віддаленого доступу (RDP), файловий сервер, платформи для обміну документами, корпоративна електронна пошта, CRM-системи, а також усі користувацькі програми, що мають вихід у мережу. Саме тут формується і обробляється корпоративна інформація, яка потім проходить усі нижні рівні для надійної й захищеної доставки.

Завдяки такій багаторівневій архітектурі мережа «ТОВ ВУСО ГРУП» характеризується високою продуктивністю, централізованим адмініструванням, масштабованістю та відповідністю сучасним стандартам інформаційної безпеки, що дозволяє компанії ефективно реагувати на виклики ринку й підтримувати якісний рівень сервісу для своїх клієнтів.

Рисунок 3.1 – Модель OSI для “ТОВ ВУСО ГРУП”

4 ТЕХНІЧНЕ РІШЕННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

4.1 Проектування мережевої архітектури

Проектування мережевої архітектури є одним із ключових етапів створення ефективної, безпечної та масштабованої корпоративної мережі. На цьому етапі визначаються базові принципи організації інфраструктури, обирається тип архітектури, формується логічна та фізична топологія, а також підбирається необхідне мережеве обладнання з урахуванням поточних і перспективних потреб підприємства.

В основі сучасної корпоративної мережі лежить ієрархічна модель, яка складається з трьох основних рівнів: ядро мережі (core), рівень розподілу (distribution) та рівень доступу (access). Ядро мережі забезпечує високошвидкісну передачу даних між ключовими сегментами, обробку міжсегментного трафіку, а також підключення до зовнішніх ресурсів та Інтернету. На рівні розподілу впроваджуються політики безпеки, здійснюється агрегація трафіку від підрозділів і реалізується маршрутизація між VLAN або підмережами. Рівень доступу відповідає за підключення кінцевих пристроїв — робочих станцій, принтерів, IP-телефонів, забезпечує базову безпеку портів і контроль доступу користувачів.

В умовах розподіленої структури, яка характерна для “ТОВ ВУСО ГРУП”, особливу увагу приділяють організації надійних захищених VPN-каналів між центральним офісом та філіями. Це гарантує цілісність і конфіденційність корпоративного трафіку, дозволяє уніфікувати політики доступу та централізовано адмініструвати всю мережу незалежно від фізичного розташування підрозділів.

Ключовими складовими архітектури виступають сучасні маршрутизатори, які підтримують балансування навантаження та резервування каналів, багатофункціональні комутатори з підтримкою VLAN,

міжмережеві екрани для контролю трафіку, а також системи запобігання вторгненням (IPS), що забезпечують активний моніторинг та реагування на потенційні загрози. Для масштабованості та зручності адміністрування використовуються патч-панелі, які дозволяють швидко перепідключати обладнання, організовувати нові сегменти або робочі місця.

Важливою складовою проектування є побудова оптимальної схеми IP-адресації з резервуванням під майбутній ріст, впровадження VLAN-сегментації для ізоляції трафіку різних служб, а також планування механізмів резервування (кластеризація серверів, UPS для критичних вузлів, дублювання каналів). Рекомендується впроваджувати багаторівневу систему інформаційної безпеки — від автентифікації портів 802.1X до централізованого моніторингу через SIEM.

Проектування мережевої архітектури завершується тестуванням працездатності ключових сценаріїв, розробкою документації з політик доступу, планом розвитку та інструкціями для адміністраторів. Завдяки цьому компанія отримує надійну, безпечну та адаптивну інфраструктуру, яка готова до розширення та впровадження нових цифрових сервісів, гарантуючи стабільну підтримку всіх бізнес-процесів у довгостроковій перспективі.

4.2 Структурна схема корпоративної мережі

Корпоративна мережа «ТОВ ВУСО ГРУП» являє собою сучасну інфраструктуру з чітко вираженою централізованою архітектурою, яка об’єднує всі ключові інформаційні ресурси компанії в єдиний, керований і захищений простір. У центрі мережі знаходиться головний офіс, де розташовані критичні для бізнесу сервіси та обладнання: серверна інфраструктура включає RDP-сервер для організації віддаленої роботи співробітників, файловий сервер для централізованого зберігання корпоративних даних, а також мережеві пристрої ядра — центральний маршрутизатор, комутатор, патч-панель для організації структурованої

кабельної системи, багаторівневі системи безпеки, зокрема корпоративний міжмережевий екран (firewall) та систему запобігання вторгненням (IPS) другого рівня.

