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 “Астраїлс Груп”

(тема)

Виконав:
здобувач 3 року навчання,
групи КІУКІу-22-2
Дмитро ЧУМАК
(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: ст. викл Артем ГУК
(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 Чумаку Дмитру Сергійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Локальна комп’ютерна мережа кол-центру компанії “Астраїлс Груп”

затверджена наказом по університету від “ 26 ” травня 2025 р. № 425 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 14 липня 2025 р.

3. Вхідні дані до роботи

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

4. Перелік питань, що потрібно опрацювати у роботі

1. Аналіз предметної області та технічних вимог до мережі кол-центру
2. Теоретичні основи проєктування мереж кол-центрів та сучасні технології
3. Проєктування локальної мережі кол-центру
4. Активне мережеве обладнання

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій 13 слайдів

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

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

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Аналіз проблеми та огляд існуючих рішень 1	10.06.25 – 13.06.25	
2	Вибір технології розробки та	14.06.25 – 17.06.25	
	інструментальних засобів		
3	Розробка алгоритмічного забезпечення	18.06.25 – 21.06.25	
4	Розробка програмних модулів	23.06.25 – 28.06.25	
5	Відлагодження програмних модулів	30.06.25 – 02.07.25	
6	Оформлення матеріалів кваліфікаційної роботи	03.07.25 – 05.07.25	
7	Подання кваліфікаційної роботи керівникові та	07.07.25 – 09.07.25	
	її попередній захист		
8	Подання кваліфікаційної роботи на рецензу-	10.07.25 – 11.07.25	
	вання		

Дата видачі завдання " 09 " червня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ ст. викл Артем ГУК
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 67 с., 8 рис., 0 табл., 1 дод., 10 джерел

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

Метою кваліфікаційної роботи є проектування та наукове обґрунтування оптимальної архітектури локальної комп’ютерної мережі кол-центру компанії "Астраїлс Груп" для тридцяти операторських робочих місць із врахуванням сучасних вимог до продуктивності, відмовостійкості та інформаційної безпеки.

У ході виконання кваліфікаційної роботи проведено комплексний аналіз особливостей функціонування контакт-центрів, визначено специфічні вимоги до мережевої інфраструктури, досліджено структуру та характеристики основних типів трафіку, а також розглянуто вплив сучасних трендів цифровізації й зростання кіберзагроз на підходи до організації корпоративних мереж. На основі системного аналізу сучасних протоколів і мережевого обладнання розроблено науково обґрунтовану ієрархічну модель мережі, оптимізовану для одночасної роботи тридцяти операторів із підтримкою VoIP-телефонії, інтегрованих CRM-систем, моніторингу якості обслуговування та гарантованою захищеністю персональних даних.

ABSTRACT

Bachelor’s thesis: 67 pages, 8 figures, 0 tables, 1 appendix, 10 references.

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

The aim of the bachelor’s thesis is to design and scientifically substantiate the optimal architecture of a local computer network for the "Astrails Group" call center, intended to support thirty operator workstations, taking into account modern requirements for performance, fault tolerance, and information security. During the thesis, a comprehensive analysis of the operational features of contact centers was conducted, specific requirements for the network infrastructure were identified, the structure and characteristics of the main types of traffic were studied, and the influence of current digitalization trends and the growing scale of cyber threats on corporate network design approaches was considered. Based on a systematic analysis of modern protocols and network equipment, a scientifically justified hierarchical network model was developed, optimized for the simultaneous operation of thirty operators with support for VoIP telephony, integrated CRM systems, quality of service monitoring, and guaranteed protection of personal data.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ACL – список контролю доступу (англ., Access Control List)

API – програмний інтерфейс застосування (англ., Application Programming Interface)

ARP – протокол визначення адрес (англ., Address Resolution Protocol)

AS – автономна система (англ., Autonomous System)

BGP – протокол прикордонного шлюзу (англ., Border Gateway Protocol)

BYOD – політика використання особистих пристроїв (англ., Bring Your Own Device)

Cat5e/Cat6A – кабель категорії 5e/6A для структурованої кабельної системи

CIDR – безкласова маршрутизація (англ., Classless Inter-Domain Routing)

CLI – інтерфейс командного рядка (англ., Command-Line Interface)

CoS – клас сервісу (англ., Class of Service)

CRM – система управління відносинами з клієнтами (англ., Customer Relationship Management)

CTI – комп’ютерна інтеграція телефонії (англ., Computer Telephony Integration)

DHCP – протокол динамічного налаштування хостів (англ., Dynamic Host Configuration Protocol)

DNS – система доменних імен (англ., Domain Name System)

DSCP – код точки диференційованого сервісу (англ., Differentiated Services Code Point)

EIGRP – розширений внутрішній протокол шлюзу (англ., Enhanced Interior Gateway Routing Protocol)

FCR – показник першого вирішення звернення (англ., First Call Resolution)

FTP – протокол передачі файлів (англ., File Transfer Protocol)

HD – відео високої чіткості (англ., High Definition)

HR – відділ кадрів (англ., Human Resources)

HSRP – протокол резервування шлюзу (англ., Hot Standby Router Protocol)

HTTP/HTTPS – протокол передачі гіпертексту / захищений HTTP (англ., Hypertext Transfer Protocol / Secure HTTP)

IGMP – інтернет-груповий протокол управління (англ., Internet Group Management Protocol)

IP – інтернет-протокол (англ., Internet Protocol)

IP-PBX – приватна телефонна станція на основі IP (англ., IP Private Branch Exchange)

IPSec – протокол захисту мережевого рівня (англ., IP Security)

L2/L3 – канальний / мережевий рівень (англ., Layer 2 / Layer 3)

LACP – протокол агрегації каналів (англ., Link Aggregation Control Protocol)

MAC – апаратна адреса мережевого інтерфейсу (англ., Media Access Control Address)

MTBF – середній час безвідмовної роботи (англ., Mean Time Between Failures)

NAS – мережеве сховище даних (англ., Network Attached Storage)

NAT – перетворення мережевих адрес (англ., Network Address Translation)

OSPF – протокол найкоротшого шляху першим (англ., Open Shortest Path First)

PC – персональний комп'ютер (англ., Personal Computer)

PoE/PoE+ – передача живлення по Ethernet (англ., Power over Ethernet)

PIM – незалежний від протоколу мультикаст (англ., Protocol Independent Multicast)

QoS – якість обслуговування (англ., Quality of Service)

