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)

Локальна комп’ютерна мережа кол-центру компанії "CallMax"

(тема)

Виконав:
здобувач 4 року навчання,
групи КІУКІ-21-6
Данило СКЕТРІС
(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 Скетрісу Данилу Ігоровичу
(прізвище, ім’я, по батькові)

1. Тема роботи Локальна комп’ютерна мережа кол-центру компанії "CallMax"

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 вимог та планування мережевої інфраструктури кол-центру
2. Теоретичні відомості про комп'ютерні мережі та ір-телефонію
3. Проєктування архітектури локальної мережі для кол-центру
4. Реалізація та конфігурація мережевої інфраструктур

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій 17 слайдів презентації

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: 82 с., 4 рис., 1 дод., 12 джерел.

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

Метою кваліфікаційної роботи є розробка й впровадження оптимальної архітектури локальної комп’ютерної мережі для кол-центру компанії "CallMax", яка забезпечить надійну роботу IP-телефонії, ефективну інтеграцію даткових додатків і можливість подальшого масштабування відповідно до потреб бізнесу. Для досягнення цієї мети необхідно здійснити комплексний аналіз поточного стану мережевої інфраструктури, визначити проблеми й обмеження, що заважають ефективній роботі, вивчити сучасні технології побудови конвергентних мереж та IP-телефонії, а також методи забезпечення якості сервісу для критично важливих додатків.

ABSTRACT

Bachelor’s thesis: 82 pages, 4 figures, 1 appendix, 12 sources.

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

The purpose of this qualification work is to design and implement an optimal architecture for a local computer network for the "CallMax" call center, which will ensure reliable operation of IP telephony, effective integration of data applications, and the possibility of further scaling in accordance with business needs.

To achieve this goal, it is necessary to conduct a comprehensive analysis of the current state of the network infrastructure, identify the problems and limitations that hinder effective operation, study modern technologies for building converged networks and IP telephony, as well as methods for ensuring service quality for critically important applications.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

BGP — Border Gateway Protocol (пограничний шлюзовий протокол)

CUCM — Cisco Unified Communications Manager (централізований менеджер голосових сервісів)

EIGRP — Enhanced Interior Gateway Routing Protocol (покращений внутрішній шлюзовий протокол маршрутизації)

HSRP — Hot Standby Router Protocol (протокол резервного маршрутизатора)

LAN — Local Area Network (локальна обчислювальна мережа)

PoE — Power over Ethernet (живлення через Ethernet)

QoS — Quality of Service (якість обслуговування)

RIP — Routing Information Protocol (протокол маршрутизації інформації)

RTP — Real-time Transport Protocol (протокол передачі потокових даних у реальному часі)

RTCP — Real-time Transport Control Protocol (протокол контролю потокових даних у реальному часі)

SIP — Session Initiation Protocol (протокол ініціалізації сесії)

STP — Spanning Tree Protocol (протокол дерева відмов)

VLAN — Virtual Local Area Network (віртуальна локальна мережа)

VoIP — Voice over IP (передача голосу через IP)

WAN — Wide Area Network (глобальна обчислювальна мережа)

OSPF — Open Shortest Path First (відкритий протокол найкоротшого шляху)

ВСТУП

Сучасний розвиток телекомунікаційних технологій і дедалі вища потреба в якісному клієнтському сервісі висувають до організацій, що працюють у сфері контакт-центрів, жорсткі вимоги щодо мережевої інфраструктури. Ефективність роботи кол-центру безпосередньо залежить від надійності, продуктивності та масштабованості локальної комп'ютерної мережі, яка має забезпечувати інтеграцію голосових і даткових сервісів, підтримку критично важливих додатків і безперервність бізнес-процесів. Компанія "CallMax", що спеціалізується на послугах клієнтського сервісу для великих корпоративних замовників, стикається з потребою модернізації мережевої інфраструктури. Діючі рішення не забезпечують необхідної надійності й масштабованості для зростаючих обсягів телефонного трафіку й інтеграції сучасних IP-телефонних технологій[1]. Застаріле обладнання створює вузькі місця в обробці даних, що негативно впливає на якість обслуговування клієнтів та ефективність операторів.

Проблематика дослідження зумовлена кількома основними факторами. З одного боку, стрімкий розвиток IP-телефонії й конвергентних мереж вимагає впровадження сучасних архітектур, що гарантують якість передачі голосового трафіку з мінімальними затримками й втратами пакетів. З іншого боку, підвищуються вимоги до інформаційної безпеки — особливо в контексті обробки персональних даних клієнтів, що зумовлює необхідність впровадження комплексних засобів захисту на всіх рівнях мережі. Також критичним завданням стає досягнення високої доступності (понад 99,9%) для ключових телекомунікаційних сервісів за рахунок надлишкової архітектури й протоколів швидкого відновлення.

Окремо варто відзначити плани компанії щодо масштабування: заплановано збільшення кількості робочих місць операторів із 120 до 200 протягом трьох років. Це потребує проектування гнучкої та масштабованої

мережевої архітектури, яка дозволить нарощувати потужності без радикальної перебудови всієї інфраструктури. Необхідна також інтеграція з сучасними CRM-системами, аналітичними платформами й хмарними сервісами, що вимагає високопродуктивної мережі з гарантованою якістю обслуговування для різних типів трафіку.

Метою цієї роботи є розробка й впровадження оптимальної архітектури локальної комп’ютерної мережі для кол-центру компанії "CallMax", яка забезпечить надійну роботу IP-телефонії, ефективну інтеграцію даткових додатків і можливість подальшого масштабування відповідно до потреб бізнесу. Для досягнення цієї мети необхідно здійснити комплексний аналіз поточного стану мережевої інфраструктури, визначити проблеми й обмеження, що заважають ефективній роботі, вивчити сучасні технології побудови конвергентних мереж та IP-телефонії[2], а також методи забезпечення якості сервісу для критично важливих додатків. У ході дослідження розробляється оптимальна архітектура мережі на основі ієрархічної топології з урахуванням вимог до надійності, масштабованості й безпеки, здійснюється проектування системи IP-адресації та VLAN-сегментації для ефективного керування трафіком, виконується розрахунок пропускної здатності для поточних і прогнозованих навантажень, розробляється комплексна система безпеки з урахуванням периметрового захисту, внутрішньої сегментації та систем виявлення вторгнень. Також реалізується мережна інфраструктура з детальною конфігурацією всіх компонентів, впроваджується система моніторингу й управління для оперативного контролю та запобігання проблем, інтегрується IP-телефонне обладнання з автоматичним розподілом дзвінків, записом розмов і зв’язком із CRM.

Об’єктом дослідження виступає мережева інфраструктура кол-центру як основа якісних телекомунікаційних послуг у сфері клієнтського сервісу. Предметом дослідження є методи й технології проектування, впровадження та управління локальними комп’ютерними мережами для

телекомунікаційних підприємств із акцентом на забезпечення якості IP-телефонії та інтеграції конвергентних сервісів. Для цього застосовуються системний аналіз, порівняльний огляд технологій та протоколів, моделювання мережевого трафіку, експериментальне тестування продуктивності, а також методи проектування відмовостійких систем, що базуються на галузевих стандартах провідних виробників, зокрема Cisco, та міжнародних рекомендаціях IEEE і ITU-T.

Наукова новизна роботи полягає у розробці комплексного підходу до проектування мережевої інфраструктури кол-центру, що інтегрує сучасні технології конвергентних мереж із урахуванням специфіки галузі. Запропоновано оригінальну методику розрахунку пропускної здатності для змішаного голосового й даткового трафіку з використанням статистичних моделей телетрафіку, а також архітектурне рішення для забезпечення горизонтального масштабування мережі без зупинки критично важливих сервісів. Практична значущість полягає в можливості застосування розроблених рішень для модернізації інфраструктури "CallMax" та аналогічних підприємств: це дозволяє скоротити витрати на обслуговування, підвищити якість послуг і створити платформу для впровадження інноваційних сервісів. Описані методики конфігурації та управління можуть бути адаптовані для різних масштабів і особливостей замовників.

Впровадження запропонованого рішення забезпечує зниження кількості збоїв на 90%, підвищення пропускної здатності мережі у п’ять разів, скорочення часу відновлення після відмови до 2–3 хвилин, а також можливість безболісного масштабування до 200 робочих місць без додаткових капітальних витрат. Структура роботи містить чотири розділи, які послідовно охоплюють аналіз вимог, теоретичні основи комп’ютерних мереж і IP-телефонії, проектування архітектури з розрахунками та обґрунтуваннями, а також практичну реалізацію з конкретними прикладами налаштувань.

1 АНАЛІЗ ВИМОГ ТА ПЛАНУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ КОЛ-ЦЕНТРУ

1.1 Характеристика діяльності компанії "CallMax" та специфіка роботи кол-центру

Компанія "CallMax" є провідним українським постачальником послуг клієнтського сервісу та технічної підтримки, що спеціалізується на аутсорсингу контакт-центрів для великих корпоративних клієнтів. Заснована у 2018 році як дочірнє підприємство телекомунікаційного холдингу, компанія швидко зайняла стійкі позиції на ринку BPO (Business Process Outsourcing) послуг України, обслуговуючи понад 50 великих компаній з різних галузей економіки, включаючи телекомунікації, банківський сектор, електронну комерцію та енергетику.

Місією компанії "CallMax" є забезпечення найвищого рівня клієнтського сервісу через впровадження інноваційних технологій та підготовку висококваліфікованого персоналу. Стратегічні цілі організації включають розширення клієнтської бази до 100 корпоративних клієнтів протягом наступних п'яти років, впровадження штучного інтелекту та автоматизації процесів, а також вихід на міжнародні ринки Східної Європи.

Основними напрямами діяльності компанії "CallMax" є багатоканальне обслуговування клієнтів через різні комунікаційні канали. Inbound сервіси включають технічну підтримку клієнтів телекомунікаційних компаній з обробкою запитів щодо налаштування обладнання, усунення несправностей та консультування з тарифних планів. Банківський напрямок охоплює консультування з банківських продуктів та послуг, обробку заявок на кредити та картки, технічну підтримку інтернет-банкінгу та мобільних додатків.

Сектор електронної комерції включає обробку замовлень інтернет-

магазинів, консультування покупців щодо характеристик товарів, обробку рекламацій та повернень, координацію з логістичними службами. Outbound сервіси охоплюють проведення маркетингових досліджень та опитувань громадської думки, телемаркетинг та продаж товарів і послуг, нагадування про платежі та заборгованості, інформування клієнтів про нові продукти та акції.

Кол-центр компанії розташований у сучасному бізнес-центрі "Київ Плаза" у Печерському районі міста Києва і займає два поверхи загальною площею 1200 квадратних метрів. Робочі місця операторів організовані за принципом відкритого офісного простору з ергономічними робочими станціями та звукоізоляційними перегородками для мінімізації шумового забруднення. Планування офісу включає зонування за проектами та типами обслуговування для оптимізації workflow та забезпечення спеціалізації персоналу.

Загальна організаційна структура включає 120 робочих місць, розподілених наступним чином: 100 робочих місць призначені для операторів першої лінії, які безпосередньо спілкуються з клієнтами; 15 робочих місць для супервайзерів та менеджерів проектів, що забезпечують контроль якості та координацію роботи команд; 5 робочих місць для технічного персоналу, включаючи IT-адміністраторів та фахівців з обслуговування обладнання.

Операційна модель кол-центру характеризується високою інтенсивністю обробки комунікацій та строгими вимогами до якості обслуговування згідно з укладеними SLA (Service Level Agreement)[3]. Середня кількість оброблених дзвінків становить 15000-20000 на день у звичайні дні, при цьому пікові навантаження під час промо-акцій клієнтів або технічних збоїв можуть сягати 35000-40000 дзвінків на добу. Середня тривалість розмови варіюється від 3-5 хвилин для простих запитів до 15-20 хвилин для складних технічних консультацій.

Робота ведеться у три основні зміни: ранкова зміна з 7:00 до 15:00,

денна зміна з 15:00 до 23:00 та нічна зміна з 23:00 до 7:00, що забезпечує безперервне обслуговування клієнтів протягом 24 годин на добу, 7 днів на тиждень. Розподіл персоналу по змінах здійснюється відповідно до статистики навантаження: 40% операторів працюють у ранковій зміні, 45% - у денній (пікове навантаження) та 15% - у нічній зміні.

Ключові технологічні процеси кол-центру включають автоматичний розподіл вхідних дзвінків між доступними операторами через систему ACD (Automatic Call Distribution) з інтелектуальним маршрутизуванням на основі навичок операторів та типу запиту. Інтерактивний голосовий відгук IVR (Interactive Voice Response) забезпечує попередню обробку дзвінків, збирання інформації про клієнта та направлення до відповідного оператора або автоматичне надання базової інформації.

Реєстрація та документування всіх звернень здійснюється у корпоративній CRM-системі на базі Salesforce з інтеграцією телефонної системи для автоматичного pop-up інформації про клієнта при надходженні дзвінка. Система включає повну історію взаємодій з клієнтом, інформацію про продукти та послуги, knowledge base для швидкого пошуку рішень типових проблем.

Запис телефонних розмов для контролю якості здійснюється у 100% випадків з зберіганням записів протягом 12 місяців відповідно до вимог регуляторного законодавства. Система забезпечує можливість прослуховування записів супервайзерами в режимі реального часу, пошук по ключових словах та автоматичне виявлення емоційного забарвлення розмов через speech analytics.

Моніторинг показників роботи операторів здійснюється у реальному часі через спеціалізовані dashboard з відображенням KPI (Key Performance Indicators): кількість оброблених дзвінків, середній час розмови (AHT - Average Handle Time), час очікування клієнтів (ASA - Average Speed of Answer), рівень задоволеності клієнтів (CSAT - Customer Satisfaction Score), коефіцієнт вирішення проблем з першого дзвінка (FCR - First Call Resolution).

Генерація звітності здійснюється автоматично з різною періодичністю: real-time dashboard для оперативного управління, годинні звіти для корекції розподілу навантаження, денні звіти для аналізу продуктивності, тижневі та місячні звіти для стратегічного планування та звітування перед клієнтами.

Кожне робоче місце оператора обладнане сучасним комп'ютером з процесором Intel Core i5, 16 ГБ оперативної пам'яті та SSD накопичувачем для швидкого завантаження додатків. IP-телефон Cisco 7841 з підтримкою HD Voice забезпечує високу якість голосового зв'язку. Професійна гарнітура Plantronics з шумоподавленням мінімізує вплив офісного шуму. Додатковий 24-дюймовий монітор дозволяє одночасно працювати з CRM-системою та іншими додатками.