Від центрального офісу відгалужуються три регіональні підрозділи — офіси у Богодухові, Лозовій та Валках. Кожен віддалений офіс має стандартизовану структуру, що включає локальне мережеве обладнання, два робочі місця (персональні комп'ютери) та два мережевих принтери. Підключення до корпоративного центру здійснюється через захищені канали зв'язку із використанням системи запобігання вторгненням першого рівня (IPS 1), яка відповідає за захист периметру кожного офісу. Такий підхід дозволяє уніфікувати політику безпеки й забезпечити єдиний стандарт організації робочого простору для всіх віддалених точок.

Метою побудови мережі стало створення масштабованого й керованого інформаційного середовища, яке забезпечує централізоване управління всіма критичними сервісами та ресурсами компанії. Ключовими завданнями були впровадження зручного адміністрування, організація централізованого зберігання даних на файловому сервері центрального офісу, забезпечення безпечного доступу віддалених офісів за допомогою захищених каналів із використанням IPS, а також надання можливості співробітникам працювати з будь-якого підрозділу через RDP-сервер. Для контролю безпеки трафіку використовується багаторівневий захист: кожен віддалений офіс обладнаний власним IPS, у центральному офісі розташований другий рівень IPS, а корпоративний firewall здійснює загальний контроль доступу та фільтрацію мережевих потоків.

Архітектурно мережа (рисунок 4.1) побудована за зірковою топологією, у якій центральний офіс виступає ядром, а віддалені офіси підключені до нього як периферійні вузли. Це дозволяє гнучко масштабувати інфраструктуру, оперативно додавати нові віддалені підрозділи без необхідності суттєвого перегляду загальної структури. Вся мережа управляється з єдиної точки — центрального офісу, що істотно спрощує

адміністрування, підвищує рівень безпеки й дозволяє реалізувати централізований моніторинг та резервне копіювання даних.

Функціональні ролі елементів інфраструктури розподіляються відповідно до моделі OSI. У центральному офісі функціонують пристрої та сервіси, що охоплюють усі сім рівнів моделі: фізичний та канальний рівні забезпечують патч-панелі й комутатори, мережевий рівень — маршрутизатор для маршрутизації трафіку між сегментами та офісами, рівні від третього до сьомого реалізуються через firewall, IPS, а також сервери прикладних сервісів (файловий та RDP). Віддалені офіси зосереджують свою діяльність на рівнях від третього до сьомого — локальні IPS забезпечують безпеку та сегментацію, а клієнтські додатки на ПК працюють на прикладному рівні.