RIP – протокол інформації маршрутизації (англ., Routing Information Protocol)

RSTP – протокол швидкої перебудови дерева (англ., Rapid Spanning Tree Protocol)

SaaS – програмне забезпечення як послуга (англ., Software as a Service)

SDN – програмно-визначена мережа (англ., Software-Defined Networking)

SIP – протокол ініціації сеансів (англ., Session Initiation Protocol)

SLA – угода про рівень обслуговування (англ., Service Level Agreement)

SNMP – протокол простого управління мережею (англ., Simple Network Management Protocol)

SSH – захищений мережевий протокол (англ., Secure Shell)

SSID – ідентифікатор бездротової мережі (англ., Service Set Identifier)

STP – протокол розгалуженого дерева (англ., Spanning Tree Protocol)

TCP – протокол керування передачею (англ., Transmission Control Protocol)

TCP/IP – стек протоколів TCP/IP

TFTP – простий протокол передачі файлів (англ., Trivial File Transfer Protocol)

UDP – протокол датаграм користувача (англ., User Datagram Protocol)

UPS – джерело безперебійного живлення (англ., Uninterruptible Power Supply)

VLAN – віртуальна локальна мережа (англ., Virtual Local Area Network)

VPN – віртуальна приватна мережа (англ., Virtual Private Network)

VRF – віртуальний маршрутизатор (англ., Virtual Routing and Forwarding)

VRRP – протокол резервування віртуальних маршрутизаторів (англ., Virtual Router Redundancy Protocol)

VoIP – передача голосу по IP (англ., Voice over IP)

ВСТУП

У сучасному бізнес-середовищі контактні центри набувають стратегічного значення для підвищення якості клієнтського обслуговування та забезпечення сталого розвитку компаній на конкурентному ринку. Рівень ефективності роботи кол-центру безпосередньо корелює з надійністю та продуктивністю його інформаційно-технологічної інфраструктури, фундаментальним елементом якої виступає локальна комп’ютерна мережа. З огляду на динамічне зростання обсягів клієнтських звернень, впровадження інноваційних цифрових технологій та посилення вимог до якості сервісу, компанія "Астраїлс Груп", основним профілем діяльності якої є клієнтська підтримка, стикається з об’єктивною необхідністю модернізації власної мережевої інфраструктури. Вказані трансформації передбачають створення масштабованої, відмовостійкої та безпечної локальної мережі, здатної підтримувати безперебійну роботу тридцяти операторських робочих місць із гарантуванням високої доступності сервісів, мінімізації затримок обробки запитів та безперервного функціонування ключових бізнес-додатків.

Особливості функціонування сучасних контакт-центрів формують специфічні технічні вимоги до мережевої інфраструктури. Передусім це забезпечення стабільної роботи VoIP-телефонії, підтримка інтегрованих CRM-систем і сервісів моніторингу якості обслуговування, а також гарантія захищеності персональних даних клієнтів у відповідності до актуальних регуляторних вимог. Додатково, вплив глобальних трендів цифровізації бізнес-процесів і наростання масштабів кіберзагроз обумовлюють необхідність інтеграції сучасних механізмів мережевої безпеки, підвищуючи вимоги до стійкості та ефективності архітектури корпоративних мереж.

Дана кваліфікаційна робота здійснюється в рамках реалізації освітньої програми підготовки бакалаврів за спеціальністю «Комп’ютерна інженерія» і відображає науково-дослідну тематику кафедри, орієнтовану на розробку

інноваційних рішень для корпоративних мережевих інфраструктур. Сформульовані завдання відповідають актуальним вітчизняним і міжнародним напрямкам досліджень у сфері мережевих технологій, а саме: проектуванню конвергентних мереж для мультимедійних сервісів, оптимізації мережевої інфраструктури для критичних бізнес-додатків, впровадженню механізмів забезпечення якості обслуговування (QoS) та інтеграції сучасних засобів мережевої безпеки. Окремий інтерес викликає кореляція цієї роботи з поточними дослідженнями щодо проєктування інфраструктури для контакт-центрів та її оптимізації, що розробляється у провідних технічних закладах країни.

Головною метою дослідження є проектування та наукове обґрунтування оптимальної архітектури локальної комп’ютерної мережі кол-центру "Астраїлс Груп" із розрахунком на тридцять операторських робочих місць, із урахуванням специфічних вимог до продуктивності, відмовостійкості й інформаційної безпеки. Для досягнення цієї мети у роботі передбачено виконання послідовного комплексу завдань, що охоплює аналіз сучасних підходів до проєктування мереж кол-центрів, вивчення особливостей функціонування компанії, визначення як функціональних, так і нефункціональних вимог до мережевої інфраструктури, розрахунок необхідної пропускної здатності та моделювання мережевого трафіку з урахуванням одночасної роботи операторів, трафіку VoIP, взаємодії з CRM-системами та іншими корпоративними додатками. У процесі дослідження здійснюється обґрунтований вибір топології та специфікація необхідного обладнання (комутатори, маршрутизатори, точки бездротового доступу), проектується структурна схема мережі з врахуванням масштабованості й відмовостійкості, а також розробляється комплексна система захисту із впровадженням сучасних методів сегментації, контролю доступу й протидії кіберзагрозам. Завершальним етапом є техніко-економічне обґрунтування інвестицій у модернізацію мережі та формування практичних рекомендацій з її впровадження й подальшого обслуговування.

Об’єктом дослідження виступають процеси проєктування та експлуатації локальних комп’ютерних мереж для кол-центрів, а предметом — методологічні й технологічні підходи, що дозволяють створити ефективну мережеву інфраструктуру для підтримки критично важливих сервісів (VoIP, CRM, моніторинг якості) на тридцять робочих місць. Застосовані у дослідженні методи включають системний аналіз для комплексного дослідження архітектурних рішень, порівняльний аналіз актуальних мережевих технологій та обладнання, математичне моделювання для розрахунку пропускної здатності й прогнозування продуктивності, а також техніко-економічний аналіз і застосування сучасних індустріальних стандартів мережевого проектування.

Наукова новизна одержаних результатів полягає в адаптації принципів проєктування корпоративних мереж до потреб контакт-центрів малого та середнього масштабу, у розробці методики розрахунку пропускної здатності із врахуванням особливостей трафіку (VoIP, CRM, web-запити), а також у визначенні оптимального співвідношення продуктивності, надійності та економічної ефективності мережевого рішення для організацій даного сегменту. Окремо підкреслюється інтеграція сучасних підходів до мережевої безпеки, спрямованих на забезпечення конфіденційності та цілісності клієнтських даних.