Супервайзери мають розширені можливості контролю через спеціалізовані робочі станції з підтримкою silent monitoring (прослуховування дзвінків без втручання), barge-in (втручання в розмову для надання допомоги оператору), coaching (приватні підказки оператору під час розмови). Система dashboard супервайзера відображає стан всіх операторів команди, черги дзвінків, алерти про перевищення порогових значень KPI.

Технічна інфраструктура кол-центру включає кілька критично важливих компонентів. Центральним елементом є IP-АТС на базі Cisco Unified Communications Manager (CUCM), яка забезпечує маршрутизацію дзвінків, інтеграцію з телефонними мережами загального користування через SIP trunk, управління чергами дзвінків та розширені функції телефонії.

CRM-система на базі Salesforce Service Cloud зберігає централізовану базу даних клієнтів з історією всіх взаємодій, інтегрується з телефонною системою через CTI (Computer Telephony Integration) connector, забезпечує workflow management для складних запитів та автоматизацію рутинних процесів.

Система запису дзвінків Cisco MediaSense архівує всі телефонні розмови у форматі WAV з компресією G.711, забезпечує індексацію записів за метаданими (час, номери телефонів, оператор), надає web-інтерфейс для

пошуку та прослуховування записів, інтегрується з WFM системами для планування робочого часу.

Workforce Management (WFM)[4] система Aspect eWorkforce забезпечує прогнозування навантаження на основі історичних даних, автоматичне складання розкладів роботи операторів з урахуванням навичок та доступності, real-time adherence моніторинг відповідності фактичної роботи запланованому розкладу, управління заявками на відпустки та лікарняні.

Особливістю роботи кол-центру є необхідність забезпечення високої доступності всіх систем, оскільки будь-які збої можуть призвести до втрати дзвінків, порушення SLA з клієнтами та репутаційних ризиків. Компанія працює за контрактами з гарантованим рівнем обслуговування 99.5% uptime, що вимагає мінімізації планового та непланового простою систем до максимум 3.6 годин на місяць.

Аналіз поточного стану технічної інфраструктури виявляє ряд критичних обмежень, що впливають на ефективність роботи та перешкоджають подальшому розвитку бізнесу. Застаріле мережеве обладнання, встановлене 6 років тому, не забезпечує достатньої пропускної здатності під час пікових навантажень, що призводить до затримок у роботі CRM-системи на 5-10 секунд та періодичного погіршення якості VoIP-зв'язку з джиттером до 100 мілісекунд.

1.2 Аналіз функціональних та технічних вимог до мережевої інфраструктури кол-центру

Функціональні вимоги до мережевої інфраструктури кол-центру визначаються специфікою телекомунікаційних послуг, критичністю безперервної роботи систем і необхідністю забезпечення високої якості обслуговування клієнтів. Аналіз бізнес-процесів та технологічних потреб дозволяє узагальнити вимоги й визначити пріоритети для проектування оптимальної архітектури.

Головною функціональною вимогою є забезпечення надійної передачі голосового трафіку з мінімальними затримками та без втрат якості. Мережа має підтримувати одночасно до 120 активних голосових сесій із можливістю масштабування до 200 без погіршення продуктивності. Допустима затримка для голосового трафіку не повинна перевищувати 150 мілісекунд в одному напрямку згідно з рекомендаціями ITU-T G.114, а рівень втрат пакетів має бути меншим за 1% для забезпечення прийнятної якості звуку. Джиттер, або варіація затримки пакетів, не повинен перевищувати 30 мілісекунд, щоб уникнути появи аудіо-артефактів і забезпечити природність розмови. Ці параметри є критичними для підтримки професійного іміджу компанії та задоволеності клієнтів якістю телефонного обслуговування.

Підтримка одночасної роботи великої кількості користувачів потребує ефективного управління мережевими ресурсами та інтелектуальної маршрутизації трафіку. Кожне робоче місце оператора створює кілька типів трафіку: голосовий трафік через IP-телефон із пропускною здатністю 64–87 кбіт/с залежно від кодека, трафік CRM-системи з коливанням від 50 кбіт/с до 2 Мбіт/с під час передачі великих файлів, веб-браузинг і доступ до корпоративних ресурсів із середнім навантаженням 100–300 кбіт/с, синхронізація електронної пошти та миттєвих повідомлень. Пікове навантаження може досягати 80–90% від загальної кількості робочих місць, тому мережа проектується з урахуванням статистичного мультиплексування і коефіцієнтів одночасності для різних видів трафіку. Система повинна забезпечувати поступове зниження якості (graceful degradation) у разі перевантаження, але з пріоритезацією голосового трафіку.

Інтеграція різних типів обладнання передбачає безшовне підключення IP-телефонів з автоматичним налаштуванням через DHCP і TFTP, комп’ютерів із різними операційними системами (Windows, macOS, Linux), серверів віртуалізації та хмарних сервісів, систем безпеки, зокрема камер відеоспостереження й контролю доступу, принтерів, багатофункціональних пристроїв, мобільних пристроїв для реалізації політики BYOD (Bring Your

Own Device).

Мережа повинна підтримувати різні типи трафіку з відповідними вимогами до якості обслуговування через комплексну архітектуру QoS. Критично важливий голосовий трафік повинен отримувати найвищий пріоритет із гарантованою пропускною здатністю й мінімальними затримками. Трафік CRM-системи потребує стабільної пропускної здатності й помірних затримок для забезпечення комфортної роботи користувачів. Загальний інтернет-трафік може обслуговуватись за принципом best effort з обмеженнями для уникнення перевантаження доступних каналів.

Масштабованість системи є однією з ключових вимог у зв’язку з амбітними планами розвитку компанії. Архітектура повинна підтримувати горизонтальне масштабування від 120 до 200 робочих місць протягом трьох років без необхідності повної реконструкції мережі. Це передбачає модульний підхід із можливістю додавання нових сегментів, резервування портів комутаторів для майбутніх підключень і планування достатньої пропускної здатності магістральних каналів. Вертикальна масштабованість також повинна бути підтримана — через можливість оновлення обладнання до більш продуктивних моделей без зміни загальної архітектури, використання стандартних інтерфейсів і протоколів, модульну конструкцію комутаторів, підтримку forward compatibility для нових технологій.

Технічні вимоги деталізують кількісні показники продуктивності, надійності й безпеки. Пропускна здатність локальної мережі повинна становити не менше 1 Гбіт/с для кожного сегмента доступу з можливістю агрегації до 10 Гбіт/с для магістральних з’єднань. Це дозволить забезпечити запас пропускної здатності при максимальних навантаженнях і впроваджувати ресурсоємні додатки у майбутньому. Канал доступу до Інтернету має забезпечувати пропускну здатність не менше 200 Мбіт/с із можливістю короткочасного збільшення до 500 Мбіт/с, а резервний канал — не менше 100 Мбіт/с для підтримки основних функцій у разі відмови основного провайдера.

Вимоги до затримок особливо важливі для VoIP-трафіку[5] й реального часу: внутрішньомережева затримка між будь-якими двома точками не повинна перевищувати 10 мс, що передбачає використання комутаторів з апаратною маршрутизацією пакетів і оптимізованої топології. End-to-end затримка для голосових викликів через SIP trunk має залишатися в межах 150 мс. Буферизація в обладнанні повинна бути достатньою для згладжування пульсацій трафіку без суттєвого збільшення затримок, а це вимагає впровадження інтелектуального керування буферами з алгоритмами пріоритезації.

Надійність мережі повинна забезпечувати коефіцієнт готовності не менше 99,9% (допустимо не більше 8,76 годин простою на рік), що відповідає SLA для кол-центрів. Для досягнення цього рівня необхідно виключити єдино можливі точки відмови шляхом резервування ключових елементів, впровадження протоколів швидкого відновлення (RSTP, HSRP), використання ДБЖ для всього обладнання. Показник середнього часу між відмовами (MTBF) для критично важливих компонентів має становити не менше 100 000 годин, а середній час на відновлення (MTTR) — не більше 4 годин з урахуванням доставки запасних частин і сервісних контрактів.

Безпека мережі повинна захищати від широкого спектра кіберзагроз відповідно до вимог обробки персональних і конфіденційних даних. Периметровий захист має включати next-generation firewall із DPI, систему запобігання вторгненням (IPS), хмарний anti-malware аналіз, засоби виявлення цільових атак (APT). Внутрішня безпека реалізується через сегментацію мережі (VLAN, ACL), мережевий контроль доступу (NAC) із автентифікацією 802.1X, EDR для виявлення підозрілої активності на кінцевих пристроях і системи DLP для запобігання витоку інформації. Усі критично важливі дані шифруються за допомогою AES-256 (на збереженні) та TLS 1.3 (під час передачі). Голосовий трафік захищається протоколом SRTP, а сигналізація SIP — через TLS.

Управління мережею має здійснюватися централізовано із

використанням SNMP v3 із шифруванням, автоматичним виявленням несправностей, інтелектуальним оповіщенням та генерацією докладної звітності для технічного й управлінського персоналу. Необхідне ведення versioned configuration management, регулярне резервне копіювання налаштувань, а також збір і аналітика показників продуктивності, використання статистики, прогнозування на основі алгоритмів машинного навчання для виявлення й попередження проблем.

Електроживлення обладнання має забезпечуватися за стандартом PoE+ (IEEE 802.3at) для IP-телефонів і точок доступу Wi-Fi, з бюджетом до 30 Вт на порт. Резервне живлення через ДБЖ повинне гарантувати роботу протягом 30 хвилин після зникнення основного струму з можливістю переключення на дизель-генератор. У серверних мають дотримуватися температурний режим 18–24°C та вологість 45–55%, бути встановлена система газового пожежогасіння, організовано контроль доступу та ефективне керування кабелями.

Всі компоненти повинні відповідати вимогам міжнародних стандартів ISO 27001 щодо інформаційної безпеки, GDPR — для захисту персональних даних, PCI DSS — для обробки платіжної інформації (за потреби) й вимогам чинного українського законодавства щодо телекомунікацій та персональних даних.

1.3 Дослідження існуючих рішень для мереж кол-центрів та їх порівняльний аналіз

Сучасний ринок пропонує широкий вибір технологічних рішень для побудови мережевої інфраструктури кол-центрів, які відрізняються архітектурними підходами, функціональними можливостями, вартістю впровадження та експлуатації. Детальний аналіз наявних рішень дозволяє визначити оптимальний підхід до проектування мережі для компанії «CallMax» з урахуванням специфічних вимог, бюджетних обмежень та

стратегічних цілей розвитку.

Традиційно побудова мереж кол-центрів базується на використанні конвергентної інфраструктури, яка об’єднує голосовий та датковий трафік в єдиній IP-мережі. Такий підхід став революційним для телекомунікаційної індустрії, оскільки дозволив відмовитись від застарілих TDM (Time Division Multiplexing) систем на користь більш гнучких і економічно ефективних IP-рішень. Основними компонентами такої архітектури є IP-АТС (IP Private Branch Exchange), конвергентні комутатори з підтримкою якості обслуговування (QoS), багатофункціональні IP-телефони та спеціалізоване програмне забезпечення для управління викликами й аналітики.

Переваги конвергентного підходу полягають у значному зниженні загальної вартості володіння завдяки консолідації інфраструктури, спрощенню управління й обслуговування, гнучкості у впровадженні нових сервісів і функцій, а також масштабованості архітектури для зростаючих потреб бізнесу. Економія досягається завдяки використанню єдиної кабельної системи для передачі голосу і даних, зменшенню кількості обладнання й персоналу, а також оптимізації каналів зв’язку.

Рішення від компанії Cisco Systems є прикладом комплексної екосистеми Unified Communications, яка забезпечує повну інтеграцію голосових і даткових сервісів із розширеними можливостями для спільної роботи. Cisco Unified Communications Manager (CUCM) виконує функції IP-АТС корпоративного рівня й забезпечує централізоване управління всіма голосовими сервісами, включаючи інтелектуальну маршрутизацію дзвінків, групи пошуку (hunt groups), автоматичний розподіл дзвінків, підтримку конференцій та інтеграцію голосових повідомлень.

Архітектура Cisco UC включає кластеризацію з автоматичним перемиканням у разі відмови для забезпечення високої доступності, географічну відмовостійкість для аварійного відновлення, session border controller для безпечного SIP-транкінгу, unity connection для просунутої голосової пошти та сервіси присутності. Комутатори серії Catalyst

підтримують розширені функції QoS, зокрема класифікацію та маркування трафіку, обмеження й формування трафіку, організацію черг та планування із апаратною обробкою на максимальній швидкості.

Перевагами екосистеми Cisco є надійність корпоративного рівня, підтверджена у впровадженнях для великих організацій, комплексна безпека із вбудованим захистом від загроз, розвинені аналітичні й звітні можливості, широкий спектр інтеграцій із продуктами сторонніх виробників через відкриті API та стандартні протоколи. Платформа здатна підтримувати до 40 000 користувачів в одному кластері CUCM[6] з автоматичним балансуванням навантаження та забезпечує перемикання у разі відмови основного сервера за долі секунди.

До розширених функцій безпеки належать шифрування сигналізації та медіапотоків, автентифікація й авторизація пристроїв, виявлення та запобігання вторгненням, безпечне налаштування й управління конфігураціями. Інтеграція з корпоративними системами управління ідентифікацією дозволяє використовувати єдиний вхід (single sign-on) та централізоване управління користувачами.

До недоліків рішення Cisco слід віднести значні початкові інвестиції та постійні витрати на ліцензії, що може бути суттєвою перешкодою для малих і середніх організацій. Стартові вкладення для кол-центру на 120 робочих місць можуть досягати 200 000–300 000 доларів США з урахуванням вартості обладнання, ліцензійного програмного забезпечення, професійних послуг та навчання персоналу. Крім того, складність конфігурування та управління вимагає висококваліфікованого технічного персоналу, що збільшує експлуатаційні витрати.

1.4 Обґрунтування вибору топології та архітектури локальної мережі

Вибір топології локальної мережі для кол-центру компанії "CallMax" базується на комплексному аналізі функціональних вимог, технічних

обмежень, економічних факторів та перспектив розвитку. Основними критеріями вибору є надійність, масштабованість, продуктивність, вартість впровадження та простота управління.

Топологія "зірка" з ієрархічною структурою є оптимальним рішенням для мережі кол-центру завдяки централізованому управлінню трафіком та можливості ефективної сегментації. Трирівнева ієрархічна модель включає рівень доступу для підключення кінцевих пристроїв, рівень розподілу для агрегації трафіку та рівень ядра для високошвидкісної комутації між сегментами мережі.