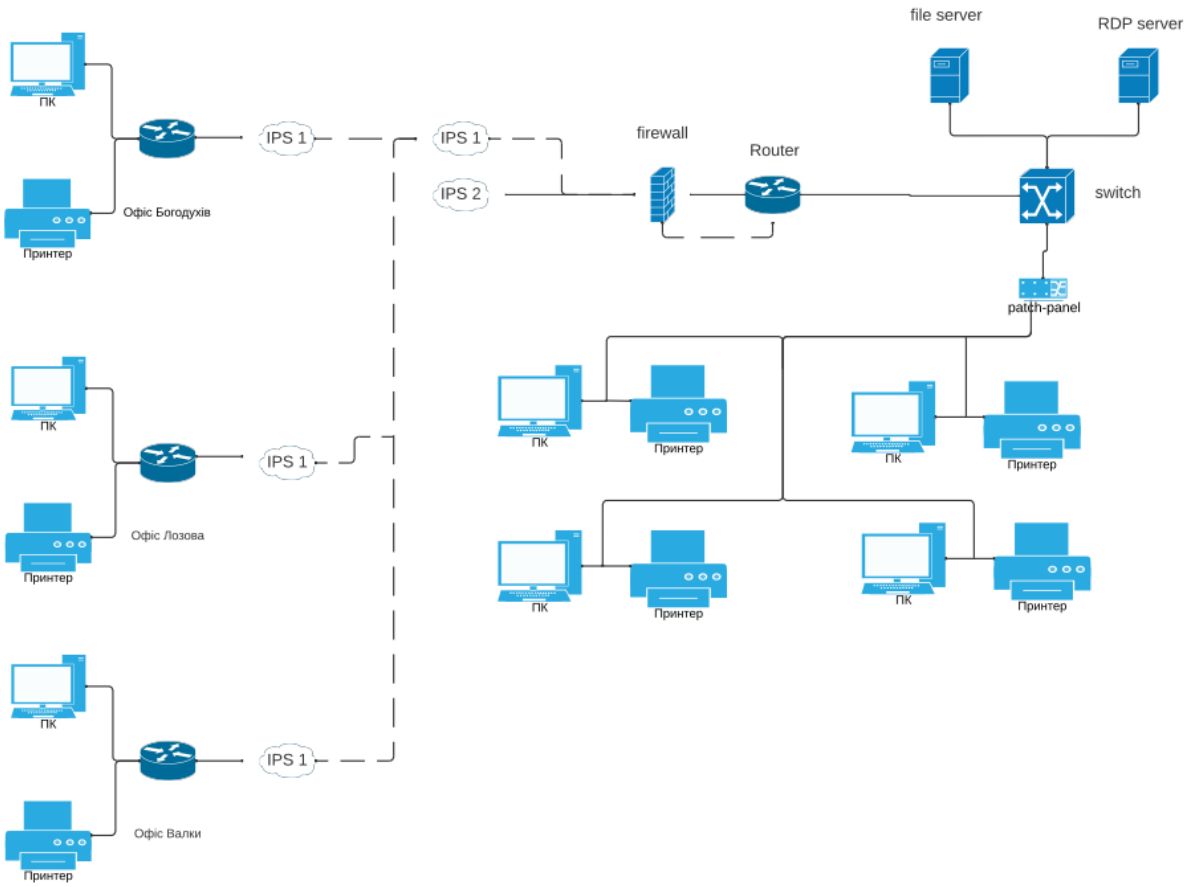


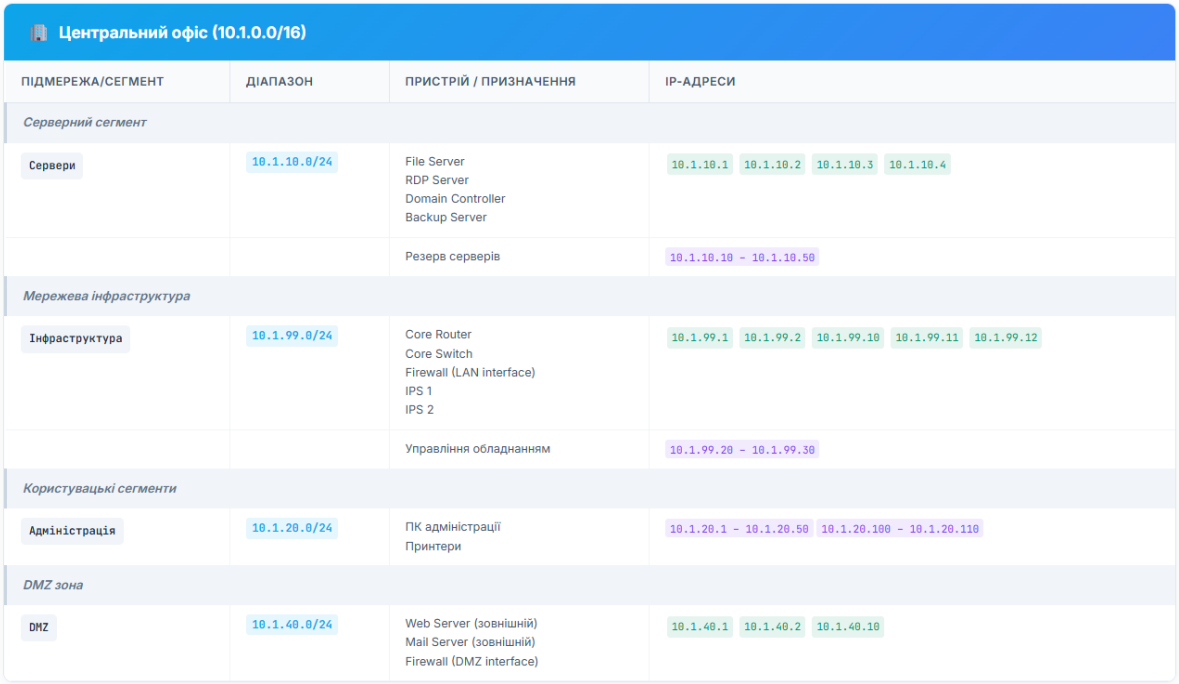
Рисунок 4.1 – Структурна схема корпоративної мережі