Практичне значення дослідження визначається можливістю безпосереднього впровадження запропонованих технічних і організаційних рішень у діяльність компанії "Астраїлс Груп", а також їхньою придатністю до використання в інших організаціях зі схожим профілем. Напрацьовані результати можуть бути використані системними інтеграторами як референтна модель для проєктування інфраструктури кол-центрів, а також слугувати практичною основою для підготовки студентів за напрямом корпоративних мереж у профільних навчальних закладах та для оптимізації мережевих інфраструктур у підприємствах сфери послуг.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ТЕХНІЧНИХ ВИМОГ ДО МЕРЕЖІ КОЛ-ЦЕНТРУ

1.1 Характеристика компанії "Астраїлс Груп" та аналіз бізнес-процесів

Компанія "Астраїлс Груп" була заснована у 2018 році як спеціалізований провайдер послуг клієнтської підтримки та аутсорсингу контакт-центрів. Від моменту свого заснування вона змогла посісти стійку позицію на ринку BPO-послуг України, поступово розширюючи свою діяльність на країни Східної Європи. Формування бізнесу компанії тісно пов’язане з розвитком цифрової економіки та стрімким зростанням попиту на якісне клієнтське обслуговування, що стало визначальним чинником для обрання ринкової ніші—надання професійних сервісів кол-центру малому та середньому бізнесу, який не мав змоги розвивати власні відділи клієнтської підтримки. Ключову роль у становленні компанії відіграли засновники, що володіли значним досвідом у сферах телекомунікацій і IT.

Основними напрямками діяльності "Астраїлс Груп" є організація вхідної та вихідної телефонії, технічна підтримка IT-продуктів, консультування клієнтів із питань використання програмного забезпечення, а також забезпечення супроводу для електронної комерції. Компанія фокусується на обслуговуванні клієнтів у фінансовій, IT-сфері, електронній комерції та телекомунікаціях, що формує її спеціалізовану експертизу. На ринку клієнтської підтримки "Астраїлс Груп" характеризується як стабільний і динамічно зростаючий гравець, який охоплює близько 3% українського сегменту BPO-послуг із річним оборотом близько 2,5 мільйона доларів США. Основними конкурентами виступають провідні компанії галузі, серед яких "Корпорація УВК", "Global Bilgi", "DataArt Contact Center" та декілька локальних постачальників. Клієнтська база компанії налічує понад 45 постійних корпоративних клієнтів із України, Польщі, Румунії та країн

Балтії. Середній розмір контракту складає 15–20 тисяч доларів на рік, а середня тривалість співпраці перевищує два роки.

Компанія демонструє стійкі темпи зростання: щорічний приріст клієнтської бази складає 25–30%, а обсяги наданих послуг зростають на 35–40%. Це зумовлено як розширенням існуючих контрактів, так і активним залученням нових клієнтів шляхом рекомендацій та ефективної маркетингової діяльності.

Організаційна структура "Астраїлс Груп" побудована за функціональним принципом із чіткою ієрархією управління, що включає чотири основні департаменти—операційний, технічний, комерційний і адміністративно-фінансовий. Генеральний директор координує роботу всіх підрозділів. Операційний департамент є найбільшим і охоплює кол-центр із 30 робочими місцями, відділ контролю якості та навчання персоналу. Структура кол-центру організована за трирівневою моделлю, що включає операторів першої лінії, експертів другої лінії й супервайзерів. Технічний департамент складається з IT-відділу й служби підтримки клієнтів, комерційний охоплює відділи продажів і маркетингу, а адміністративно-фінансовий—бухгалтерію, HR та загальне адміністрування.

Бізнес-модель компанії базується на аутсорсингових підходах із комбінацією оплати "pay-per-service" та фіксованих щомісячних платежів. Найвагомішу частку доходів складають послуги телефонії, технічної підтримки, консультування та додаткових сервісів (email-підтримка, чат-боти). Ключовими партнерами компанії є великі телекомунікаційні провайдери, постачальники CRM та workforce management-систем, а також рекрутингові агентства.

До стратегічних цілей "Астраїлс Груп" на найближчі роки належать розширення клієнтської бази до 75 компаній, збільшення штату операторів до 50 осіб, впровадження AI-технологій для автоматизації рутинних операцій і вихід на ринки Центральної Європи. Відповідно до планів розвитку компанія інвестує у модернізацію IT-інфраструктури, сертифікацію за

міжнародними стандартами якості та створення власних цифрових продуктів для малого бізнесу.

Основу операційної діяльності складають процеси обробки вхідних дзвінків клієнтів, яких щодня надходить від 800 до 1200, а під час пікових навантажень—до 1800. Середня тривалість дзвінка—4,5 хвилини, а час очікування у черзі не перевищує 30 секунд у переважній більшості випадків. Обробка кожного дзвінка включає автоматичну ідентифікацію клієнта, маршрутизацію дзвінка на основі навичок і спеціалізації операторів, відображення клієнтської інформації у CRM-системі, роботу за стандартизованими скриптами та документування результатів.

Маршрутизація виконується за допомогою технології ACD із застосуванням skill-based routing, що дозволяє оптимально розподіляти дзвінки за компетенціями та пріоритетами клієнтів. Для VIP-клієнтів передбачений окремий канал із мінімальним часом очікування.

Другим за значимістю напрямом діяльності є технічна підтримка, яка включає складніші сценарії обробки запитів із більш тривалою взаємодією. Вирішення інцидентів передбачає багаторівневу діагностику, ескалацію до експертів другої лінії та детальне документування у базі знань компанії.

Робота з CRM-системою на базі Salesforce забезпечує повний доступ операторів до історії взаємодій із клієнтом, автоматичний облік контактів, створення і ведення follow-up завдань та оновлення даних у режимі реального часу. Інтеграція CRM із телефонною платформою дозволяє фіксувати всі дзвінки та пов’язувати їх із відповідними записами у базі даних.

Щомісяця у CRM-системі опрацьовується понад 25 тисяч записів про взаємодію з клієнтами, створюється близько 1 500 нових лідів та оновлюється інформація по 8 000 контактах. Активна база даних охоплює понад 15 тисяч клієнтів компаній-замовників.