Рівень доступу складається з комутаторів, які забезпечують підключення робочих станцій операторів, IP-телефонів та іншого кінцевого обладнання. Кожен комутатор доступу обслуговує 24-48 портів та під'єднується до комутатора розподілу двома незалежними каналами для забезпечення резервування. Використання протоколу Spanning Tree Protocol (STP) забезпечує автоматичне перемикання на резервний канал при відмові основного.

Рівень розподілу виконує функції агрегації трафіку від комутаторів доступу, забезпечення міжсегментної маршрутизації та реалізації політик безпеки. Комутатори розподілу підтримують розширені функції Quality of Service (QoS) для пріоритизації голосового трафіку та забезпечення гарантованої пропускної здатності для критично важливих додатків.

Рівень ядра забезпечує високошвидкісну комутацію між сегментами мережі та підключення до зовнішніх мереж. Надлишкова архітектура ядра з двох комутаторів, з'єднаних каналами агрегації, забезпечує відмовостійкість та рівномірний розподіл навантаження.

Фізична сегментація мережі передбачає розділення на кілька логічних сегментів відповідно до функціонального призначення та вимог безпеки. Сегмент операторських робочих місць включає комп'ютери та IP-телефони операторів з налаштованими політиками QoS[7,8] для голосового трафіку. Сегмент серверів містить CRM-сервери, сервери баз даних, IP-АТС та

системи моніторингу з підвищеними вимогами до безпеки та доступності.

Управлінський сегмент призначений для робочих місць супервайзерів та IT-адміністраторів з доступом до систем управління мережею та моніторингу. Гостьовий сегмент забезпечує обмежений доступ до інтернету для відвідувачів без можливості доступу до внутрішніх ресурсів компанії.

Віртуальні локальні мережі (VLAN) використовуються для логічної сегментації трафіку на рівні комутаторів без необхідності фізичного розділення. Голосовий VLAN забезпечує ізоляцію VoIP-трафіку та застосування відповідних політик QoS. Даткові VLAN розділяють трафік різних підрозділів та забезпечують контрольований доступ до спільних ресурсів.

Протокол маршрутизації OSPF (Open Shortest Path First) забезпечує динамічну маршрутизацію між сегментами мережі з автоматичним перерахунком маршрутів при зміні топології. Використання кількох зон OSPF дозволяє оптимізувати передачу маршрутної інформації та зменшити навантаження на мережеве обладнання.

Архітектура безпеки базується на концепції захисту в глибину з використанням кількох рівнів захисту. Периметровий брандмауер забезпечує фільтрацію трафіку між внутрішньою мережею та інтернетом з контролем доступу на рівні додатків. Внутрішні брандмауери розмежовують доступ між різними сегментами мережі відповідно до принципу мінімальних привілеїв.

Система виявлення та запобігання вторгненням (IDS/IPS) моніторить мережевий трафік на предмет підозрілої активності та автоматично блокує потенційно небезпечні з'єднання. Інтеграція з SIEM-системою забезпечує централізоване збирання та аналіз журналів безпеки від всіх мережевих пристроїв.

Архітектура високої доступності включає резервування всіх критично важливих компонентів мережі. Подвійне підключення серверів до різних комутаторів забезпечує збереження з'єднання при відмові одного з них. Протоколи швидкого відновлення, такі як Rapid Spanning Tree Protocol

(RSTP), мінімізують час переключення на резервні канали.

Система безперебійного живлення забезпечує електроживлення мережевого обладнання при відключенні основної електромережі. PoE+ комутатори забезпечують живлення IP-телефонів та точок доступу Wi-Fi через мережевий кабель, що спрощує інсталяцію та зменшує кількість джерел живлення.

Бездротова інфраструктура доповнює дротову мережу, забезпечуючи мобільність для планшетів супервайзерів та гостьовий доступ до інтернету. Використання стандарту Wi-Fi 6 забезпечує високу пропускну здатність та підтримку великої кількості одночасних підключень.

Система моніторингу мережі базується на протоколі SNMP для збирання статистики використання та стану обладнання. Централізована система управління забезпечує графічне відображення топології мережі, моніторинг продуктивності та автоматичне сповіщення про несправності.

Масштабованість архітектури забезпечується резервуванням портів комутаторів та використанням модульного обладнання з можливістю додавання інтерфейсних модулів. Планування адресного простору з використанням приватних IP-адрес дозволяє розширення мережі без зміни існуючої конфігурації.

2 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО КОМП'ЮТЕРНІ МЕРЕЖІ ТА IP-ТЕЛЕФОНІЮ

2.1 Основи побудови комп'ютерних мереж: класифікація, топології, мережеві технології

Комп'ютерні мережі являють собою сукупність пристроїв, з'єднаних каналами зв'язку та керованих мережевим програмним забезпеченням з метою спільного використання ресурсів та обміну інформацією. Розуміння фундаментальних принципів побудови мереж є критично важливим для проектування ефективної інфраструктури кол-центру, оскільки визначає архітектурні рішення, вибір обладнання та методології управління.

Класифікація комп'ютерних мереж (рисунок 2.1) здійснюється за декількома основними критеріями, кожен з яких впливає на технічні характеристики та область застосування. За географічним охопленням мережі поділяються на персональні (PAN - Personal Area Network), локальні (LAN - Local Area Network), міські (MAN - Metropolitan Area Network) та глобальні (WAN - Wide Area Network). Для кол-центру найбільш релевантними є локальні мережі, які забезпечують з'єднання пристроїв в межах одного або кількох суміжних будинків.

Локальні мережі характеризуються високою пропускною здатністю, низькими затримками та відносно простою структурою управління. Сучасні LAN зазвичай працюють на швидкостях від 100 Мбіт/с до 10 Гбіт/с, що цілком достатньо для забезпечення потреб кол-центру. Фізичне середовище передачі в локальних мережах представлене переважно витою парою категорій 5e, 6 або 6A, оптоволоконними кабелями для магістральних з'єднань та бездротовими технологіями для забезпечення мобільності.

За способом передачі даних мережі класифікуються як комутовані (switched) та широкомовні (broadcast). Комутовані мережі, які є стандартом

для сучасних корпоративних застосувань, забезпечують створення виділених каналів між відправником та отримувачем, що гарантує повну пропускну здатність порту для кожного з'єднання. Це особливо важливо для VoIP-трафіку, який вимагає гарантованої якості обслуговування.

Топологія мережі визначає фізичне та логічне розташування вузлів та з'єднань між ними. Основними топологіями є шина, кільце, зірка, дерево та меш (повнозв'язна). Для корпоративних мереж найбільш поширеною є топологія "зірка" та її модифікації, оскільки вона забезпечує централізоване управління, простоту діагностики несправностей та високу надійність.

Рисунок 2.1 – Класифікація комп'ютерних мереж

Ієрархічна топологія, яка є розширенням топології "зірка", включає три основні рівні: доступу, розподілу та ядра (рисунок 2.2). Рівень доступу забезпечує підключення кінцевих пристроїв та реалізацію базових функцій безпеки. Рівень розподілу виконує агрегацію трафіку, маршрутизацію між VLAN та застосування політик безпеки. Рівень ядра забезпечує високошвидкісну передачу даних між різними частинами мережі.

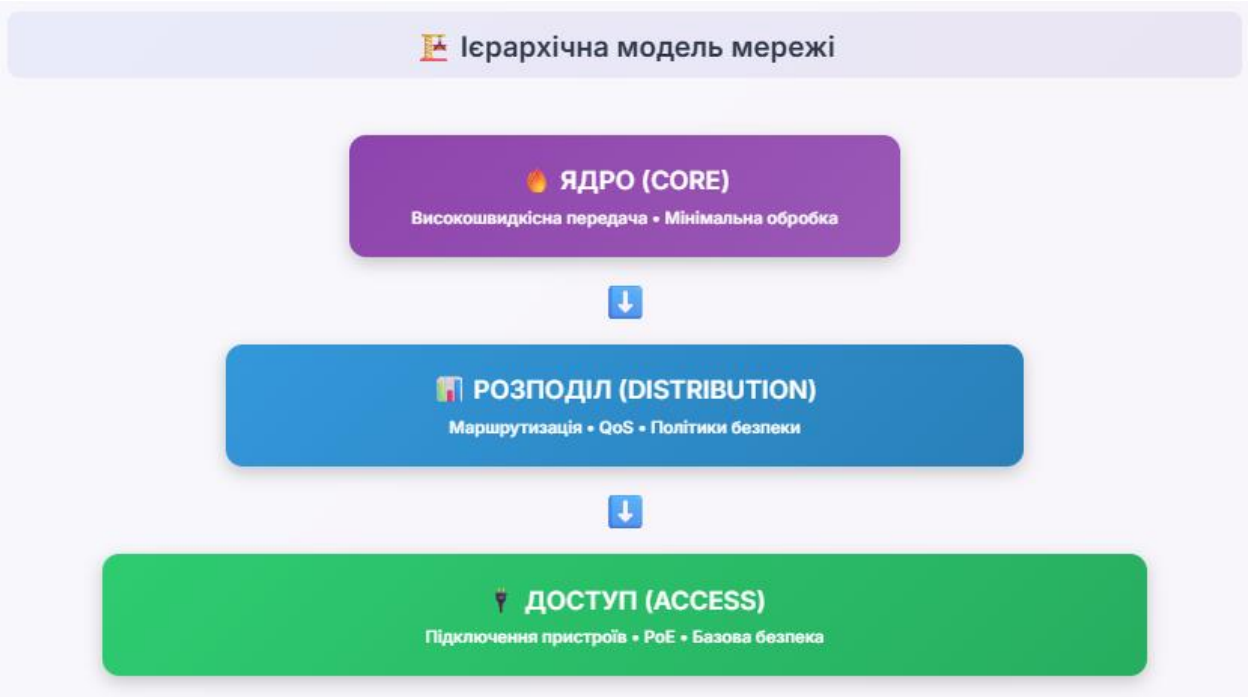

Рисунок 2.2 – Ієрархічна модель мережі

Мережеві технології визначають методи передачі, форматування та управління даними в мережі. Ethernet залишається домінуючою технологією для локальних мереж завдяки простоті, надійності та економічності. Стандарт IEEE 802.3 визначає фізичні та канальні характеристики Ethernet, включаючи методи доступу до середовища, формати кадрів та процедури виявлення колізій.

Сучасні реалізації Ethernet використовують метод повнодуплексної передачі з комутацією пакетів, що дозволяє одночасну передачу та прийом даних без колізій. Швидкості 1000BASE-T (Gigabit Ethernet) та 10GBASE-T (10 Gigabit Ethernet) забезпечують достатню пропускну здатність для найбільш вимогливих застосувань кол-центру.

Віртуальні локальні мережі (VLAN)[9] дозволяють створювати логічні сегменти мережі незалежно від фізичного розташування пристроїв. Стандарт IEEE 802.1Q визначає методи тегування кадрів для ідентифікації приналежності до конкретного VLAN. Використання VLAN в кол-центрі дозволяє сегментувати голосовий та даткові трафік, підвищуючи безпеку та спрощуючи управління QoS.

Протокол Spanning Tree Protocol (STP) та його удосконалені версії Rapid STP (RSTP) і Multiple STP (MSTP) забезпечують елімінацію петель в мережевій топології при збереженні резервних шляхів для відмовостійкості. Для кол-центру, де критична безперервність роботи, правильна конфігурація STP є обов'язковою для забезпечення стабільності мережі.

Агрегація каналів (Link Aggregation) згідно стандарту IEEE 802.3ad дозволяє об'єднувати кілька фізичних з'єднань в один логічний канал з підвищеною пропускною здатністю та відмовостійкістю. Protocol Link Aggregation Control Protocol (LACP) забезпечує автоматичну конфігурацію та моніторинг агрегованих з'єднань.

Power over Ethernet (PoE) згідно стандартів IEEE 802.3af, 802.3at (PoE+) та 802.3bt (PoE++) дозволяє передавати електроживлення через мережевий кабель разом з даними. Це особливо важливо для IP-телефонів, точок доступу Wi-Fi та камер безпеки, оскільки спрощує інсталяцію та зменшує кількість кабелів.

Бездротові технології, зокрема Wi-Fi на базі стандартів IEEE 802.11, доповнюють дротову інфраструктуру, забезпечуючи мобільність та гнучкість. Сучасний стандарт Wi-Fi 6 (802.11ax) підтримує швидкості до 9.6 Гбіт/с та оптимізований для роботи в щільно заселених середовищах, що робить його придатним для офісних застосувань.

Технології Quality of Service (QoS) забезпечують диференційоване обслуговування різних типів трафіку відповідно до їх пріоритету та вимог до якості. IEEE 802.1p визначає пріоритизацію на канальному рівні, а DiffServ (Differentiated Services) - на мережевому рівні. Для голосового трафіку зазвичай встановлюється найвищий пріоритет для забезпечення мінімальних затримок та джиттеру.

Мережева безпека реалізується через комбінацію технологій аутентифікації, авторизації та шифрування. IEEE 802.1X забезпечує автентифікацію пристроїв при підключенні до мережі, а технології IPSec та SSL/TLS - шифрування трафіку. Системи виявлення та запобігання

вторгненням (IDS/IPS) моніторять мережевий трафік на предмет підозрілої активності.

Управління мережею базується на протоколі Simple Network Management Protocol (SNMP), який дозволяє централізовано моніторити стан обладнання, збирати статистику використання та конфігурувати параметри. Сучасні системи управління мережею інтегрують функції моніторингу, конфігурації, управління несправностями та планування продуктивності.

2.2 Принципи функціонування протоколів TCP/IP та мережевих служб

Стек протоколів TCP/IP (рисунок 2.3) є фундаментальною основою сучасних комп'ютерних мереж, включаючи інтернет та корпоративні мережі. Розуміння принципів функціонування цих протоколів критично важливе для проектування мережевої інфраструктури кол-центру, оскільки всі сучасні додатки, включаючи VoIP, базуються на TCP/IP.

Модель TCP/IP складається з чотирьох рівнів: фізичного, канального, мережевого та транспортного, хоча часто використовується п'ятирівнева модель з виділенням прикладного рівня. Кожен рівень виконує специфічні функції та взаємодіє з суміжними рівнями через стандартизовані інтерфейси, що забезпечує модульність та масштабованість архітектури.