4.3 Принципи ip-адресації, структура

У корпоративній мережі «ТОВ ВУСО ГРУП» IP-адресація побудована з використанням внутрішнього приватного діапазону 10.0.0.0/8, що дозволяє організувати масштабовану і гнучку систему адресування для всіх підрозділів підприємства. Центральний офіс отримує підмережу 10.1.0.0/16, у межах якої виділені окремі сегменти для різних сервісів та структурних одиниць. Серверний сегмент використовує діапазон 10.1.10.0/24, де окремі IP-адреси призначаються ключовим серверам: файловий сервер розташовується на 10.1.10.1, сервер віддаленого доступу на 10.1.10.2, контролер домену на 10.1.10.3, а сервер резервного копіювання – на 10.1.10.4. Додатково передбачений резерв адрес для розгортання нових серверів у межах цього сегменту.

Інфраструктурна частина центрального офісу (рисунок 4.2) згрупована в підмережу 10.1.99.0/24, де знаходяться основні мережеві пристрої: основний маршрутизатор (10.1.99.1), ядерний комутатор (10.1.99.2), міжмережевий екран (10.1.99.10), IPS-системи (10.1.99.11 та 10.1.99.12), а також адреси для управління обладнанням (10.1.99.20 – 10.1.99.30). Для адміністративного сегменту, що включає робочі місця адміністрації, використовується підмережа 10.1.20.0/24, у якій ПК співробітників отримують адреси в діапазоні 10.1.20.1 – 10.1.20.50, а принтери – у діапазоні 10.1.20.100 – 10.1.20.110.

Зона DMZ організована в підмережі 10.1.40.0/24, де розташовано зовнішній веб-сервер (10.1.40.1), поштовий сервер (10.1.40.2) і зовнішній інтерфейс міжмережевого екрану (10.1.40.10). Для розмежування та ізоляції критичних служб у DMZ застосовується окрема VLAN і відповідні політики контролю доступу.



Центральний офіс (10.1.0.0/16)

ПІДМЕРЕЖА/СЕГМЕНТ	ДІАПАЗОН	ПРИСТРІЙ / ПРИЗНАЧЕННЯ	IP-АДРЕСИ
Серверний сегмент			
Сервери	10.1.10.0/24	File Server RDP Server Domain Controller Backup Server	10.1.10.1 10.1.10.2 10.1.10.3 10.1.10.4
		Резерв серверів	10.1.10.10 – 10.1.10.50
Мережева інфраструктура			
Інфраструктура	10.1.99.0/24	Core Router Core Switch Firewall (LAN interface) IPS 1 IPS 2	10.1.99.1 10.1.99.2 10.1.99.10 10.1.99.11 10.1.99.12
		Управління обладнанням	10.1.99.20 – 10.1.99.30
Користувацькі сегменти			
Адміністрація	10.1.20.0/24	ПК адміністрації Принтери	10.1.20.1 – 10.1.20.50 10.1.20.100 – 10.1.20.110
DMZ зона			
DMZ	10.1.40.0/24	Web Server (зовнішній) Mail Server (зовнішній) Firewall (DMZ interface)	10.1.40.1 10.1.40.2 10.1.40.10

Рисунок 4.2 – Таблиця IP-адресації корпоративної мережі “ТОВ ВУСО ГРУП”

Для кожної філії (рисунок 4.3) організовано власний адресний простір. Так, для філії у Богодухові зарезервовано підмережу 10.2.0.0/16, для філії у Лозовій – 10.3.0.0/16, для філії у Валках – 10.4.0.0/16. У межах кожної з цих підмереж для локальної мережі виділено окремий діапазон, наприклад, 10.2.1.0/24 для Богодухова, 10.3.1.0/24 для Лозової, 10.4.1.0/24 для Валків. У кожній філії локальний маршрутизатор чи комутатор отримує першу адресу підмережі (наприклад, 10.2.1.1), IPS-система — адресу 10.2.1.10, користувацькі комп’ютери – адреси від 10.2.1.20 до 10.2.1.100, а принтери – адреси у межах 10.2.1.150 – 10.2.1.160. Для керування мережевим обладнанням у філіях додатково виділені службові підмережі типу 10.2.99.0/24, 10.3.99.0/24 тощо.