Контроль якості обслуговування та система звітності інтегровані у всі бізнес-процеси. Якість оцінюється шляхом автоматичного запису дзвінків,

вибіркового аналізу розмов, регулярного оцінювання операторів і проведення навчальних сесій. Всі показники роботи вимірюються за стандартизованими критеріями: дотримання скриптів, точність інформації, професійність спілкування, ефективність вирішення проблем і відповідність процедурним вимогам. Мінімальні цільові показники якості встановлені на рівні 85%.

Система звітності забезпечує автоматичне формування аналітики для управління та клієнтів компанії. Основні метрики включають обсяг оброблених дзвінків, середній час обробки, рівень задоволеності клієнтів, показники FCR і дотримання SLA. Доступ до ключових показників забезпечується через веб-портал у вигляді персоналізованих дашбордів.

Всі процеси компанії орієнтовані на безперервне вдосконалення, що забезпечується регулярним аналізом показників, впровадженням коригувальних заходів, оновленням процедур та навчальних матеріалів, а також активним використанням зворотного зв’язку від клієнтів для підвищення якості сервісу.

1.2 Структура кол-центру та аналіз робочих місць операторів

Кол-центр компанії "Астраїлс Груп" розрахований на 30 робочих місць та має багаторівневу операційну структуру, що дозволяє ефективно обслуговувати клієнтів різних напрямків. Основну частину персоналу становлять оператори першої лінії, які приймають і обробляють стандартні звернення, а також спеціалізовані групи підтримки — технічної, фінансової та електронної комерції. Другий рівень складають експерти, що вирішують складні технічні та профільні питання, а управління командою здійснюють супервайзери, відповідальні за якість роботи й координацію операторів. Організаційна ієрархія забезпечує чіткий розподіл ролей, ефективну комунікацію та контроль виконання стандартів сервісу.

Робота організована у змінному графіку, щоб забезпечити покриття у робочі та вихідні дні відповідно до потреб клієнтів. Розклад формують на

основі даних workforce management-системи, що враховує динаміку дзвінків і сезонні коливання. Автоматизована система маршрутизації дзвінків ACD з елементами штучного інтелекту направляє запити до відповідних спеціалістів з урахуванням складності, спеціалізації та поточного навантаження операторів.

Кожне робоче місце обладнане сучасною комп'ютерною технікою із двома моніторами, професійною гарнітурою з шумозаглушенням і VoIP-телефоном з підтримкою PoE. Операційною системою є Windows 10 Pro з централізованим керуванням через домен Active Directory. Додаткове оснащення для експертів і супервайзерів включає веб-камери для відеозв'язку, планшети для мобільного доступу до систем та інструменти для візуалізації даних.

Програмне забезпечення включає інтегровану CRM-систему Salesforce, телефонну платформу Asterisk із комп'ютерною інтеграцією (CTI), рішення для підтримки віддаленого доступу та управління тікетами, засоби для внутрішньої комунікації й документообігу. Всі розмови операторів автоматично записуються, що дає змогу здійснювати якісний контроль, проводити навчання й аудит роботи.

Робочі місця облаштовані згідно з вимогами ергономіки та безпеки, із сучасними меблями, системою освітлення, кондиціонування та шумоізоляції. Просторове зонування open-space забезпечує ізольованість функціональних груп і ефективну взаємодію з керівниками. Така організація простору та технічна база створюють умови для стабільної роботи кол-центру, підтримки високої якості сервісу та масштабованості бізнесу.

1.3 Аналіз поточного стану IT-інфраструктури компанії

Поточна мережева інфраструктура компанії "Астраїлс Груп" була впроваджена у 2019 році та базується на ієрархічній топології із застарілими компонентами. Центральний комутатор Cisco Catalyst 2960-X виконує роль

ядра та точки розподілу, до якого підключаються три комутатори доступу— два Cisco Catalyst 2960-L для робочих місць операторів і один D-Link DGS-1100-24 для допоміжного обладнання. Сервери підключені напряму до центрального комутатора, при цьому відсутня окрема серверна VLAN, що підвищує ризики безпеки.

Обладнання має неоднорідні характеристики і обмежені можливості для подальшого масштабування: підключення комутаторів доступу до центрального вузла здійснюється через одинарні Gigabit Ethernet-лінки, що створює вузькі місця при пікових навантаженнях. У години підвищеної активності використання каналів сягає 70–85% їх пропускної здатності, що призводить до затримок доступу до серверів та погіршення якості VoIP-з’єднань.

Система не має резервування ключових компонентів — уся мережа залежить від одного центрального комутатора, що є єдиною точкою відмови. Відсутня централізована система моніторингу, що ускладнює вчасне виявлення проблем та управління інфраструктурою. Додатково, використання кабельної інфраструктури категорії 5e не дозволяє підтримувати сучасні високошвидкісні стандарти, обмежуючи модернізацію мережі у майбутньому.

1.4 Сучасні підходи до проектування мереж кол-центрів та технологічні тренди

Архітектура мереж сучасних кол-центрів відрізняється від класичних корпоративних рішень через високі вимоги до обробки трафіку й безперервності бізнес-процесів. Основу інфраструктури складає конвергентна IP-мережа, яка поєднує голос, відео й дані, підтримує багатоканальні комунікації та дозволяє інтегрувати додаткові сервіси без складної модернізації. Для кол-центрів критично важливими є мінімальні затримки для голосового трафіку, висока доступність сервісів, надійна

інтеграція з CRM-системами та можливість масштабування відповідно до змін бізнесу. Мережа проектується на трирівневій архітектурі з чітким розділенням ролей: рівень доступу підключає операторів і забезпечує базову безпеку, розподільний рівень відповідає за агрегацію трафіку, політики QoS та VLAN-сегментацію, а рівень ядра забезпечує швидкісний транспорт між сегментами й зовнішніми підключеннями. На всіх рівнях впроваджують резервування каналів і вузлів, використовують стекові комутатори й сучасні протоколи швидкої конвергенції. Якість сервісу для критичних додатків гарантують завдяки гнучкому налаштуванню QoS — голос отримує найвищий пріоритет і захист від затримок, відео-трафік масштабують під реальні навантаження, а CRM-трафік забезпечують стабільною пропускною здатністю. Модульна архітектура та віртуалізація мережевих функцій дозволяють швидко розширювати мережу, а програмно-визначені мережі (SDN) і автоматизоване налаштування значно спрощують адміністрування та масштабування. В сучасних рішеннях активно впроваджують хмарні сервіси, edge computing, елементи штучного інтелекту для аналітики трафіку та моделі zero-trust для комплексного захисту інфраструктури.