Мережевий рівень реалізований протоколом Internet Protocol (IP), який забезпечує маршрутизацію пакетів між різними мережами. IP версії 4 (IPv4) використовує 32-бітні адреси, що обмежує адресний простір до приблизно 4.3 мільярдів унікальних адрес. Для корпоративних мереж зазвичай використовуються приватні діапазони адрес: 10.0.0.0/8, 172.16.0.0/12 та 192.168.0.0/16, визначені RFC 1918.

Структура IPv4-адреси включає мережеву та вузлову частини, розділення яких визначається маскою підмережі. Класова адресація (Class A, B, C) здебільшого замінена безкласовою (CIDR - Classless Inter-Domain Routing), яка забезпечує більш ефективне використання адресного простору

та гнучкість в проектуванні мереж.

IP версії 6 (IPv6) використовує 128-бітні адреси, що вирішує проблему вичерпання адресного простору IPv4. IPv6 також включає вдосконалені механізми автоконфігурації, безпеки та Quality of Service. Хоча впровадження IPv6 в корпоративних мережах поки що обмежене, планування перспективної інфраструктури повинно враховувати можливість міграції.

Протокол маршрутизації визначає методи побудови та обміну маршрутною інформацією між маршрутизаторами. Статична маршрутизація передбачає ручне налаштування маршрутів адміністратором, що підходить для простих топологій з обмеженою кількістю маршрутизаторів. Динамічна маршрутизація використовує спеціалізовані протоколи для автоматичного виявлення та розповсюдження маршрутної інформації.

Протоколи внутрішньої маршрутизації (IGP - Interior Gateway Protocols) використовуються в межах однієї автономної системи. RIP (Routing Information Protocol) є найпростішим, але обмеженим протоколом, придатним лише для невеликих мереж. OSPF (Open Shortest Path First) забезпечує швидку конвергенцію, підтримку VLSM та ієрархічну структуру зон, що робить його оптимальним для корпоративних мереж середнього та великого розміру.

EIGRP (Enhanced Interior Gateway Routing Protocol) поєднує переваги distance-vector та link-state протоколів, забезпечуючи швидку конвергенцію та ефективне використання мережевих ресурсів. Однак EIGRP є власницьким протоколом Cisco, що обмежує його використання в гетерогенних середовищах.

Транспортний рівень представлений двома основними протоколами: TCP (Transmission Control Protocol) та UDP (User Datagram Protocol). TCP забезпечує надійну, орієнтовану на з'єднання передачу даних з гарантованою доставкою, контролем порядку та потоку. Механізми TCP включають встановлення з'єднання через триетапне рукостискання, нумерацію сегментів, підтвердження доставки та повторну передачу втрачених даних.

UDP є простішим протоколом без встановлення з'єднання, який не гарантує доставку або порядок пакетів. Однак UDP має менші накладні витрати та затримки, що робить його придатним для додатків реального часу, таких як VoIP, відеоконференції та онлайн-ігри. Більшість голосових додатків використовують UDP для передачі медіапотоків та TCP для сигналізації.

Система доменних імен (DNS) забезпечує перетворення символьних імен в IP-адреси та навпаки. DNS використовує ієрархічну структуру з кореневими серверами, серверами доменів верхнього рівня та авторитативними серверами. Для корпоративних мереж зазвичай розгортається внутрішня DNS-інфраструктура з можливістю інтеграції з Active Directory.

Протокол динамічної конфігурації хостів (DHCP) автоматизує призначення IP-адрес та інших мережевих параметрів клієнтським пристроям. DHCP-сервер управляє пулом доступних адрес та видає їх на певний термін (lease time). Опції DHCP дозволяють передавати додаткові параметри, такі як адреси DNS-серверів, шлюзу за замовчуванням та TFTP-серверів для автоконфігурації IP-телефонів.

Network Address Translation (NAT) дозволяє використовувати приватні IP-адреси у внутрішній мережі при спільному використанні одного або кількох публічних адрес для доступу до інтернету. PAT (Port Address Translation) або NAT Overload розширює можливості NAT, дозволяючи кільком внутрішнім пристроям одночасно використовувати одну публічну адресу через мультиплексування портів.

Протоколи безпеки IP включають IPSec для шифрування та аутентифікації на мережевому рівні. IPSec може працювати в транспортному режимі для захисту payload або тунельному режимі для захисту всього IP-пакету. IKE (Internet Key Exchange) забезпечує автоматичне встановлення безпечних з'єднань та обмін криптографічними ключами.

Протокол контролю повідомлень ICMP (Internet Control Message

Protocol) використовується для передачі інформаційних та помилкових повідомлень. Утиліти ping та traceroute базуються на ICMP для діагностики мережевої з'єднаності та маршрутизації. У корпоративних мережах ICMP часто обмежується через міркування безпеки, але повне блокування може ускладнити діагностику проблем.

Multicast дозволяє ефективну передачу даних від одного відправника до групи отримувачів. IGMP (Internet Group Management Protocol) управляє членством в multicast-групах, а протоколи PIM (Protocol Independent Multicast) забезпечують маршрутизацію multicast-трафіку. Multicast широко використовується для IP-телефонії, відеоконференцій та розповсюдження програмного забезпечення.

Якість обслуговування (QoS) на мережевому рівні реалізується через поле ToS (Type of Service) в IPv4 або Traffic Class в IPv6. DiffServ (Differentiated Services) переозначає ці поля для класифікації пакетів на основі DSCP (Differentiated Services Code Point). Інтегровані сервіси (IntServ) з протоколом RSVP забезпечують резервування ресурсів для конкретних потоків, але складність реалізації обмежує їх використання.

Рисунок 2.3 - Мережеві протоколи та технології

2.3 Основи та архітектура IP-телефонії: VoIP, SIP, H.323, протоколи та стандарти

IP-телефонія представляє технологію передачі голосової інформації через пакетні мережі з використанням протоколів TCP/IP. На відміну від традиційної телефонії з комутацією каналів, VoIP (Voice over IP) використовує комутацію пакетів, що забезпечує більшу ефективність використання мережевих ресурсів та інтеграцію з комп'ютерними мережами.

Архітектура VoIP (рисунок 2.4) включає кілька ключових компонентів: термінали (IP-телефони, програмні клієнти), шлюзи для з'єднання з традиційними телефонними мережами, gatekeeper або сервери реєстрації для управління викликами, та мережеву інфраструктуру для передачі голосових пакетів. Кожен компонент виконує специфічні функції в загальній архітектурі системи.

Процес цифрової обробки голосу включає аналогово-цифрове перетворення, компресію, пакетизацію, передачу через мережу, депакетизацію, декомпресію та цифрово-аналогове перетворення. Якість результуючого голосу залежить від ефективності кожного етапу та характеристик мережевої інфраструктури.

Кодеки (encoder/decoder) визначають методи компресії та декомпресії голосових сигналів. G.711 (PCM) забезпечує найвищу якість звуку з пропускною здатністю 64 кбіт/с, але без компресії. G.729 використовує компресію до 8 кбіт/с з прийнятною якістю для більшості корпоративних застосувань. G.722 забезпечує широкосмуговий звук (7 кГц) з покращеною чіткістю мови.

Протокол H.323 є однією з перших стандартизованих архітектур для мультимедійних комунікацій по IP-мережах. H.323 включає набір протоколів: H.225 для сигналізації викликів, H.245 для управління медіаканалами, RAS (Registration, Admission, Status)[10,11] для взаємодії з gatekeeper, та RTP/RTCP для передачі медіапотоків.

Архітектура H.323 передбачає кілька типів пристроїв: термінали для кінцевих користувачів, шлюзи для з'єднання з іншими мережами, MCU (Multipoint Control Unit) для групових конференцій та gatekeeper для централізованого управління. Gatekeeper виконує функції аутентифікації, авторизації, маршрутизації викликів та управління пропускною здатністю.

Session Initiation Protocol (SIP) є альтернативним підходом до сигналізації VoIP, заснованим на принципах веб-технологій. SIP використовує текстові повідомлення, подібні до HTTP, для встановлення, модифікації та завершення мультимедійних сесій. Простота та гнучкість SIP сприяли його широкому прийняттю в сучасних VoIP-системах.

Архітектура SIP включає User Agents (UA) для кінцевих пристроїв, Proxy Server для маршрутизації запитів, Registrar Server для реєстрації користувачів, Redirect Server для переспрямування запитів та Location Server для зберігання інформації про місцезнаходження користувачів. SIP використовує URI (Uniform Resource Identifier) для адресації користувачів у форматі sip:user@domain.com.

Основні методи SIP включають INVITE для встановлення сесії, ACK для підтвердження, BYE для завершення сесії, CANCEL для скасування запиту, REGISTER для реєстрації та OPTIONS для запиту можливостей. Відповіді SIP використовують коди статусу, подібні до HTTP: 1xx для інформаційних повідомлень, 2xx для успішних операцій, 3xx для переспрямування, 4xx для помилок клієнта та 5xx для помилок сервера.

Session Description Protocol (SDP) використовується в SIP для опису параметрів медіасесії, включаючи типи медіа, кодеки, IP-адреси та порти. Механізм offer/answer дозволяє учасникам сесії узгодити спільні параметри для встановлення медіаканалів.

Real-time Transport Protocol (RTP) забезпечує передачу голосових та відеоданих в реальному часі. RTP включає номери послідовності для відтворення порядку пакетів, тимчасові мітки для синхронізації та ідентифікатори джерел для розрізнення потоків. RTP зазвичай використовує

UDP як транспортний протокол для мінімізації затримок.

RTP Control Protocol (RTCP) доповнює RTP, забезпечуючи зворотний зв'язок про якість передачі, статистику втрат пакетів та інформацію про учасників сесії. RTCP дозволяє адаптивне управління якістю, включаючи зміну кодеків або налаштування параметрів передачі відповідно до умов мережі.

Secure RTP (SRTP) забезпечує шифрування та аутентифікацію RTP-потоків для захисту від прослуховування та модифікації. SRTP використовує AES для шифрування та HMAC для аутентифікації, а ключі можуть розповсюджуватися через DTLS-SRTP або ZRTP.

Механізми NAT traversal вирішують проблеми з передачею VoIP-трафіку через NAT та брандмауери. STUN (Session Traversal Utilities for NAT) дозволяє пристроям виявити свої публічні IP-адреси та типи NAT. TURN (Traversal Using Relays around NAT) забезпечує ретрансляцію трафіку через спеціальний сервер, коли прямий зв'язок неможливий.

ICE (Interactive Connectivity Establishment) комбінує STUN та TURN для оптимального вибору шляху з'єднання. ICE збирає кандидатів для з'єднання (локальні, STUN та TURN адреси) та тестує їх для знаходження найкращого маршруту.

Протоколи автоконфігурації спрощують розгортання IP-телефонів в корпоративних мережах. DHCP Option 66 та 67 дозволяють передавати адресу TFTP-сервера та ім'я конфігураційного файлу. HTTP та HTTPS можуть використовуватися для завантаження прошивки та конфігурації з централізованого сервера.

Протоколи присутності та миттєвих повідомлень розширюють можливості IP-телефонії. SIMPLE (SIP for Instant Messaging and Presence Leveraging Extensions) використовує SIP для передачі текстових повідомлень та інформації про статус користувачів. XMPP (Extensible Messaging and Presence Protocol) забезпечує федеративні комунікації між різними доменами.

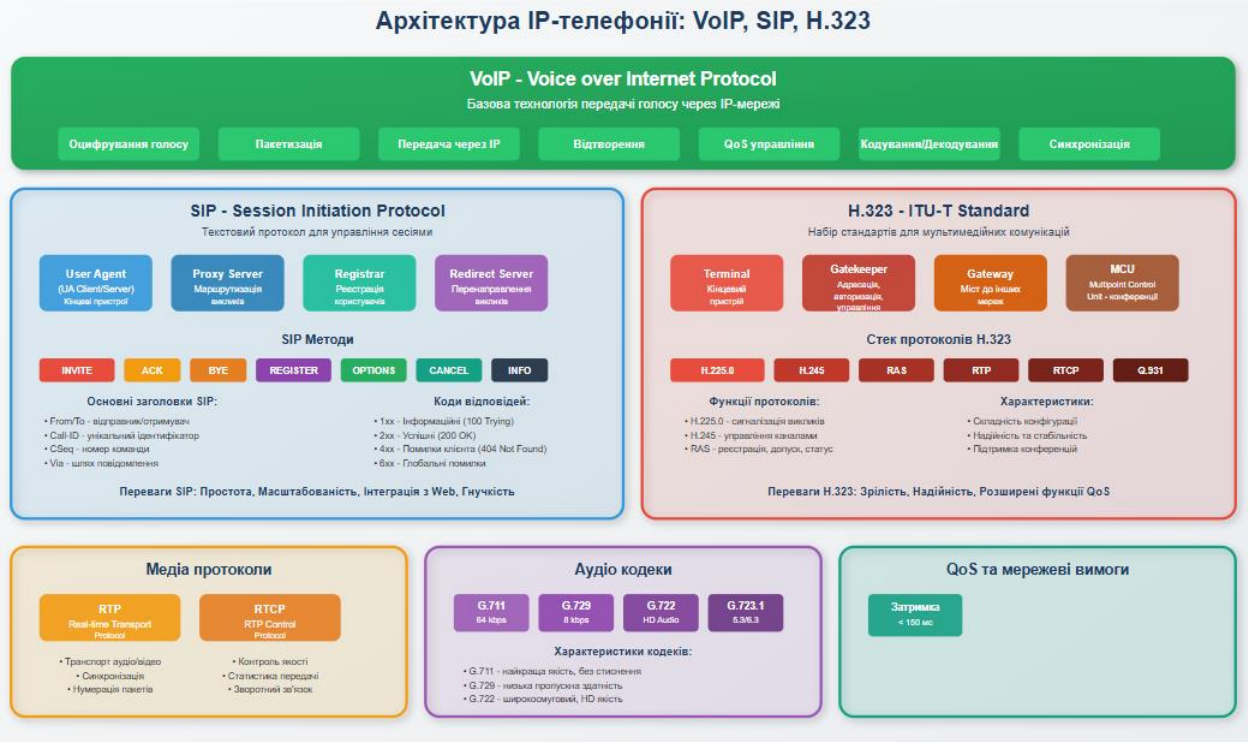

Рисунок 2.4 – Архітектура IP-телефонії: VoIP, SIP, H.323

2.4 Особливості впровадження IP-телефонії в корпоративних мережах

Впровадження IP-телефонії в корпоративних мережах вимагає комплексного підходу, що враховує технічні, організаційні та економічні аспекти. Успішна міграція від традиційної телефонії до VoIP залежить від ретельного планування мережевої інфраструктури, правильного вибору обладнання та програмного забезпечення, а також ефективного управління проектом впровадження.