Такий підхід до IP-адресації забезпечує логічну сегментацію, зручне масштабування при розширенні мережі, а також простий і зрозумілий розподіл адрес серед пристроїв різних ролей та рівнів критичності. Він спрощує управління мережею, полегшує впровадження політик безпеки, сегментації та резервування, а також створює надійну основу для реалізації

централізованої маршрутизації і впровадження гнучких механізмів доступу до корпоративних ресурсів у масштабах всієї організації.

Філія Богодухів (10.2.0.0/16)

ПІДМЕРЕЖА/СЕГМЕНТ	ДІАПАЗОН	ПРИСТРІЙ / ПРИЗНАЧЕННЯ	IP-АДРЕСИ
Локальна мережа	10.2.1.0/24	Локальний Router/Switch IPS 1 ПК користувачів Принтери	10.2.1.1 10.2.1.10 10.2.1.20 - 10.2.1.100 10.2.1.150 - 10.2.1.160
Управління	10.2.99.0/24	Управління обладнанням	10.2.99.1

Філія Лозова (10.3.0.0/16)

ПІДМЕРЕЖА/СЕГМЕНТ	ДІАПАЗОН	ПРИСТРІЙ / ПРИЗНАЧЕННЯ	IP-АДРЕСИ
Локальна мережа	10.3.1.0/24	Локальний Router/Switch IPS 1 ПК користувачів Принтери	10.3.1.1 10.3.1.10 10.3.1.20 - 10.3.1.100 10.3.1.150 - 10.3.1.160

Філія Валки (10.4.0.0/16)

ПІДМЕРЕЖА/СЕГМЕНТ	ДІАПАЗОН	ПРИСТРІЙ / ПРИЗНАЧЕННЯ	IP-АДРЕСИ
Локальна мережа	10.4.1.0/24	Локальний Router/Switch IPS 1 ПК користувачів Принтери	10.4.1.1 10.4.1.10 10.4.1.20 - 10.4.1.100 10.4.1.150 - 10.4.1.160

Рисунок 4.3 – Таблиця IP-адресації філіалів “ТОВ ВУСО ГРУП”

4.4 Компоненти мережевої інфраструктури

Компоненти мережевої інфраструктури корпоративної мережі формують цілісну систему, яка забезпечує надійний обмін даними, доступність сервісів і високий рівень захисту інформації для всіх підрозділів компанії. Ключову роль у цій інфраструктурі відіграють маршрутизатори та шлюзи, зокрема пристрої Mikrotik, які відповідають за організацію міжмережевої маршрутизації, розмежування трафіку, створення захищених VPN-каналів для підключення віддалених офісів і контролю доступу до зовнішніх та внутрішніх ресурсів. Завдяки їхній функціональності стає можливим реалізувати політики безпеки, балансування навантаження та резервування основних маршрутів передачі даних.

Комутаційна інфраструктура представлена сучасними комутаторами,

які забезпечують ефективну агрегацію трафіку від кінцевих пристроїв, створення сегментованих VLAN для розмежування доступу різних служб, а також швидке й зручне підключення нових робочих місць. Комутатори працюють у тісній зв’язці з патч-панелями, що дозволяє організувати структуровану кабельну систему та оптимізувати адміністрування мережі.

Важливим елементом є централізоване сховище даних — файловий сервер, який гарантує надійне зберігання корпоративної інформації, підтримку резервного копіювання, контроль доступу до даних і швидкий обмін файлами між підрозділами. Такий підхід дозволяє зменшити ризики втрати або несанкціонованого доступу до важливих документів, а також оптимізувати роботу з великими обсягами інформації.

Серверне середовище включає всі програмно-апаратні ресурси, необхідні для забезпечення роботи прикладних сервісів компанії — це сервер віддаленого доступу (RDP), файловий сервер, контролер домену, поштовий сервер та інші спеціалізовані служби. Сучасне серверне обладнання розміщується у центральному офісі, що забезпечує централізований моніторинг, резервування критичних вузлів, швидке масштабування ресурсів відповідно до потреб бізнесу і реалізацію єдиної політики інформаційної безпеки. У сукупності всі ці компоненти створюють надійну основу для стабільної роботи корпоративної мережі, підвищують гнучкість управління та дають змогу оперативно впроваджувати нові сервіси для користувачів по всій організації.