У сфері IP-телефонії стандартом є SIP, який забезпечує просту інтеграцію різних пристроїв, масштабованість та підтримку голосових, відео й текстових сервісів. Його переваги — легкість налаштування, модульність і гнучкість, проте цей протокол потребує додаткового захисту та спеціальних рішень для проходження NAT. У деяких організаціях ще використовують H.323, однак SIP поступово витісняє його завдяки простоті та адаптивності до сучасних вимог. Архітектура IP-телефонії для кол-центрів базується на використанні SIP-сервера або IP-PBX, медіашлюзів для зв'язку із традиційними телефонними мережами, контролерів безпеки й платформ для інтеграції з CRM та запису розмов. Все частіше функціонал IP-телефонії частково або повністю переноситься у хмару, що спрощує масштабування, знижує витрати та дозволяє швидко впроваджувати нові сервіси.

Інтеграція із CRM-системами здійснюється через CTI-протоколи, API

та автоматичний обмін даними, що дозволяє значно підвищити ефективність роботи операторів і забезпечити персоналізований підхід до клієнтів. Новітні рішення дозволяють використовувати аналітику й штучний інтелект для предиктивної маршрутизації, автоматичного збору статистики та підвищення якості обслуговування.

Для забезпечення безпеки даних і надійності бізнес-процесів використовуються багаторівневі стратегії резервного копіювання: локальні бекапи, віддалені копії та хмарні сервіси. Всі критичні дані (розмови, CRM, налаштування, журнали) дублюються з урахуванням мінімальних показників часу відновлення та втрати інформації. Сучасні стратегії резервування комбінують швидкі локальні бекапи, автоматизовану відправку у хмару та гнучкі сценарії аварійного відновлення, що дозволяє забезпечити безперервність роботи кол-центру навіть у випадку серйозних інцидентів.

1.5 Формування технічних вимог до локальної мережі кол-центру

Функціональні вимоги до мережевої інфраструктури. Підтримка одночасної роботи 30 операторів. Забезпечення якісного VoIP-зв'язку без затримок. Інтеграція з CRM-системами та базами даних клієнтів. Підтримка систем моніторингу та запису розмов. Нефункціональні вимоги: продуктивність та надійність. Вимоги до пропускної здатності та затримок мережі. Показники доступності системи (uptime 99.9%). Масштабованість для майбутнього розширення. Відмовостійкість критичних компонентів. Вимоги до безпеки та захисту інформації. Захист персональних даних клієнтів. Сегментація мережі та контроль доступу. Системи виявлення та запобігання вторгненням. Політики резервного копіювання та відновлення даних. Вимоги до інтеграції та сумісності. Інтеграція з зовнішніми системами клієнтів. Сумісність з обладнанням різних виробників. Підтримка стандартних протоколів та інтерфейсів. Можливості для майбутньої модернізації.

Економічні та експлуатаційні вимоги. Обмеження бюджету на мережеву інфраструктуру. Вимоги до простоти управління та обслуговування. Енергоефективність та екологічність рішень. Планування операційних витрат на 3-5 років.

2 ТЕОРЕТИЧНІ ОСНОВИ ПРОЕКТУВАННЯ МЕРЕЖ КОЛ-ЦЕНТРІВ ТА СУЧАСНІ ТЕХНОЛОГІЇ

2.1 Принципи проектування мережевої інфраструктури для кол-центрів

Проєктування мережевої інфраструктури для кол-центрів ґрунтується на ключових принципах, що гарантують надійність, масштабованість та ефективність функціонування всієї системи, враховуючи специфічні потреби інтенсивного оброблення комунікаційного трафіку і високу вимогу до безперервної роботи сервісів. Відмінністю від типових корпоративних рішень є фокус на мінімізації затримок, забезпеченні стійкості до відмов і здатності мережі адаптуватися до швидкої зміни бізнес-навантаження.

Один із базових принципів — забезпечення прогнозованої продуктивності мережі. Для критичних сервісів (зокрема VoIP і систем реального часу) потрібно гарантувати фіксовані показники затримки, джитеру і втрат пакетів. Для цього проводиться детальний розрахунок пропускної здатності, впроваджується якісна політика QoS і резервуються ресурси під пріоритетний трафік.

Відмовостійкість є ще одним фундаментальним принципом: резервування впроваджується на всіх рівнях — від дублювання мережевого обладнання і каналів зв’язку до використання кількох незалежних маршрутів передавання даних. Важливою складовою є можливість автоматичного перемикання (seamless failover), особливо для голосових сервісів, що мають працювати без пауз навіть у разі аварій.

Масштабованість у проєктуванні означає здатність поступово розширювати інфраструктуру без значної перебудови: для цього застосовується модульний підхід, ієрархічна структура з чітко визначеними межами відповідальності та впровадження стандартизованих технологій і протоколів. Це дозволяє оперативно підключати нові робочі місця, сегменти

мережі або додаткові сервіси.

Безпека інформації є ключовим фактором, оскільки в мережі кол-центру обробляються як персональні дані клієнтів, так і критично важлива бізнес-інформація. Архітектура мережі має забезпечувати логічну сегментацію трафіку, багаторівневий контроль доступу, шифрування даних і комплексний моніторинг стану безпеки.

Конвергенція трафіку — ще одна характерна риса сучасних рішень, адже голосові, відео- й інформаційні сервіси об’єднуються в єдину IP-мережу. Це оптимізує використання ресурсів і спрощує управління, але вимагає чіткого планування політик QoS і розподілу смуги пропускання відповідно до типу трафіку.

Керованість інфраструктури досягається впровадженням централізованих систем моніторингу та управління, уніфікованих підходів до конфігурації обладнання, системного ведення журналів і автоматизації рутинних процесів для зниження людського чинника і спрощення адміністрування.

Не менш важливим є економічний підхід: проєктування має враховувати оптимальне співвідношення витрат і продуктивності, розглядати повний життєвий цикл інфраструктури — від початкових інвестицій до обслуговування, модернізацій і ліцензування програмного забезпечення.

Типова ієрархічна архітектура мережі кол-центру включає три рівні: ядро (core), розподілення (distribution) та доступ (access). Ядро відповідає за високошвидкісне з’єднання між сегментами мережі й зовнішніми каналами, має мінімальні затримки, максимальну пропускну здатність і резервування для уникнення простоїв. Рівень розподілення агрегує трафік, реалізує політики безпеки й QoS, здійснює маршрутизацію між VLAN та підключає ключові сервіси — сервери, сховища, інтернет-шлюзи. Рівень доступу забезпечує підключення робочих місць операторів, телефонів і точок бездротового доступу, має високу щільність портів та впроваджує базову безпеку й автентифікацію користувачів.