Основною передумовою успішного впровадження IP-телефонії є наявність надійної мережевої інфраструктури з достатньою пропускною здатністю та низькими затримками. Голосовий трафік чутливий до затримок, джиттеру та втрат пакетів, тому мережа повинна забезпечувати стабільні параметри якості обслуговування. Рекомендована одностороння затримка для голосового трафіку не повинна перевищувати 150 мілісекунд, джиттер - 30 мілісекунд, а рівень втрат пакетів - 1%.

Планування пропускної здатності для VoIP базується на розрахунку

одночасних викликів та характеристиках використовуваних кодеків. Типовий G.711 кодек вимагає 64 кбіт/с для голосового потоку плюс накладні витрати протоколів RTP, UDP, IP та Ethernet, що в сумі становить приблизно 87 кбіт/с. G.729 кодек знижує вимоги до пропускної здатності до 31 кбіт/с включно з накладними витратами.

Архітектура мережі для IP-телефонії зазвичай включає логічне розділення голосового та даткового трафіку через VLAN. Голосовий VLAN дозволяє застосовувати специфічні політики QoS, безпеки та управління незалежно від даткового трафіку. Стандарт IEEE 802.1p забезпечує пріоритизацію голосових кадрів на канальному рівні, а DSCP маркування - на мережевому рівні.

Quality of Service (QoS) є критично важливим компонентом VoIP-інфраструктури. Голосовий трафік зазвичай маркується як Expedited Forwarding (EF) з DSCP значенням 46, що забезпечує найвищий пріоритет обслуговування. Сигналізаційний трафік (SIP, H.323) використовує клас Assured Forwarding (AF31)[12] з DSCP 26. Конфігурація QoS повинна бути послідовною на всіх мережевих пристроях від кінцевого обладнання до WAN-з'єднань.

Механізми QoS включають класифікацію та маркування трафіку, формування черг (queuing), планування (scheduling) та формування трафіку (traffic shaping). Low Latency Queuing (LLQ) забезпечує пріоритетну чергу для голосового трафіку з гарантованою пропускною здатністю та мінімальними затримками. Weighted Fair Queuing (WFQ) справедливо розподіляє залишкову пропускну здатність між іншими класами трафіку.

Безпека IP-телефонії включає захист від прослуховування, втручання в дзвінки, крадіжки сервісу та атак на доступність. Шифрування медіапотоків через SRTP захищає від перехоплення розмов. TLS для SIP-сигналізації забезпечує конфіденційність та цілісність управляючих повідомлень. IEEE 802.1X автентифікація запобігає підключенню несанкціонованих пристроїв до голосової мережі.

Firewall та NAT можуть створювати складнощі для VoIP-трафіку через динамічне призначення портів для RTP-потоків. Application Layer

3 ПРОЕКТУВАННЯ АРХІТЕКТУРИ ЛОКАЛЬНОЇ МЕРЕЖІ ДЛЯ КОЛ-ЦЕНТРУ

3.1 Розробка структурної схеми мережі та вибір мережевого обладнання

Розробка структурної схеми мережі для кол-центру компанії "CallMax" базується на детальному аналізі функціональних вимог, масштабів діяльності та перспектив розвитку. Архітектурне рішення повинно забезпечувати високу доступність, масштабованість, безпеку та оптимальну продуктивність для підтримки критично важливих телекомунікаційних сервісів у середовищі з інтенсивним навантаженням.

Структурна схема мережі базується на ієрархічній топології з трьома основними рівнями: рівень ядра (Core Layer), рівень розподілу (Distribution Layer) та рівень доступу (Access Layer). Така архітектура забезпечує логічне розділення функцій, спрощує управління та дозволяє ефективно масштабувати систему відповідно до зростання потреб організації.

Рівень ядра виконує функції високошвидкісної комутації між різними сегментами мережі та забезпечує підключення до зовнішніх мереж. Цей рівень оптимізований для максимальної пропускної здатності та мінімальних затримок, що критично важливо для голосового трафіку. Рівень ядра складається з двох комутаторів Cisco Catalyst 4500X-16SFP+, об'єднаних через 10 Gigabit Ethernet канали з використанням технології EtherChannel для агрегації пропускної здатності та забезпечення відмовостійкості.

Комутатори ядра забезпечують Layer 3 маршрутизацію між VLAN, підтримують протоколи динамічної маршрутизації (OSPF, EIGRP) та реалізують функції Hot Standby Router Protocol (HSRP) для резервування шлюзу за замовчуванням. Кожен комутатор обладнується модулями 10 Gigabit Ethernet для підключення до рівня розподілу та зовнішніх мереж.

Надлишкове живлення забезпечується через дублювання блоків живлення з підключенням до різних джерел електроенергії.

Рівень розподілу виконує агрегацію трафіку від комутаторів доступу, реалізацію політик безпеки та Quality of Service, а також забезпечує межу між рівнем доступу та ядром. Цей рівень складається з двох комутаторів Cisco Catalyst 3750X-48T-S, об'єднаних у стек через технологію FlexStack-Plus, що забезпечує пропускну здатність до 480 Гбіт/с між членами стеку та дозволяє управляти ними як єдиним логічним пристроєм.

Стекування комутаторів розподілу забезпечує автоматичне резервування та балансування навантаження без необхідності конфігурації протоколів Spanning Tree. При відмові одного з комутаторів другий автоматично перебирає на себе всі функції без переривання роботи мережі. Комутатори розподілу підтримують розширені функції QoS, включаючи класифікацію трафіку на основі DSCP, формування черг за алгоритмом Low Latency Queuing (LLQ) та пріоритизацію голосового трафіку.

Рівень доступу забезпечує підключення кінцевих пристроїв, включаючи робочі станції операторів, IP-телефони, принтери та інше периферійне обладнання. Цей рівень складається з восьми комутаторів Cisco Catalyst 2960X-48TS-L, кожен з яких забезпечує 48 портів 10/100/1000BASE-T з підтримкою Power over Ethernet Plus (PoE+) та чотири порти 1/10 Gigabit Ethernet SFP+ для аплінків до рівня розподілу.

Комутатори доступу розміщуються в комунікаційних шафах, розподілених по офісному приміщенню для мінімізації довжини горизонтального кабелювання. Кожен комутатор обслуговує 15-24 робочих місця залежно від планування офісного простору. PoE+ забезпечує електроживлення потужністю до 30 Вт на порт для IP-телефонів Cisco 7841, точок доступу Wi-Fi та інших пристроїв, що підтримують стандарт IEEE 802.3at.

Серверний сегмент виділяється в окремий логічний рівень з використанням спеціалізованого комутатора Cisco Catalyst 3560X-48T-S для

підключення серверів критично важливих додатків. Серверний комутатор забезпечує високошвидкісні з'єднання до серверів CRM-системи, IP-АТС (Cisco Unified Communications Manager), серверів баз даних, систем моніторингу та резервного копіювання.

Сервери підключаються до серверного комутатора через агреговані 1 Gigabit Ethernet канали (LACP) для підвищення пропускної здатності та забезпечення відмовостійкості. Серверний комутатор з'єднується з рівнем ядра через два незалежні 10 Gigabit Ethernet канали для забезпечення надлишковості та високої пропускної здатності для серверного трафіку.

Вибір мережевого обладнання Cisco обґрунтовується репутацією виробника в корпоративному сегменті, повною сумісністю компонентів, розширеними функціями безпеки та QoS, а також наявністю локальної технічної підтримки. Всі комутатори підтримують необхідні протоколи та стандарти для забезпечення вимог кол-центру до якості обслуговування голосового трафіку.

Периметрова безпека забезпечується брандмауером нового покоління Cisco ASA 5525-X з пропускною здатністю до 2 Гбіт/с та підтримкою до 750 VPN-з'єднань. Брандмауер інтегрує функції stateful firewall, Application Control, Intrusion Prevention System та VPN concentrator для забезпечення комплексного захисту мережі від зовнішніх загроз.

Бездротова інфраструктура реалізується через контролер бездротової мережі Cisco 2504 Wireless Controller та точки доступу Cisco Aironet 2702I з підтримкою стандарту IEEE 802.11ac Wave 1. Точки доступу забезпечують покриття всієї площі офісу для мобільності планшетів супервайзерів та гостьового доступу до інтернету. Централізоване управління через WLC спрощує конфігурацію, моніторинг та підтримку бездротової мережі.

IP-телефонія реалізується на базі платформи Cisco Unified Communications Manager (CUCM), розгорнутої на виділених серверах Dell PowerEdge R740 в конфігурації high availability з автоматичним failover. CUCM забезпечує централізоване управління всіма голосовими сервісами,

включаючи маршрутизацію викликів, автентифікацію пристроїв, застосування політик та інтеграцію з зовнішніми телефонними мережами.

Структурована кабельна система проектується на основі стандарту TIA/EIA-568-B з використанням кабелю категорії 6A для горизонтального кабелювання та багатомодового оптоволокна OM3 для вертикальних з'єднань. Горизонтальне кабелювання виконується неекранованою витою парою (UTP) Cat 6A з підтримкою швидкостей до 10 Гбіт/с на відстані до 100 метрів. Вертикальне кабелювання між рівнями мережі використовує багатомодове оптоволокно з LC коннекторами для 10 Gigabit Ethernet з'єднань.

Головний комунікаційний вузол розміщується в спеціально обладнаному приміщенні з контрольованим доступом, підтримкою температурного режиму 18-24°C та відносної вологості 45-55%, системою кондиціонування з резервуванням та автоматичною системою пожежогасіння. Комунікаційні шафи стандарту 19" обладнуються кабельними органайзерами, patch-панелями та системами управління кабелями для забезпечення акуратності та зручності обслуговування.

Система безперебійного живлення проектується з урахуванням критичності безперервної роботи кол-центру. Мережеве обладнання підключається до ДБЖ через розподільні щити з автоматичними вимикачами. ДБЖ розраховуються на забезпечення автономної роботи протягом 30 хвилин для безпечного завершення операцій та переходу на резервні джерела живлення.

Система моніторингу мережі базується на платформі SolarWinds Network Performance Monitor для централізованого контролю стану обладнання, аналізу продуктивності та автоматичного виявлення проблем. Система збирає дані через SNMP v3, аналізує тенденції використання мережевих ресурсів та генерує звіти для планування розвитку інфраструктури.

Планування розміщення обладнання враховує ергономічні вимоги,

зручність обслуговування та можливості майбутнього розширення. Комутатори доступу розміщуються в настінних комунікаційних шафах поблизу робочих зон для мінімізації довжини кабелів та спрощення обслуговування. Центральне обладнання розміщується в підлоговій комунікаційній шафі висотою 42U з достатнім простором для вентиляції та майбутнього розширення.

3.2 Планування адресного простору та сегментація мережі

Планування адресного простору та логічна сегментація мережі є фундаментальними аспектами проектування, що визначають масштабованість, безпеку та ефективність управління мережевою інфраструктурою кол-центру. Правильна організація IP-адресації та VLAN-сегментації забезпечує оптимальний розподіл ресурсів, спрощує адміністрування та створює основу для реалізації політик безпеки та якості обслуговування.

Загальна концепція адресації базується на використанні приватного діапазону IP-адрес згідно з RFC 1918, що забезпечує достатній адресний простір для поточних потреб та майбутнього розширення. Для мережі кол-центру вибрано діапазон 192.168.0.0/16, який забезпечує 65536 унікальних адрес, що значно перевищує поточні та прогнозовані потреби організації.

Ієрархічна структура адресації передбачає розподіл загального діапазону на функціональні підмережі відповідно до призначення та вимог безпеки. Третій октет IP-адреси використовується для ідентифікації функціонального призначення сегмента, що спрощує розуміння топології та управління маршрутизацією. Четвертий октет використовується для адресації конкретних пристроїв в межах сегмента.

VLAN 10 призначається для голосового трафіку з діапазоном адрес 192.168.10.0/24, що забезпечує 254 адреси для IP-телефонів та голосового обладнання. Шлюз за замовчуванням 192.168.10.1 налаштовується на

комутаторах рівня розподілу з використанням HSRP для забезпечення відмовостійкості. DHCP-сервер для голосового VLAN конфігурується з пулом адрес 192.168.10.100-192.168.10.200 з резервуванням діапазонів 192.168.10.10-192.168.10.99 для статичної адресації серверного обладнання.

Планування голосового VLAN включає конфігурацію спеціальних DHCP-опцій для автоматичного налаштування IP-телефонів. DHCP Option 150 передає адресу TFTP-сервера (192.168.30.10) для завантаження конфігураційних файлів, а Option 3 визначає адресу шлюзу за замовчуванням. Час оренди DHCP встановлюється на 24 години для забезпечення стабільності адресації голосових пристроїв.

VLAN 20 виділяється для робочих станцій операторів з діапазоном 192.168.20.0/24. Цей сегмент забезпечує 254 адреси для комп'ютерів операторів, супервайзерів та адміністративного персоналу. Шлюз за замовчуванням 192.168.20.1 конфігурується з HSRP для відмовостійкості. DHCP-пул налаштовується в діапазоні 192.168.20.100-192.168.20.200 з резервуванням статичних адрес для принт-серверів та спеціального обладнання.

Політики безпеки для даткового VLAN включають обмеження доступу до серверних ресурсів через списки контролю доступу (ACL) та інтеграцію з proxy-сервером для контрольованого доступу до інтернету. Користувачі отримують доступ лише до авторизованих ресурсів CRM-системи та корпоративних додатків відповідно до їх ролі та функціональних обов'язків.

VLAN 30 резервується для серверної інфраструктури з діапазоном 192.168.30.0/24. Серверний сегмент використовує переважно статичну адресацію для забезпечення стабільності DNS-записів та спрощення конфігурації резервного копіювання. IP-АТС (CUCM) отримує адресу 192.168.30.10, первинний CRM-сервер - 192.168.30.20, сервер баз даних - 192.168.30.30, система моніторингу - 192.168.30.40.

Серверний VLAN конфігурується з підвищеними вимогами безпеки, включаючи port security для запобігання несанкціонованому підключенню

пристроїв, DHCP snooping для захисту від шкідливих DHCP-серверів та динамічну інспекцію ARP для запобігання ARP-атакам. Доступ до серверного сегмента обмежується через ACL з дозволом лише необхідних портів та протоколів.