4.4.1 Маршрутизатори та шлюзи (Mikrotik)

У центральному офісі доцільно використовувати продуктивні моделі маршрутизаторів Mikrotik, наприклад, Mikrotik CCR1009-7G-1C-1S+ (рисунок 4.4). Такі пристрої підтримують гігабітні та 10-гігабітні інтерфейси, що дозволяє агрегувати трафік із різних сегментів мережі, реалізовувати складні схеми маршрутизації та забезпечувати високу пропускну здатність

для внутрішніх та зовнішніх з’єднань. Центральний маршрутизатор відповідає за обробку міжсегментного трафіку, підключення до зовнішніх провайдерів, організацію резервованих каналів та підключення VPN-тунелів із усіма віддаленими філіями. На ньому налаштовується політика міжмережевого екрану, обмеження адміністративного доступу, а також моніторинг та журналювання подій безпеки.

Рисунок 4.4 – Mikrotik CCR1009-7G-1C-1S+

Для філій ідеально підходять компактні та енергоефективні маршрутизатори, такі як Mikrotik hEX S (RB760iGS) (рисунок 4.5). Вони забезпечують стабільний захищений зв’язок із центральним офісом через VPN, маршрутизацію локального трафіку у філії, а також інтеграцію з локальною інфраструктурою (комутаторами, IPS, принтерами та ПК). Завдяки вбудованому апаратному шифруванню пристрої Mikrotik здатні обробляти захищений трафік без зниження швидкості навіть при підключенні декількох десятків користувачів. У філіях маршрутизатор виконує роль шлюзу для локальної мережі, контролює доступ до зовнішніх ресурсів, веде облік активності користувачів та реалізує базові політики безпеки.

Рисунок 4.5 – Mikrotik hEX S

В обох випадках Mikrotik дозволяє гнучко налаштовувати резервування основних каналів (наприклад, підключення до другого провайдера чи організацію додаткового VPN-каналу), а також централізовано управляти всіма пристроями за допомогою єдиної платформи адміністрування. Такий підхід дає змогу підтримувати стабільний і захищений обмін даними між офісами, забезпечує централізований контроль і дає змогу оперативно масштабувати інфраструктуру у разі відкриття нових філій чи розширення компанії.

4.4.2 Комутаційна інфраструктура

У центральному офісі використовується високопродуктивний керований комутатор (Mikrotik CRS326-24G-2S+RM), який виконує функції ядра мережі (core switch) та основної точки агрегації трафіку від усіх серверів, систем безпеки та робочих станцій. Завдяки підтримці VLAN і 802.1Q комутатор дозволяє логічно розділяти трафік між різними службами й сегментами мережі (серверна зона, адміністрація, користувачі, DMZ, гостьова мережа тощо), забезпечуючи ізоляцію і підвищення рівня інформаційної безпеки. Розподіл портів, контроль пропускної здатності, моніторинг і управління можливі завдяки централізованому інтерфейсу налаштувань.

Всі фізичні підключення у серверній кімнаті організовані через патч-панелі, що значно спрощує адміністрування, дозволяє швидко перепідключати пристрої, а також забезпечує акуратний і структурований вигляд кабельної системи.

У віддалених офісах (Богодухів, Лозова, Валки) застосовуються компактні керовані комутатори (Mikrotik CSS326-24G-2S+RM), які дозволяють підключати локальні робочі станції, принтери й інше мережеве обладнання. Навіть на рівні філій комутатори можуть підтримувати базову сегментацію (VLAN), що дає змогу виділяти службові підмережі або

забезпечувати гостевий доступ до Інтернету ізольовано від корпоративного трафіку.

Завдяки використанню сучасних комутаторів і гнучкої структури підключень, компанія може безпечно та оперативно додавати нові робочі місця, масштабувати мережу, здійснювати централізований моніторинг активності, впроваджувати політики якості обслуговування (QoS) для критично важливих сервісів.

4.4.3 Централізоване сховище даних

В якості централізованого сховища даних у цьому проєкті доцільно застосовувати спеціалізовані мережеві сховища NAS (Network Attached Storage), наприклад, Synology DS220+(рисунок 4.6). Такі пристрої забезпечують багатокористувацький доступ до файлів через стандартні протоколи SMB/CIFS, NFS, FTP, а також можуть інтегруватися з доменною структурою компанії для централізованого контролю доступу. Завдяки підтримці RAID-масивів забезпечується висока надійність зберігання — навіть у разі виходу з ладу одного з жорстких дисків дані залишаються доступними без втрат.