Сучасні підходи доповнюють класичну модель впровадженням спрощеної (collapsed core) архітектури для невеликих кол-центрів, spine-and-leaf топологій для дата-центрів і використанням програмно-визначених мереж (SDN) для централізованого управління політиками та швидкої автоматизації змін.

2.2 Технології комутації та маршрутизації в мережах кол-центрів

Технології комутації та маршрутизації в мережах кол-центрів є основою їхньої надійності, гнучкості й ефективності. На канальному рівні (Layer 2) основою залишається стандарт Ethernet із підтримкою сучасних функцій, що дозволяють сегментувати мережу, запобігати петлям і підвищувати пропускну здатність. Одним з ключових рішень є впровадження VLAN — віртуальних локальних мереж, які дають змогу логічно розділяти трафік незалежно від фізичної топології, ізолювати голосовий і користувацький трафік, виділяти адміністративні сегменти та захищати гостьовий доступ. Використання Voice VLAN дозволяє ізолювати VoIP-трафік і гарантувати йому потрібний рівень пріоритету, тоді як окремі VLAN для робочих місць, адміністрування та гостьового доступу забезпечують безпеку й керованість.

Стандарт IEEE 802.1Q визначає механізм VLAN-тегування, що дозволяє одному фізичному з’єднанню передавати трафік декількох VLAN одночасно і підтримувати цілісність логічної структури на всій довжині мережі. У великих або провайдерських мережах використовуються розширені механізми 802.1ad і 802.1ah для глибшої ізоляції та масштабування.

Для запобігання петлям у Layer 2 мережах застосовують протокол Spanning Tree (STP) та його сучасні варіації — Rapid Spanning Tree Protocol (RSTP), який значно пришвидшує час перебудови мережі у разі відмови каналу, та Multiple Spanning Tree Protocol (MSTP), який дозволяє балансувати

навантаження між кількома інстанціями для різних VLAN. Це підвищує стійкість і оптимізує використання смуги пропускання в мережі.

Ще одним важливим рішенням є агрегація каналів — об’єднання кількох фізичних лінків у єдиний логічний канал (LAG) через протокол LACP або статичну конфігурацію. Це дозволяє збільшити пропускну здатність між вузлами доступу, ядром і серверами, а також забезпечити резервування на випадок виходу з ладу окремого кабелю.

На третьому рівні (Layer 3) впроваджується маршрутизація між VLAN, підключення до Інтернету, обробка трафіку між філіями або дата-центрами, балансування навантаження між провайдерами. У простих мережах можна використовувати статичну маршрутизацію, однак для динамічного розподілу трафіку та адаптації до змін топології доцільніше застосовувати динамічні протоколи маршрутизації.

Серед динамічних протоколів у корпоративних мережах найпоширенішим є OSPF, який забезпечує швидке сходження, масштабованість і підтримку змінних масок підмереж. У мережах на обладнанні Cisco може використовуватися EIGRP, який вирізняється гнучкою маршрутизацією, швидким реагуванням на зміни й автоматичною агрегацією маршрутів.

Для підключення до Інтернету й організації зв’язку з кількома провайдерами використовується BGP — протокол, що дозволяє управляти маршрутами на основі політик, забезпечує автоматичне перемикання при відмові провайдера та дає змогу оптимізувати маршрутизацію в глобальних мережах.

У складних мережах важливо коректно налаштовувати взаємодію між різними протоколами маршрутизації (redistribution), використовуючи фільтрацію маршрутів і маршрутні карти для запобігання петлям і нераціональній маршрутизації.

Для забезпечення відмовостійкості шлюзів використовуються протоколи VRRP або HSRP, які створюють віртуальний шлюз із

автоматичним перемиканням на резервний пристрій у разі відмови основного. Це дозволяє уникнути втрати зв'язку для кінцевих пристроїв навіть у разі збоїв на рівні маршрутизаторів.

Рисунок 2.1 – Технології комутації та маршрутизації в мережах кол-центрів

2.3 Мережеві протоколи та стандарти передачі даних

2.3.1. Сімейство протоколів TCP/IP

Протокольний стек TCP/IP є основою сучасних комп'ютерних мереж і мережі Інтернет. Його розробка почалася в 1970-х роках у рамках проєкту ARPANET і з часом еволюціонувала до універсального стандарту мережевої взаємодії. У локальних мережах кол-центрів TCP/IP забезпечує надійну, масштабовану й ефективну передачу даних між різними пристроями та застосунками. Архітектура TCP/IP базується на чотирирівневій моделі, що включає рівень додатків, транспортний рівень, мережевий рівень і рівень доступу до мережі. Кожен рівень виконує свої функції й взаємодіє з іншими

через стандартизовані інтерфейси.

Рівень додатків забезпечує взаємодію між мережевими сервісами та користувацькими застосунками. На ньому працюють протоколи HTTP і HTTPS для веб-сервісів, FTP для передачі файлів, SMTP для електронної пошти, DNS для розв'язання імен, DHCP для автоматичного налаштування параметрів, SNMP для управління обладнанням. У кол-центрі цей рівень особливо важливий, оскільки тут працюють SIP для встановлення й завершення IP-телефонних сесій, RTP та RTCP для передачі голосових і відеоданих у реальному часі. CRM-системи використовують HTTP/HTTPS і API, а протоколи доступу до баз даних забезпечують роботу з корпоративними сховищами.

Транспортний рівень відповідає за надійну передачу даних між застосунками. TCP як протокол з установленням з'єднання гарантує доставку даних, упорядкування пакетів і контроль перевантажень, що особливо важливо для CRM-систем, тікет-сервісів та веб-додатків. UDP не встановлює з'єднання, має мінімальні накладні витрати й забезпечує швидку доставку, що ідеально для IP-телефонії та DNS-запитів, де важлива швидкість і допускаються втрати окремих пакетів.

Мережевий рівень реалізується протоколом IP, який виконує адресацію та маршрутизацію пакетів. IPv4 використовує 32-бітні адреси й підтримує CIDR, а в локальних мережах застосовують приватні діапазони з NAT для виходу в Інтернет. IPv6 використовує 128-бітні адреси, має вбудовані механізми безпеки та підтримку автоматичної конфігурації. Перехід на IPv6 відбувається поступово, сучасне обладнання часто підтримує одночасно IPv4 і IPv6, що спрощує міграцію. ICMP використовується для діагностики й передачі повідомлень про помилки, а утиліти ping і traceroute допомагають моніторити доступність і діагностувати проблеми.