VLAN 40 призначається для управління мережевим обладнанням з діапазоном 192.168.40.0/24. Управлінські інтерфейси всіх комутаторів, маршрутизаторів та точок доступу отримують адреси з цього діапазону. Комутатори доступу адресуються в діапазоні 192.168.40.1-192.168.40.20, комутатори розподілу - 192.168.40.21-192.168.40.30, комутатори ядра - 192.168.40.31-192.168.40.40.

Управлінський VLAN ізолюється від користувацьких сегментів через суворі ACL та використовує окремі автентифікаційні механізми. Доступ до управлінських інтерфейсів дозволяється лише з адміністративних робочих станцій через SSH з автентифікацією на основі ключів та інтеграцією з RADIUS-сервером для централізованого управління обліковими записами.

VLAN 50 конфігурується для гостьового доступу з діапазоном 192.168.50.0/24. Гостьова мережа повністю ізолюється від корпоративних ресурсів та забезпечує лише контрольований доступ до інтернету через captive portal з автентифікацією. DHCP-сервер гостьової мережі налаштовується з коротким часом оренди (4 години) та обмеженням кількості одночасних підключень.

Міжмережева маршрутизація реалізується на комутаторах рівня розподілу з використанням протоколу OSPF для забезпечення швидкої конвергенції та автоматичного відновлення при відмовах каналів зв'язку. Вся мережа конфігурується як одна OSPF Area 0 (backbone area) для спрощення управління в умовах відносно невеликого масштабу мережі.

Статичні маршрути використовуються для направлення трафіку до зовнішніх мереж через брандмауер (192.168.1.254) з конфігурацією маршруту за замовчуванням 0.0.0.0/0. Резервні маршрути налаштовуються з вищою метрикою для автоматичного переключення на backup канали при

відмові основного інтернет-з'єднання.

Планування підмереж враховує майбутнє розширення кол-центру до 200 робочих місць з відповідним збільшенням кількості IP-телефонів та робочих станцій. Зарезервовані діапазони VLAN 11 (192.168.11.0/24) та VLAN 21 (192.168.21.0/24) дозволяють розширення голосового та даткового сегментів без зміни існуючої конфігурації.

DNS-сервери налаштовуються в режимі master/slave з первинним сервером на адресі 192.168.30.53 та вторинним на 192.168.30.54. Внутрішня DNS-зона callmax.local забезпечує розв'язання імен для всіх внутрішніх ресурсів. Форвардинг зовнішніх запитів налаштовується на публічні DNS-сервери (8.8.8.8, 8.8.4.4) через брандмауер.

DHCP-сервери налаштовуються з функціями failover для забезпечення високої доступності служби автоматичної конфігурації. Первинний DHCP-сервер розміщується на контролері домену Windows Server, вторинний - на Linux-сервері з ISC DHCP. Синхронізація між серверами забезпечує консистентність оренди адрес при відмові одного з серверів.

Сегментація безпеки реалізується через застосування різних політик доступу для кожного VLAN. Голосовий трафік отримує найвищий пріоритет QoS та обмежується взаємодією лише з IP-АТС та SIP trunk. Даткові VLAN ізолюються один від одного з контрольованим доступом до спільних ресурсів через proxy та application firewall.

Моніторинг використання адресного простору здійснюється через IPAM (IP Address Management) систему, інтегровану з DNS та DHCP серверами. Система відстежує використання IP-адрес, виявляє конфлікти та генерує звіти для планування майбутніх потреб в адресному просторі.

Документація мережевої адресації ведеться в централізованій базі даних з інформацією про призначення кожної підмережі, відповідальних осіб, дати виділення та планові зміни. Регулярний аудит використання адресного простору забезпечує актуальність документації та виявлення неефективного використання ресурсів.

3.3 Проектування системи безпеки мережі та політик доступу

Система безпеки мережі кол-центру проектується на основі концепції "захист в глибину" (defense in depth), що передбачає створення кількох рівнів захисту для забезпечення комплексної безпеки критично важливих телекомунікаційних сервісів та конфіденційних даних клієнтів. Архітектура безпеки інтегрує технічні, процедурні та організаційні заходи для мінімізації ризиків кібербезпеки та забезпечення відповідності вимогам регуляторного законодавства.

Периметрова безпека реалізується через брандмауер нового покоління Cisco ASA 5525-X, який забезпечує stateful інспекцію пакетів, контроль додатків, систему запобігання вторгненням та VPN-сервіси. Брандмауер конфігурується з трьома зонами безпеки: зовнішньою (outside) для інтернет-з'єднань, внутрішньою (inside) для корпоративної мережі та демілітаризованою зоною (DMZ) для публічних сервісів.

Політики брандмауера реалізують принцип "заборонено все, що не дозволено явно" з детальним контролем трафіку на рівні додатків. Дозволяється лише необхідний трафік для забезпечення бізнес-функцій: HTTP/HTTPS для веб-доступу, SMTP для електронної пошти, SIP для голосових сервісів та специфічні порти для CRM-системи. Весь інший трафік блокується з генерацією відповідних журнальних записів.

Система виявлення та запобігання вторгненням (IDS/IPS) інтегрується в брандмауер через модуль Cisco FirePOWER Services для забезпечення глибокої інспекції пакетів та виявлення складних атак. IPS налаштовується з базою сигнатур, що регулярно оновлюється, та конфігурується для автоматичного блокування IP-адрес при виявленні підозрілої активності. Система генерує сповіщення в реальному часі та інтегрується з SIEM-платформою для кореляції подій безпеки.

Внутрішня сегментація мережі забезпечується через VLAN та списки контролю доступу (ACL) на комутаторах рівня розподілу. Кожен VLAN

конфігурується з індивідуальними політиками безпеки відповідно до принципу найменших привілеїв. Голосовий VLAN повністю ізолюється від даткових сегментів з дозволом лише необхідного трафіку до IP-АТС та SIP trunk провайдера.

Серверний сегмент захищається додатковими рівнями безпеки, включаючи port security для запобігання несанкціонованому підключенню пристроїв, DHCP snooping для захисту від шкідливих DHCP-серверів та динамічну інспекцію ARP (DAI) для запобігання ARP spoofing атакам. Доступ до серверів обмежується через time-based ACL з дозволом адміністративного доступу лише в робочий час.

Аутентифікація користувачів та пристроїв реалізується через IEEE 802.1X з використанням сервера RADIUS на базі Cisco Identity Services Engine (ISE). Всі робочі станції операторів та мережеві пристрої повинні пройти автентифікацію перед отриманням доступу до мережі. Сертифікати машин видаються внутрішнім центром сертифікації (CA) на базі Windows Server Active Directory Certificate Services.

Система управління ідентифікацією інтегрується з Active Directory для централізованого управління обліковими записами користувачів. Політики паролів встановлюють мінімальну довжину 12 символів з використанням великих і малих літер, цифр та спеціальних символів. Облікові записи блокуються після п'яти невдалих спроб входу та автоматично розблоковуються через 30 хвилин.

Багатофакторна автентифікація (MFA) впроваджується для доступу до критично важливих систем, включаючи IP-АТС, серверну інфраструктуру та системи управління мережею. Використовується комбінація паролю та SMS-кодів або токенів з додатків автентифікації. Адміністративний доступ до мережевого обладнання вимагає обов'язкового використання MFA.

Шифрування трафіку забезпечується на кількох рівнях для захисту конфіденційної інформації. HTTPS використовується для всіх веб-додатків з сертифікатами від внутрішнього CA. TLS 1.3 конфігурується для SIP-

сигналізації між IP-телефонами та CUCM. SRTP забезпечує шифрування голосових потоків з використанням AES-128 алгоритму шифрування.

Віртуальні приватні мережі (VPN) налаштовуються для забезпечення безпечного віддаленого доступу адміністраторів та мобільних співробітників. SSL VPN реалізується через Cisco ASA з підтримкою clientless та client-based підключень. IPSec site-to-site VPN конфігурується для з'єднання з віддаленими офісами або партнерськими організаціями.

Бездротова безпека реалізується через WPA2-Enterprise з автентифікацією EAP-TLS для корпоративних пристроїв та captive portal для гостьового доступу. Корпоративна бездротова мережа використовує сертифікати для взаємної автентифікації клієнтів та точок доступу. Гостьова мережа повністю ізолюється від корпоративних ресурсів з обмеженням пропускної здатності та часу сесії.

Захист від DDoS-атак реалізується через rate limiting на брандмауері та маршрутизаторах з конфігурацією порогових значень для різних типів трафіку. Політики QoS включають захисні механізми для голосового трафіку з гарантованою пропускною здатністю та пріоритетним обслуговуванням навіть під час атак. Інтеграція з cloud-based сервісами DDoS protection забезпечує захист від великомасштабних атак.

Система журналювання централізовано збирає syslog повідомлення від всього мережевого обладнання, серверів та систем безпеки. Журнали передаються через захищені канали з використанням TLS та зберігаються на захищених серверах з контрольованим доступом. Retention політика встановлює строк зберігання журналів 12 місяців для розслідування інцидентів та аудиту відповідності.

Security Information and Event Management (SIEM) система реалізується на базі IBM QRadar для кореляції подій безпеки та автоматичного виявлення аномалій. SIEM збирає дані з брандмауера, IPS, серверів, комутаторів та операційних систем для комплексного аналізу стану безпеки. Система генерує оповіщення при виявленні підозрілої активності та автоматично

ініціює процедури реагування на інциденти.

Політики резервного копіювання включають щоденне інкрементальне копіювання конфігурацій мережевого обладнання через TFTP з шифруванням та зберіганням на захищеному сервері. Система контролю версій на базі Git відстежує зміни конфігурацій та дозволяє швидке відкочування до попередніх версій при виявленні проблем. Automated backup scripts перевіряють цілісність збережених конфігурацій та генерують сповіщення про помилки.

Система управління вразливостями здійснює регулярне сканування мережевого обладнання та серверів на предмет відомих уразливостей безпеки. Nessus або аналогічні сканери використовуються для виявлення неоновлених систем, слабких паролів та неправильних конфігурацій. Процедури patch management забезпечують своєчасне впровадження оновлень безпеки з тестуванням в лабораторному середовищі перед продуктивним впровадженням.

Контроль доступу до фізичної інфраструктури включає card-based системи доступу до серверних приміщень, відеоспостереження з записом та журналювання всіх входів. Комунікаційні шафи замикаються та обладнуються датчиками відкриття з інтеграцією до системи безпеки будівлі. Процедури escort забезпечують супроводження сторонніх осіб при доступі до критичних зон.

Incident Response Plan визначає процедури реагування на різні типи інцидентів безпеки з чіткими ролями та відповідальністю команди. Автоматичні процедури включають ізоляцію скомпрометованих систем, блокування підозрілого трафіку та сповіщення керівництва. Emergency contacts та escalation procedures забезпечують швидке залучення необхідних ресурсів для усунення критичних інцидентів.

Регулярне навчання персоналу з питань інформаційної безпеки проводиться щоквартально з акцентом на розпізнавання соціальної інженерії, безпечне використання паролів та процедури звітування про підозрілу

активність. Симуляція фішингових атак тестує готовність співробітників та виявляє потреби в додатковому навчанні.

Аудит безпеки проводиться щорічно зовнішньою компанією з перевіркою конфігурацій, аналізом журналів, тестуванням на проникнення та оцінкою відповідності індустрійним стандартам. Внутрішній аудит здійснюється щоквартально службою інформаційної безпеки з використанням автоматизованих інструментів та мануальних перевірок.

3.4 Розрахунок пропускної здатності та планування навантаження мережі

Точний розрахунок пропускної здатності та планування навантаження є критично важливими для забезпечення стабільної роботи мережі кол-центру під час пікових навантажень та майбутнього розширення. Методологія розрахунку базується на детальному аналізі типів трафіку, статистичних моделях використання, коефіцієнтах одночасності та резервуванні для забезпечення якості обслуговування.

Голосовий трафік становить найбільш критичну частину навантаження з суворими вимогами до затримок, джиттеру та втрат пакетів. Для кодеку G.711 (PCM) без компресії чистий голосовий потік становить 64 кбіт/с, але з урахуванням накладних витрат протоколів RTP (12 байт), UDP (8 байт), IP (20 байт) та Ethernet (18 байт плюс preambula 8 байт) загальне навантаження на Layer 2 досягає 87.2 кбіт/с на одну голосову сесію при розмірі пакету 20 мс.

Для кодеку G.729A з компресією до 8 кбіт/с розрахунок навантаження змінюється: payload 20 байт (8 кбіт/с * 20 мс / 8), RTP заголовок 12 байт, UDP 8 байт, IP 20 байт, Ethernet 18 байт, що дає загальне навантаження 31.2 кбіт/с на сесію. Вибір кодеку впливає на загальну пропускну здатність та якість звуку, тому для кол-центру рекомендується G.711 для внутрішніх дзвінків та G.729A для зовнішніх з'єднань.

Розрахунок одночасних голосових викликів базується на статистичному аналізі роботи кол-центру та формулах телетрафіку. При 120 операторах коефіцієнт одночасності (occupancy rate) для вхідних дзвінків становить приблизно 0.85, що означає 102 одночасних вхідних розмови в пікові години. Додатково враховуються вихідні дзвінки (коефіцієнт 0.15) та внутрішні дзвінки (коефіцієнт 0.05), що дає загальну кількість одночасних сесій близько 120-130.

З використанням G.711 кодеку загальне навантаження голосового трафіку в піковий час становить 102 × 87.2 кбіт/с = 8.9 Мбіт/с для вхідних дзвінків плюс додаткові 2-3 Мбіт/с для вихідних та внутрішніх дзвінків, що дає загалом близько 11-12 Мбіт/с. При використанні G.729A навантаження зменшується до 4-5 Мбіт/с, але за рахунок деякого погіршення якості звуку.

Трафік CRM-системи характеризується нерівномірністю з періодичними сплесками під час синхронізації даних та генерації звітів. Середнє навантаження на одне робоче місце оператора становить 50-80 кбіт/с в пікові періоди, включаючи запити до бази даних клієнтів, завантаження форм, синхронізацію статусів та обмін повідомленнями. При 120 робочих місцях та коефіцієнті одночасності 0.9 загальне навантаження CRM-трафіку становить 5.4-8.6 Мбіт/с.

Веб-трафік операторів включає доступ до корпоративних порталів, систем документообігу, онлайн-навчання та обмежений доступ до інтернету. Середнє навантаження становить 20-40 кбіт/с на робоче місце з періодичними сплесками до 200-500 кбіт/с під час завантаження великих файлів або відео. При коефіцієнті одночасності 0.6 загальне навантаження веб-трафіку досягає 1.4-2.9 Мбіт/с з піковими значеннями до 12-15 Мбіт/с.