Рисунок 4.6 – Synology DS220+

Централізоване сховище підключається до основного комутатора центрального офісу по гігабітному або 10-гігабітному інтерфейсу, що гарантує високу швидкість обміну даними навіть при значному навантаженні. Дані із регіональних філій передаються у сховище через захищені VPN-канали, що дозволяє співробітникам працювати з корпоративними файлами у єдиному інформаційному просторі, незалежно від їхнього фізичного розташування.

Для підвищення безпеки у сховищі налаштовуються багаторівневі права доступу, ведеться журналювання дій користувачів, впроваджується система регулярного резервного копіювання на окремий носій або у хмару. Додатково, сучасні NAS-системи підтримують сервіси версіонування файлів, антивірусний захист і можуть працювати як FTP-сервер, сервер резервного копіювання, або навіть як майданчик для обміну великими файлами між партнерами компанії.

4.4.4 Серверне середовище

У центральному офісі, в окремій захищеній серверній кімнаті, розміщується серверна шафа (rack), у якій встановлені основні вузли корпоративної IT-інфраструктури.

Наприклад, до складу серверного середовища входять такі компоненти:

- фізичний сервер Hewlett Packard Enterprise ProLiant DL380 Gen10 (рисунок 4.7). із процесором Intel Xeon Silver, 64 ГБ оперативної пам’яті та масивом SSD/HDD дисків у RAID 10. На цьому сервері розгортається гіпервізор (наприклад, VMware ESXi або Proxmox VE), що дозволяє створювати декілька ізольованих віртуальних машин для різних корпоративних сервісів;

- віртуальний сервер контролера домену (Active Directory Domain Controller), який відповідає за автентифікацію та централізоване управління користувачами;

- віртуальний файловий сервер (на базі Windows Server або Linux Samba), який забезпечує спільний доступ до документів, електронних архівів, резервних копій і файлів проектів для всіх співробітників;

- віртуальний сервер віддаленого доступу (RDP), що надає можливість підключення співробітників з віддалених офісів до корпоративної мережі через термінальні сесії;

- сервер резервного копіювання (наприклад, Veeam Backup або Bacula), який щодня автоматично створює резервні копії важливих даних на окремий NAS-сховище або хмарний ресурс;

- поштовий сервер (наприклад, Microsoft Exchange чи аналог на Linux), якщо компанія використовує власну корпоративну пошту;

- NAS-сховище Synology DS220+ для зберігання великих обсягів архівної інформації, організації спільного файлового простору й додаткового резервного копіювання.

Рисунок 4.7 – Hewlett Packard Enterprise ProLiant DL380 Gen1

Усі ці сервери з’єднані з ядром мережі через гігабітні або 10-гігабітні комутатори, мають резервне живлення (UPS), підключені до централізованої системи моніторингу та захищені багаторівневими політиками доступу (ACL, групові політики Active Directory, firewall).

4.4.5 Засоби моніторингу та управління

Конкретними прикладами засобів моніторингу та управління для

корпоративної мережі «ТОВ ВУСО ГРУП» є впровадження сучасних рішень як у центральному офісі, так і для віддалених філій. Наприклад, для комплексного моніторингу всієї мережевої інфраструктури доцільно використовувати Zabbix як основну платформу. Zabbix встановлюється на сервер у центральному офісі, збирає дані з маршрутизаторів Mikrotik (через SNMP, API), комутаторів, серверів, NAS-сховищ, а також здійснює моніторинг доступності сервісів RDP, файлового сервера, пошти тощо.

Всі пристрої додаються до системи моніторингу, для ключових вузлів налаштовуються тригери — наприклад, сповіщення у разі втрати зв’язку з філією, перевантаження процесора чи заповнення сховища.

Для глибшого аналізу трафіку і виявлення аномалій можна впровадити PRTG Network Monitor або Nagios, які дозволяють будувати графіки навантаження, відслідковувати пропускну здатність каналів між офісами, контролювати стан портів комутаторів і бачити активність користувачів у реальному часі.

Для централізованого збору логів застосовується Graylog або ELK Stack (Elasticsearch, Logstash, Kibana). Такі системи дають змогу аналізувати події безпеки, логувати підключення VPN, зміни в налаштуваннях Mikrotik, збої на серверах чи несанкціоновані спроби доступу.

Адміністрування маршрутизаторів Mikrotik здійснюється через Winbox — фірмову утиліту, яка дозволяє зручно й швидко підключатися до пристроїв, налаштовувати VPN-тунелі, моніторити стан інтерфейсів, резервувати конфігурації. Для хмарного або централізованого керування Mikrotik можна використовувати MikroTik Cloud Hosted Router (CHR). Для оновлення, резервування і віддаленого моніторингу комутаторів застосовується web-інтерфейс пристроїв або SNMP-менеджери (наприклад, ManageEngine OpManager).