Рівень доступу до мережі забезпечує взаємодію з фізичними технологіями, такими як Ethernet, Wi-Fi чи PPP. Він відповідає за інкапсуляцію IP-пакетів у кадри канального рівня та їх передачу фізичним

середовищем. Механізми якості сервісу реалізуються через поля ToS або Traffic Class, а DiffServ класифікує трафік і задає правила його обробки. У кол-центрах QoS критично важливий для пріоритету голосового трафіку, надання пропускної здатності для CRM-сервісів та обмеження фонових процесів. Безпека TCP/IP забезпечується через IPSec для шифрування й аутентифікації на мережевому рівні, SSL/TLS для безпечного транспорту веб-даних і роботу міжмережевих екранів, які фільтрують трафік за IP-адресами, портами та правилами.

2.3.2 Протоколи канального рівня (Ethernet, Wi-Fi)

Протоколи канального рівня відповідають за передачу даних між безпосередньо з’єднаними мережевими вузлами, забезпечують надійну доставку кадрів через фізичний носій, виявлення та виправлення помилок, а також контроль доступу до спільного середовища. Ethernet є найпоширенішою технологією локальних мереж, що еволюціонувала від стандартів 1970-х років до сучасних високошвидкісних рішень, а специфікації для різних швидкостей та типів носіїв визначає стандарт IEEE 802.3. Структура кадру Ethernet включає преамбулу для синхронізації, поля адреси призначення й відправника з MAC-адресами, поле EtherType або Length, корисні дані розміром від 46 до 1500 байт з можливим додаванням падінгу та поле Frame Check Sequence з CRC-контролем. MAC-адреса є унікальним 48-бітним ідентифікатором мережевого інтерфейсу, де перші 24 біти визначають виробника, а решта — сам пристрій. Методи доступу до середовища розвивалися від CSMA/CD у спільному середовищі до сучасних комутованих рішень без колізій, що підтримують повнодуплексну передачу.

Сучасний Ethernet охоплює швидкості від 10 Мбіт/с до сотень гігабіт, серед найпоширеніших стандартів — 10BASE-T на мідних кабелях категорії 3, 100BASE-TX для категорії 5, 1000BASE-T для категорії 5e, 10GBASE-T

для категорії 6a, а також оптоволоконні рішення 1000BASE-SX і LX та 10GBASE-SR і LR для різних відстаней. Power over Ethernet дозволяє передавати живлення й дані одним кабелем, стандарти IEEE 802.3af, 802.3at і 802.3bt забезпечують від 15,4 до 100 Вт, що зручно для IP-телефонів, Wi-Fi-точок та камер відеоспостереження. VLAN створює логічні сегменти мережі незалежно від фізичної топології за допомогою тегу IEEE 802.1Q, що дозволяє розділяти трафік IP-телефонії, робочих станцій, серверів та управління. Link Aggregation за стандартом IEEE 802.3ad об’єднує кілька фізичних каналів у один логічний, збільшуючи пропускну здатність і забезпечуючи резервування, а LACP автоматизує налаштування.

Wi-Fi протоколи базуються на IEEE 802.11 і забезпечують бездротовий доступ до мережі. Їх еволюція охоплює 802.11a на 5 ГГц зі швидкістю 54 Мбіт/с, 802.11b на 2,4 ГГц зі швидкістю 11 Мбіт/с, 802.11g із сумісністю з b та швидкістю 54 Мбіт/с, 802.11n (Wi-Fi 4) із технологією MIMO та швидкістю до 600 Мбіт/с, 802.11ac (Wi-Fi 5) з роботою у діапазоні 5 ГГц та швидкістю до 6,93 Гбіт/с, а також 802.11ax (Wi-Fi 6) з OFDMA, BSS Coloring та швидкістю до 9,6 Гбіт/с. Структура кадру Wi-Fi складніша, містить поле Frame Control, до чотирьох адресних полів, Sequence Control, корисні дані та контрольну суму. Методи доступу до середовища ґрунтуються на CSMA/CA, а механізм RTS/CTS використовується для резервування каналу. Безпека розвивалася від WEP до WPA2 з AES-CCMP та далі до WPA3 з покращеним захистом, а керування потужністю дає змогу оптимізувати енергоспоживання та зменшувати інтерференцію.

2.3.3. Протоколи маршрутизації та комутації

Протоколи маршрутизації та комутації є ключовими для роботи сучасних мереж, оскільки вони визначають оптимальні шляхи передавання даних і забезпечують ефективне використання ресурсів. Вони функціонують на різних рівнях архітектури й застосовують різні алгоритми для прийняття

рішень про переспрямування трафіку. Маршрутизація полягає у виборі найкращого шляху для пакетів між вузлами, а маршрутизатори використовують таблиці з інформацією про доступні мережі, наступні переходи та метрики. Статична маршрутизація задається адміністратором і не змінюється автоматично, що дає передбачуваність, але потребує ручного обслуговування. Вона корисна для критично важливих або резервних маршрутів. Динамічна маршрутизація використовує протоколи, що автоматично обмінюються даними про топологію та коригують шляхи при змінах у мережі, підвищуючи відмовостійкість і продуктивність.

У межах однієї автономної системи використовуються IGP-протоколи: RIP, OSPF і EIGRP. RIP заснований на алгоритмі distance vector, передає таблиці маршрутизації між сусідами та використовує кількість переходів як метрику, але має обмеження у масштабованості та швидкості конвергенції. OSPF застосовує алгоритм Дейкстри, будує базу даних топології й розраховує найкоротші шляхи, підтримує ієрархічну структуру з областями та балансування навантаження. EIGRP, власний протокол Cisco, поєднує принципи distance vector і link-state, використовує алгоритм DUAL, враховує кілька параметрів у метриці, підтримує швидку конвергенцію та нерівнодоступне балансування.

Для взаємодії між автономними системами застосовують BGP. Цей протокол типу path vector використовується в Інтернеті, підтримує складні політики маршрутизації та стабільність глобальної мережі. Він використовує AS Path для запобігання петель, працює у режимах eBGP та iBGP, а для масштабування використовує route reflectors і конфедерації.