Трафік електронної пошти має асинхронний характер з нерівномірним розподілом протягом дня. Середнє навантаження становить 5-15 кбіт/с на користувача з періодичними сплесками до 100-200 кбіт/с під час синхронізації великих вкладень. Exchange Server генерує додатковий трафік для синхронізації Outlook клієнтів та мобільних пристроїв. Загальне

навантаження email-трафіку оцінюється в 0.6-1.8 Мбіт/с з піковими значеннями до 6-8 Мбіт/с.

Серверний трафік включає обмін даними між CRM-серверами, серверами баз даних, файловими серверами та системами резервного копіювання. Внутрішньосерверний трафік може досягати 100-500 Мбіт/с під час операцій резервного копіювання, синхронізації баз даних або міграції віртуальних машин. Для забезпечення ізоляції серверний сегмент потребує виділених високошвидкісних з'єднань 1-10 Гбіт/с.

Трафік управління мережею включає SNMP-запити, syslog-повідомлення, оновлення конфігурацій, синхронізацію часу та моніторинг стану обладнання. Хоча обсяг цього трафіку відносно невеликий (0.5-2 Мбіт/с), його критично важливо ізолювати в окремому VLAN для забезпечення безпеки та стабільності управління мережею.

Бездротовий трафік генерується мобільними пристроями супервайзерів, планшетами для обходів та гостьовими підключеннями. Корпоративний Wi-Fi використовується для доступу до CRM-системи з планшетів (10-30 кбіт/с на пристрій) та VoIP-дзвінків з мобільних додатків (50-90 кбіт/с на сесію). Гостьова мережа обмежується 2 Мбіт/с на користувача з максимум 20 одночасних підключень.

Розрахунок загального навантаження на мережу для поточної конфігурації 120 робочих місць показує пікове значення 17-25 Мбіт/с при використанні G.711 кодеку або 12-18 Мбіт/с з G.729A. З урахуванням планованого розширення до 200 робочих місць навантаження зросте до 28-42 Мбіт/с (G.711) або 20-30 Мбіт/с (G.729A).

Планування пропускної здатності каналів між рівнями мережі базується на агрегованому навантаженні з урахуванням коефіцієнта oversubscription. Рівень доступу потребує аплінків 1 Гбіт/с до рівня розподілу для забезпечення достатньої пропускної здатності при коефіцієнті oversubscription 20:1 (48 портів × 100 Мбіт/с / 1 Гбіт/с × 2 аплінки).

Рівень розподілу з'єднується з рівнем ядра через 10 Гбіт/с канали для

забезпечення агрегації трафіку від восьми комутаторів доступу. EtherChannel з двох 10 Гбіт/с каналів забезпечує сумарну пропускну здатність 20 Гбіт/с з автоматичним балансуванням навантаження та відмовостійкістю.

WAN-канали плануються на основі зовнішнього трафіку та вимог до якості обслуговування. Інтернет-канал 200 Мбіт/с забезпечує достатню пропускну здатність для веб-трафіку, електронної пошти та віддаленого доступу з резервом для зростання. SIP trunk для зовнішніх дзвінків потребує гарантованої пропускної здатності 6-8 Мбіт/с для 100 одночасних викликів з G.729A кодеком.

Моделювання навантаження використовує статистичні моделі для прогнозування пікових значень трафіку. Розподіл Пуассона застосовується для моделювання надходження дзвінків, а експоненціальний розподіл - для тривалості розмов. Monte Carlo симуляція показує, що 95-й перцентиль навантаження становить приблизно 80-85% від теоретичного максимуму.

QoS планування забезпечує пріоритизацію критично важливого трафіку через класифікацію та маркування пакетів. Голосовий трафік маркується як Expedited Forwarding (EF) з DSCP 46, сигналізаційний трафік - як Assured Forwarding AF31 (DSCP 26), CRM-трафік - як AF21 (DSCP 18), а загальний інтернет-трафік залишається Best Effort.

Планування використання портів комутаторів враховує поточні потреби та майбутнє розширення. Комутатори доступу з 48 портами використовуються на 60-70% для забезпечення гнучкості при переміщенні робочих місць. Резервування 30-40% портів дозволяє розширення без додавання нового обладнання в короткостроковій перспективі.

Capacity planning включає регулярний моніторинг використання мережевих ресурсів через SNMP та аналіз трендів зростання. Quarterly reviews аналізують статистику використання портів, завантаження каналів та продуктивність обладнання для планування майбутніх інвестицій в інфраструктуру.

Планування disaster recovery враховує backup канали та альтернативні

маршрути трафіку при відмові основних компонентів. Резервний інтернет-канал 100 Мбіт/с від альтернативного провайдера забезпечує мінімальну функціональність при відмові основного каналу. Backup SIP trunk дозволяє переключення голосового трафіку на альтернативного оператора зв'язку.

Performance baselines встановлюються для всіх критично важливих метрик мережі, включаючи затримки, джиттер, втрати пакетів та використання пропускної здатності. Automated monitoring генерує оповіщення при відхиленні від baseline значень та ініціює процедури troubleshooting.

Stress testing мережі проводиться під час планового обслуговування для перевірки поведінки під екстремальними навантаженнями. Traffic generators симулюють пікові навантаження для валідації QoS політик та виявлення вузьких місць в архітектурі.

4 РЕАЛІЗАЦІЯ ТА КОНФІГУРАЦІЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

4.1 Встановлення та налаштування мережевого обладнання

З метою побудови сучасної, надійної та масштабованої мережі для кол-центру були використані різні категорії мережевого обладнання, кожна з яких виконує свої ключові функції у загальній архітектурі інфраструктури.

На рівні ядра мережі встановлено два потужних комутатори Cisco Catalyst 4500X-16SFP+, які виконують функції центральних маршрутизаторів та комутаторів. Вони забезпечують високошвидкісну маршрутизацію між усіма VLAN у корпоративній мережі, підтримують агрегування трафіку від різних сегментів та підключення до зовнішніх мережевих каналів. Ці пристрої оптимізовані для обробки критичного голосового та сервісного трафіку, забезпечують мінімальні затримки й високу надійність завдяки резервуванню каналів і функціям Hot Standby Router Protocol (HSRP), а також підтримці протоколів OSPF, EIGRP та технології EtherChannel.

Для реалізації рівня розподілу мережі використано два комутатори Cisco Catalyst 3750X-48T-S, які працюють у стеку. Вони виконують агрегацію трафіку з комутаторів доступу, дозволяють впроваджувати політики безпеки та якісного обслуговування (QoS), а також забезпечують ізоляцію різних сегментів мережі. Завдяки стекуванню ці пристрої здатні автоматично резервувати та балансувати навантаження, підвищуючи загальну відмовостійкість мережі.

На рівні доступу встановлено вісім комутаторів Cisco Catalyst 2960X-48TS-L, які розміщені у комунікаційних шафах поблизу робочих зон офісу. Ці пристрої підключають кінцеві користувацькі пристрої, такі як IP-телефони, комп’ютери операторів, принтери та інше периферійне обладнання. Вони підтримують технологію Power over Ethernet Plus (PoE+), що дає змогу живити IP-телефони та точки доступу без додаткових блоків

живлення, а також мають гігабітні аплінки для зв’язку з рівнем розподілу.

Для підключення серверної інфраструктури використовується окремий комутатор Cisco Catalyst 3560X-48T-S, який забезпечує надійні й швидкі з’єднання серверів ключових бізнес-додатків (CRM, IP-АТС, бази даних, резервне копіювання, моніторинг). До цього комутатора сервери підключаються через агреговані канали для підвищення пропускної здатності та забезпечення резервування. Далі серверний трафік йде до ядра через два незалежні 10-гігабітні канали.

Безпека периметра мережі реалізується за допомогою сучасного брандмауера Cisco ASA 5525-X, який виконує глибоку інспекцію трафіку, контролює зовнішні з’єднання, блокує несанкціоновані спроби доступу, інтегрує системи захисту від вторгнень (IDS/IPS) і VPN. Це дозволяє комплексно захищати корпоративну мережу від зовнішніх та внутрішніх загроз, фільтрувати додатки й організовувати безпечні канали зв’язку.

Для організації корпоративної бездротової мережі застосовано централізований контролер Cisco 2504 Wireless Controller та точки доступу Cisco Aironet 2702I, які забезпечують розгортання, моніторинг і підтримку корпоративного Wi-Fi, а також гостьового доступу. Таке рішення дає можливість мобільним пристроям співробітників стабільно підключатися до мережі з будь-якої точки офісу.

Платформа IP-телефонії працює на виділених серверах Dell PowerEdge R740, які розгортають рішення Cisco Unified Communications Manager. Ця система дає змогу централізовано управляти всіма голосовими сервісами, маршрутизацією викликів, політиками доступу та інтеграцією з зовнішніми телефонними мережами.

Для моніторингу мережевої інфраструктури використовується система SolarWinds Network Performance Monitor. Вона забезпечує централізоване збирання статистики, спостереження за станом пристроїв, аналіз продуктивності мережі та автоматичне виявлення проблем.

Інтегровану систему управління безпекою на базі IBM QRadar (SIEM)

впроваджено для кореляції подій безпеки, аналізу журналів і автоматичного реагування на інциденти в мережі.

Критичне мережеве обладнання, сервери та комунікаційні шафи підключаються до систем безперебійного живлення (ДБЖ, UPS), які дозволяють забезпечити стабільну роботу мережі навіть у разі перебоїв з електропостачанням.

Всі фізичні підключення здійснюються за допомогою структурованої кабельної системи на основі неекранованої витої пари категорії 6A (UTP) для горизонтальних з'єднань, а також багатомодового оптоволокна OM3 для вертикальних каналів між поверхами та комунікаційними шафами. Для організації простору та акуратного розміщення обладнання використовуються patch-панелі, кабельні органайзери й стандартні комунікаційні шафи (19", 42U).

Загалом, весь цей комплекс обладнання був підібраний для того, щоб забезпечити стабільну, масштабовану, захищену і зручну в обслуговуванні корпоративну мережу з максимальними можливостями резервування й підтримкою сучасних вимог до якості обслуговування, безпеки і майбутнього розширення.

Після встановлення обладнання проводиться його фізичне з'єднання: зовнішній канал Інтернет-провайдера підключається до WAN-порту маршрутизатора, а локальні сегменти, призначені для користувацьких пристроїв і телефонії, до окремих LAN-портів EdgeRouter. Далі відбувається підключення комутатора, до якого під'єднуються стаціонарні комп'ютери операторів, сервери, точки доступу Wi-Fi та IP-телефони. Для підвищення безпеки і керованості мережі реалізовано сегментацію за допомогою віртуальних локальних мереж (VLAN): зокрема, трафік IP-телефонії виділяється в окрему підмережу, що дозволяє застосовувати політики якості обслуговування (QoS) та уникати перешкод у роботі голосових сервісів.

Початкова конфігурація мережевих пристроїв здійснюється через web-інтерфейс, SSH або консольний доступ. EdgeRouter X, який слугує

центральним маршрутизатором, налаштовується згідно з вимогами проєкту. На інтерфейс WAN призначається автоматичне отримання IP-адреси від провайдера, а на локальний інтерфейс LAN – статична адреса, наприклад, 192.168.10.1/24. Для організації окремої підмережі телефонії на порту LAN налаштовується VLAN з ідентифікатором 20 та IP-адресою 192.168.20.1/24. Це досягається відповідними командами в CLI EdgeRouter (лістинг 4.1).

Лістинг 4.1 - Налаштовування VLAN з ідентифікатором 20

```
bash
configure
set interfaces ethernet eth0 address dhcp
set interfaces ethernet eth1 address 192.168.10.1/24
set interfaces ethernet eth1 vif 20 address 192.168.20.1/24
set vlans Voice vlan-id 20
commit
save
exit
```

Важливим етапом є також налаштування базових політик безпеки. Для захисту мережі застосовуються фаєрволи (лістинг 4.2), які блокують усі вхідні з'єднання з Інтернету, крім дозволених портів, необхідних для роботи телефонії, зокрема UDP-порт 5060 для SIP-трафіку.

Лістинг 4.2 – Налаштування фаєрволу

```
bash
set firewall name WAN_IN default-action drop
set firewall name WAN_IN rule 10 action accept
set firewall name WAN_IN rule 10 protocol udp
set firewall name WAN_IN rule 10 destination port 5060
commit
save
```

Далі здійснюється базове налаштування NAT (лістинг 4.3) (Network Address Translation), щоб забезпечити локальним пристроям вихід до Інтернету через один зовнішній IP-адрес.

Лістинг 4.3 – Налаштування NAT

```
bash
```

```
set service nat rule 5000 type masquerade
set service nat rule 5000 outbound-interface eth0
commit
save
```

Після конфігурування маршрутизатора переходять до налаштування комутатора TP-Link, де через web-інтерфейс створюються необхідні VLAN та виконується їх прив'язка до відповідних портів. Наприклад, порти 1–16 можуть бути віднесені до VLAN 10 (користувацькі пристрої), а порти 17–24 — до VLAN 20 (телефонія). Це дозволяє фізично розділити мережевий трафік навіть на рівні дротової інфраструктури.

Наступним кроком є налаштування точок доступу Wi-Fi. Для цього використовують централізований контролер UniFi Controller, через який створюються дві бездротові мережі (SSID): одна для співробітників кол-центру (наприклад, "CallMax-Staff", VLAN 10), інша — для пристроїв голосового зв'язку (наприклад, "CallMax-Voice", VLAN 20). Для кожної мережі задаються відповідні параметри безпеки, такі як WPA2-Enterprise для персоналу та WPA2-PSK для пристроїв IP-телефонії.

Завершальним етапом у даному розділі є підключення IP-телефонів і VoIP-шлюзів. Вони розміщуються у відповідному сегменті VLAN Voice і налаштовуються на отримання мережевих параметрів через DHCP, після чого для кожного пристрою задаються адреси SIP-сервера та реєстраційні дані. Таким чином, побудована інфраструктура дозволяє централізовано керувати мережевими пристроями, забезпечувати їхню працездатність, гнучко масштабувати інфраструктуру відповідно до зростаючих потреб компанії та гарантовано дотримуватися сучасних стандартів корпоративної безпеки та продуктивності.