Сервери віртуалізації адмініструються через VMware vSphere Client або Proxmox VE Web UI. Для управління віртуальними машинами на Windows — Windows Admin Center, на Linux — Cockpit або Webmin.

Усе це дає змогу команді адміністраторів оперативно реагувати на будь-які проблеми в мережі, швидко виявляти й локалізувати збої, ефективно управляти масштабованою корпоративною IT-інфраструктурою, підтримуючи безперервність бізнес-процесів.

Такий набір інструментів — Zabbix, Winbox, Graylog/ELK, PRTG/Nagios, VMware vSphere, Proxmox VE, SNMP-менеджери — дає змогу побудувати для «ТОВ ВУСО ГРУП» надійну, прозору й легко керовану систему моніторингу та управління навіть у складній розподіленій мережі.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було проаналізовано особливості організації діяльності великих корпоративних структур, визначено основні технічні та організаційні виклики, з якими стикаються страхові компанії під час цифрової трансформації. Було розроблено архітектуру мережі, яка забезпечує надійний захищений зв’язок між головним офісом і віддаленими філіями, централізоване управління ресурсами, ефективний захист персональних даних клієнтів і можливість подальшого розширення мережі відповідно до динаміки розвитку бізнесу.

Особливу увагу у проекті приділено питанням безпеки — впровадженню багаторівневих систем захисту, централізованому моніторингу, механізмам резервного копіювання та швидкого відновлення даних. Це дозволяє гарантувати не лише захист від сучасних кіберзагроз, а й підтримувати високу стійкість мережевої інфраструктури навіть у кризових ситуаціях. Окремо підкреслено важливість гнучкості архітектурних рішень, які дозволяють швидко реагувати на зміни у структурі компанії, відкриття нових підрозділів або необхідність переходу на віддалений режим роботи.

Практична цінність проведеного дослідження полягає у тому, що розроблені підходи й проектні рішення можуть бути застосовані не лише у страховій компанії «ВУСО ГРУП», а й адаптовані для інших організацій з аналогічною структурою. Використання описаних технологій і принципів проектування сприятиме підвищенню технологічної зрілості галузі, покращенню якості обслуговування клієнтів та підвищенню конкурентоспроможності підприємств на ринку.

Таким чином, результати роботи мають важливе практичне та теоретичне значення, підтверджують актуальність комплексного підходу до проектування корпоративних мереж і слугують основою для подальшого впровадження інноваційних цифрових рішень у страховому секторі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Оліфер В.Г., Оліфер Н.А. Комп'ютерні мережі: принципи, технології, протоколи. – 2006. – 958 с.

2. Столлінгс В. Комп'ютерні мережі, протоколи і технології Інтернету. –.: BHV, 2005. – 832 с.

3. Таненбаум Е. С., Уезеролл Д. Дж. Комп'ютерні мережі: підручник. – 5-те вид. – К.: Видавництво «Вільямс», 2012. – 880 с.

4. Річардс Д. Основи локальних мереж. – К.: Діалектика, 2004. – 416 с.

5. Бех М.О., Ярошенко О.О. Технології побудови структурованих кабельних систем: навчальний посібник. – Х.: ХНУРЕ, 2019. – 135 с.

6. Каток В.Б., Руденко І.Є. Сучасні технології з'єднань волоконних світловодів зі складу оптичних кабелів зв'язку // Інформатизація та нові технології. – 1996, №1. – С. 41–43.

7. IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 3: CSMA/CD Access Method and Physical Layer Specifications. IEEE Std 802.3-2018.

8. RFC 1918 Address Allocation for Private Internets [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc1918

9. Ubiquiti Inc. EdgeRouter – User Guide [Електронний ресурс]. – Режим доступу: https://help.ui.com/hc/en-us/articles/204959174-EdgeRouter-User-Guide

10. Cisco Systems. IP Addressing and Subnetting for New Users [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13788-3.html

11. Synology Inc. NAS User's Guide [Електронний ресурс]. – Режим доступу: https://kb.synology.com/en-

global/DSM/help/DSM/AdminCenter/system_information

12. Yealink SIP-T21P E2 IP Phone – User Manual [Електронний ресурс]. – Режим доступу: https://support.yealink.com/