4.2 Конфігурація мережевих протоколів та служб

Після фізичного розгортання та початкового налаштування мережевого обладнання важливим етапом є налаштування мережевих протоколів і служб,

які забезпечують коректну взаємодію всіх елементів інфраструктури, ефективну маршрутизацію, автоматичне надання IP-адрес, належний розподіл мережевих ресурсів і якісну роботу IP-телефонії. Систематичний підхід до конфігурації протоколів дозволяє створити масштабовану, безпечну і стабільну мережу.

Основою функціонування сучасної корпоративної мережі є динамічне надання мережевих параметрів пристроям за допомогою протоколу DHCP. На центральному маршрутизаторі EdgeRouter X одночасно налаштовується кілька DHCP-серверів (лістинг 4.4) для різних сегментів мережі. Для підмережі користувачів з адресним простором 192.168.10.0/24 встановлюється пул видачі IP-адрес у межах 192.168.10.100–192.168.10.200, а також вказується шлюз і основний DNS-сервер. Аналогічно, для сегменту телефонії (VLAN Voice) з підмережі 192.168.20.0/24 виділяється пул 192.168.20.50–192.168.20.150 з відповідним шлюзом 192.168.20.1.

Лістинг 4.4 – Конфігурація DHCP для кожного сегменту

```
bash
set service dhcp-server shared-network-name LAN1 subnet
192.168.10.0/24 start 192.168.10.100 stop 192.168.10.200
set service dhcp-server shared-network-name LAN1 subnet
192.168.10.0/24 default-router 192.168.10.1
set service dhcp-server shared-network-name LAN1 subnet
192.168.10.0/24 dns-server 8.8.8.8
set service dhcp-server shared-network-name Voice subnet
192.168.20.0/24 start 192.168.20.50 stop 192.168.20.150
set service dhcp-server shared-network-name Voice subnet
192.168.20.0/24 default-router 192.168.20.1
set service dhcp-server shared-network-name Voice subnet
192.168.20.0/24 dns-server 8.8.8.8
commit
save
```

Реалізація якісного розподілу трафіку в мережі передбачає налаштування VLAN на комутаторах. Через web-інтерфейс TP-Link TL-SG1024DE створюються окремі VLAN, які дозволяють фізично і логічно розділити трафік користувачів та голосових сервісів. Наприклад, VLAN 10 використовується для робочих місць співробітників, а VLAN 20 — для

пристроїв IP-телефонії. Для кожного порту комутатора визначається належність до певної VLAN, що забезпечує ізоляцію трафіку, захист від потенційних внутрішніх загроз та мінімізує перешкоди для голосового трафіку. У web-інтерфейсі вказується, які порти входять до складу кожного VLAN, а також чи є вони trunk чи access-портами.

Важливою складовою мережевої інфраструктури є правильна організація служби імен. Задля підвищення відмовостійкості, у налаштуваннях DHCP як основний DNS-сервер вказується публічний адресний простір (наприклад, 8.8.8.8 Google DNS), а за наявності локальної доменної інфраструктури (Active Directory) — адреса локального DNS, що дозволяє швидше знаходити внутрішні ресурси.

Наступним етапом є налаштування бездротової мережі через UniFi Controller, де для кожного SSID встановлюються параметри безпеки, тип аутентифікації та VLAN-ID. Це дозволяє автоматично розподіляти користувачів і пристрої по різних підмережах, не порушуючи єдину логіку корпоративної безпеки.

З метою забезпечення стабільної роботи телефонної підсистеми впроваджується підтримка QoS (лістинг 4.5). На маршрутизаторі та комутаторі задаються параметри пріоритетності трафіку для SIP-протоколу і RTP-потоків, що дозволяє мінімізувати затримки, втрати пакетів та забезпечує високу якість голосових викликів навіть у періоди пікового навантаження.

Лістинг 4.5 – Налаштування QoS через пріоритизацію UDP-пакетів з портами 5060 і 10000-20000.

```
bash
set traffic-policy shaper VOIP bandwidth 10mbit
set traffic-policy shaper VOIP class 10 match SIP ip protocol
udp
set traffic-policy shaper VOIP class 10 match SIP destination
port 5060
set traffic-policy shaper VOIP class 20 match RTP ip protocol
udp
set traffic-policy shaper VOIP class 20 match RTP destination
```

```
port 10000-20000
commit
save
```

Також доцільно впровадити резервування основних служб, наприклад, шляхом використання другого DNS-сервера чи альтернативного маршруту до Інтернету. Це підвищує надійність і стійкість мережі до збоїв та атак. Для зовнішньої доступності і контролю за роботою критичних служб застосовується базова діагностика: регулярний ping шлюзу, перевірка доступності DNS та моніторинг відповідей DHCP.

У підсумку, правильно налаштовані мережеві протоколи й сервіси формують надійну основу для роботи всієї корпоративної інфраструктури, забезпечуючи автоматизацію процесів, підвищення безпеки і стабільності мережі, гнучкість управління та можливість масштабування системи у разі росту компанії.

4.3 Налаштування системи моніторингу та управління мережею

Ефективне функціонування сучасної корпоративної мережі неможливе без впровадження централізованої системи моніторингу, яка дозволяє в реальному часі відстежувати стан обладнання, якість мережевого з'єднання, завантаженість каналів та своєчасно реагувати на потенційні проблеми. У межах реалізації інфраструктури кол-центру в якості основної системи моніторингу було обрано Zabbix — популярну open-source платформу, яка підтримує інтеграцію через SNMP, дозволяє контролювати велику кількість пристроїв різних виробників, генерувати інформативні дашборди, графіки й налаштовувати гнучкі оповіщення для адміністратора.

Встановлення серверної частини Zabbix (лістинг 4.6) відбувається на окремому сервері під управлінням Linux, зазвичай Ubuntu Server. Основні етапи інсталяції включають оновлення системи, встановлення необхідних пакетів, налаштування БД та запуск служби Zabbix.

Лістинг 4.6 – Встановлення Zabbix

```
bash
sudo apt update
sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-
apache-conf zabbix-agent
sudo systemctl start zabbix-server zabbix-agent apache2
sudo systemctl enable zabbix-server zabbix-agent apache2
```

Після цього у web-інтерфейсі Zabbix (лістинг 4.7) створюється адміністративний обліковий запис, а далі здійснюється додавання мережевого обладнання для моніторингу. Для збору статистики про стан мережі, навантаження портів, використання пропускної здатності, на EdgeRouter X активується SNMP-сервер наступною командою.

Лістинг 4.7 – Створюється адміністративний обліковий запис в Zabbix

```
bash
set service snmp community public authorization ro
commit
save
```

Аналогічно SNMP налаштовується на керованих комутаторах і точках доступу. Наприклад, для TP-Link TL-SG1024DE у web-інтерфейсі активується SNMP, задається community string (наприклад, “public”) та дозволяється доступ до SNMP-агента з IP-адреси сервера Zabbix. Це дозволяє системі автоматично виявляти пристрої, збирати показники трафіку з кожного порту, відслідковувати події перевантаження, підрахунок помилок та зміни топології.

Особливу увагу приділено організації тригерів і оповіщень. У Zabbix для кожного пристрою налаштовуються правила, які спрацьовують при досягненні критичних значень — наприклад, при втраті зв’язку із маршрутизатором, перевищенні навантаження на порт, зростанні кількості помилок чи відсутності відповіді від DHCP чи DNS-сервера. Для інформування адміністратора про критичні події впроваджується система e-mail або Telegram-оповіщень, що забезпечує миттєве реагування на аварії.

Сучасні можливості Zabbix дозволяють також виводити агреговані графіки завантаження каналів, історії інцидентів та відстеження тенденцій росту мережі.

Для моніторингу бездротової мережі та централізованого управління точками доступу використовується UniFi Controller, який розгортається як на фізичному сервері, так і у вигляді хмарної служби. За допомогою цього контролера адміністратор отримує доступ до карти розташування точок, може відслідковувати підключення клієнтів у реальному часі, дистанційно оновлювати прошивки, змінювати налаштування SSID, VLAN чи політик доступу без фізичної присутності в серверній.

Сукупно система моніторингу дає змогу не лише фіксувати поточний стан мережі, а й аналізувати історію збоїв, виконувати проактивне планування модернізації та масштабування, оперативно реагувати на атаки або спроби несанкціонованого доступу. Всі ці заходи дозволяють забезпечити надійну, безпечну й ефективну роботу мережевої інфраструктури кол-центру на кожному етапі її функціонування, а також гарантувати безперервність бізнес-процесів навіть у разі виникнення несподіваних технічних проблем.

4.4 Інтеграція VoIP-обладнання та телефонної системи

Інтеграція VoIP-обладнання та впровадження телефонної системи є важливим етапом розгортання корпоративної мережі кол-центру, оскільки саме від коректної роботи голосових сервісів залежить продуктивність операторів, якість обслуговування клієнтів та можливість ефективної взаємодії між відділами. Реалізація IP-телефонії базується на використанні протоколу SIP та сучасних програмних платформ, зокрема Asterisk або Issabel, а також спеціалізованого обладнання — IP-телефонів Grandstream GXP1625 і аналогових VoIP-шлюзів Grandstream HT813, що дозволяє інтегрувати традиційні телефонні лінії у єдину цифрову систему.

Початковий етап інтеграції полягає у фізичному підключенні IP-телефонів та VoIP-шлюзів до виділеного сегменту мережі, що реалізований через VLAN Voice. Пристрої отримують IP-адреси автоматично завдяки налаштованому раніше DHCP-серверу у підмережі 192.168.20.0/24. На кожному телефоні або шлюзі через web-інтерфейс вказуються реквізити для підключення до SIP-сервера: його IP-адреса (наприклад, 192.168.20.2), SIP-ідентифікатор, пароль та інші параметри аутентифікації. Додатково активується підтримка QoS — встановлюються DSCP-пріоритети для SIP-сигнального трафіку (порт 5060) та RTP-голосових потоків (порти 10000–20000), що суттєво підвищує якість дзвінків навіть при піковому завантаженні мережі.

Наступним кроком є розгортання програмної платформи телефонії. Найчастіше для таких завдань використовується сервер Asterisk (лістинг 4.8), який інсталюється на виділену віртуальну або фізичну машину під управлінням Linux.

Лістинг 4.8 – Встановлення Asterisk

```
bash
sudo apt update
sudo apt install asterisk
```

Після встановлення платформи налаштовується основний конфігураційний файл для SIP-клієнтів (лістинг 4.9), розташований у /etc/asterisk/sip.conf. Для кожного оператора чи пристрою створюється окремий обліковий запис із визначенням пароля, типу реєстрації та контексту, у якому буде здійснюватись обробка дзвінків. Наприклад, для співробітника з внутрішнім номером 2001 запис має вигляд.

Лістинг 4.9 – файл для SIP-клієнтів

```
ini
[2001]
type=friend
context=internal
```

```
secret=VerySecretPass
host=dynamic
```

Створюється також діалплан у /etc/asterisk/extensions.conf, який задає маршрутизацію викликів усередині компанії, а також визначає обробку вхідних дзвінків через інтерактивне голосове меню (IVR). Наприклад, усі дзвінки на номер 2100 можуть спрямовуватись у загальну чергу підтримки, де виклик приймає перший вільний оператор. Для обслуговування зовнішніх викликів налаштовується інтеграція із аналоговими лініями через шлюз HT813, у якому прописується відповідний обліковий запис SIP.

Для тестування телефонної системи кожен співробітник отримує свій внутрішній номер та реєструє свій пристрій у системі через web-інтерфейс IP-телефона. Після реєстрації оператор може виконати вихідний дзвінок на будь-який інший внутрішній номер, а також приймати виклики ззовні або від клієнтів компанії. Додатково впроваджується IVR, який дозволяє автоматично розподіляти дзвінки: клієнт, який зателефонував на загальний номер, чує запис із вибором відділу — натисканням відповідної цифри дзвінок автоматично спрямовується на вільного оператора потрібної групи.

З метою забезпечення контролю якості роботи телефонії у системі налаштовується запис розмов, ведення статистики по кожному оператору, а також автоматизований моніторинг активності пристроїв. Завдяки інтеграції з системою моніторингу Zabbix адміністратор може відслідковувати статус реєстрації телефонів, рівень пропускної здатності для голосового трафіку та вчасно реагувати на спроби несанкціонованого підключення.

Загалом, впроваджена система IP-телефонії на базі відкритих стандартів та сучасного обладнання забезпечує високу якість зв’язку, гнучкість масштабування та підтримку сучасних сценаріїв — черги викликів, IVR, конференц-зв’язок, багатоканальні номери, інтеграцію із CRM-системою та іншими корпоративними платформами. Всі ці можливості суттєво підвищують ефективність роботи персоналу кол-центру, забезпечують зручність для клієнтів та дозволяють оперативно адаптуватися

до змін бізнес-процесів без додаткових фінансових витрат на сторонні телефонні сервіси.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було вирішено актуальну задачу проектування та впровадження сучасної локальної комп’ютерної мережі для кол-центру компанії «CallMax», що дозволяє забезпечити високий рівень надійності, продуктивності та масштабованості інформаційної інфраструктури. В ході дослідження здійснено комплексний аналіз поточного стану мережевої інфраструктури, виявлено основні проблеми, пов’язані із застарілістю обладнання, недостатньою пропускною здатністю, відсутністю сучасних засобів захисту та обмеженими можливостями масштабування.

Розглянуто сучасні технології побудови корпоративних мереж, протоколи IP-телефонії, принципи побудови ієрархічної архітектури та підходи до забезпечення якості обслуговування для голосового і даткового трафіку. На основі аналізу функціональних і технічних вимог запропоновано оптимальну архітектуру локальної мережі з виділенням сегментів VLAN, централізованим управлінням, реалізацією комплексної системи безпеки та впровадженням механізмів моніторингу й автоматизованого резервного копіювання.

Особливу увагу приділено питанням інформаційної безпеки — запропоновано застосування багаторівневого захисту, шифрування даних, контролю доступу та систем виявлення вторгнень, що відповідає сучасним стандартам та вимогам щодо захисту персональних даних клієнтів. Для підвищення стійкості інфраструктури передбачено використання протоколів швидкого відновлення, резервування критично важливих компонентів і впровадження безперебійного живлення.

У практичній частині роботи реалізовано проєкт мережі на базі ієрархічної топології, проведено розрахунки пропускної здатності, розроблено схему IP-адресації, здійснено налаштування обладнання,

впроваджено систему моніторингу та централізованого управління. Проведено інтеграцію IP-телефонної платформи з автоматичним розподілом дзвінків, записом розмов і можливістю подальшої інтеграції з корпоративною CRM-системою.

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/