Комутація працює на канальному рівні й забезпечує доставку кадрів у межах локальної мережі. Комутатори навчаються MAC-адрес через аналіз трафіку, формують таблицю відповідностей MAC-адрес і портів та переадресовують кадри без зайвих широкомовних передач. Якщо адреса призначення невідома, виконується flooding, а broadcast і multicast кадри поширюються на всі порти VLAN. Для запобігання петель використовується

STP, який формує деревоподібну топологію та блокує зайві з’єднання. Сучасні варіанти STP, як RSTP та MSTP, забезпечують швидшу конвергенцію. VLAN протоколи дозволяють створювати логічні сегменти мережі, а VTP синхронізує їхню конфігурацію між комутаторами. LACP дає змогу об’єднувати кілька фізичних каналів у один логічний для підвищення пропускної здатності та резервування. QoS-протоколи забезпечують пріоритизацію трафіку, IEEE 802.1p реалізує це на канальному рівні, а DiffServ використовує маркування DSCP на мережевому рівні. SNMP, NETCONF та YANG забезпечують централізований моніторинг і керування пристроями.

У кол-центрах ці протоколи повинні гарантувати високу доступність, швидку адаптацію до змін і підтримку якості сервісів. IP-телефонія та інші критичні додатки потребують гарантованої пропускної здатності та мінімальних затримок, а резервування обладнання й каналів дозволяє уникнути перерв у роботі навіть при відмовах окремих компонентів.

3 ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ КОЛ-ЦЕНТРУ

3.1 Аналіз бізнес-процесів та мережевих сценаріїв роботи

Ефективне проєктування мережевої інфраструктури кол-центру ґрунтується на глибокому розумінні бізнес-процесів і типових сценаріїв роботи операторів. Для компанії "Астраїлс Груп" основними бізнес-процесами є приймання та обробка вхідних дзвінків клієнтів через IP-АТС із подальшим автоматичним розподілом викликів (ACD) на вільних операторів, а також інтеграція з CRM-системою для швидкого доступу до картки клієнта та історії звернень. У стандартному сценарії обслуговування оператор ідентифікує клієнта, аналізує історію, діагностує проблему, використовує базу знань для пошуку рішень, а при необхідності створює тікет для ескалації питання — при цьому одночасно працюють IP-телефонія, CRM, база знань і система тікетів, що створює інтенсивний мережевий трафік.

Вихідні дзвінки реалізуються через predictive dialer для проактивного інформування клієнтів про нові послуги чи технічні роботи. Це вимагає від мережі швидкої реакції та мінімальних затримок під час встановлення з’єднання. Важливе місце займає й віддалений моніторинг клієнтських систем: оператори підключаються через VPN до серверів і обладнання клієнтів, обмінюються логами, скріншотами, даними моніторингу — такі операції формують додаткове навантаження, особливо під час передачі великих обсягів графічної інформації чи відеопотоків.

Внутрішні комунікації реалізуються за допомогою відеоконференцій (наприклад, щотижневі навчальні сесії, наради супервайзерів), корпоративних месенджерів для обміну короткими повідомленнями, а також через файлові сервіси для роботи з документами. Під час групових відеосесій (20-30 учасників у HD-форматі) мережа має витримувати навантаження до 100 Мбіт/с.

Протягом дня трафік мережі суттєво змінюється. У ранковий пік (8:00–10:00) спостерігається до 70 одночасних розмов і максимальне навантаження на CRM — мережа працює на межі своїх можливостей. В денний час (10:00–17:00) навантаження стабільне, але з періодичними піками через оновлення баз даних і віддалений моніторинг; використання ресурсів коливається у межах 60–80%. Ввечері зменшується кількість дзвінків, але зростає трафік через формування звітів і резервне копіювання — до 70% пропускної здатності. Вночі (20:00–8:00) активність мінімальна, але проходять автоматичні оновлення, обробка відкладених задач, моніторинг — навантаження падає до 20–40%.

Особливу увагу приділяють критичним сценаріям. Масові інциденти (наприклад, збої в IT-системах клієнтів) різко збільшують кількість дзвінків (до 90 одночасних з’єднань) і використання віддаленого доступу. У періоди інформаційних кампаній predictive dialer генерує високе навантаження на IP-телефонію. Навчальні сесії нових операторів призводять до різкого зростання відеотрафіку. В разі аварій мережа повинна швидко перемикатися на резервні канали: для IP-телефонії — не більше 30 секунд простою, для критичних даних — не більше 1 хвилини.

Різні види трафіку мають специфічні вимоги. IP-телефонія вимагає гарантованої смуги 64–128 кбіт/с на дзвінок, затримки до 150 мс, джитеру не більше 30 мс, втрат не більше 1%. CRM-система генерує піковий трафік при обробці даних (до 10–15 Мбіт/с на оператора), при цьому затримки понад 2 секунди істотно знижують продуктивність. Віддалений доступ та відеоконференції можуть потребувати від 5 до 20 Мбіт/с на канал. Файлові сервіси мають пікове навантаження при резервному копіюванні, яке може сягати 100 Мбіт/с.

Режим роботи 24/7 висуває вимоги до безперебійності мережі: обслуговування і оновлення мають проводитися без втрат доступу для користувачів, для цього критичні елементи резервуються. В окремі сезони (початок року, кінець кварталу, періоди акцій) навантаження зростає на 30–

50% у порівнянні із середніми показниками — мережа має бути готовою до таких змін без втрат якості обслуговування.

3.2 Визначення технічних і функціональних вимог до мережі

Визначення технічних і функціональних вимог до мережі базується на глибокому аналізі бізнес-процесів та сценаріїв роботи кол-центру, враховуючи особливості IP-телефонії, інтенсивної роботи з CRM-системами, масових відеоконференцій і цілодобового режиму функціонування. Мережева інфраструктура повинна гарантувати стабільну та комфортну роботу користувачів у будь-який час доби навіть під час пікових навантажень. Наприклад, магістральні з’єднання між комутаторами розподілу і ядра мають забезпечувати не менше 10 Гбіт/с, з можливістю агрегації до 20 Гбіт/с, а канали між комутаторами доступу та розподілу — не менше 1 Гбіт/с, з можливістю розширення до 2 Гбіт/с. Робочі місця операторів мають бути підключені на швидкості 1 Гбіт/с, що дозволяє без затримок працювати з CRM-системами та передавати великі файли, а IP-телефони можуть використовувати швидкість 100 Мбіт/с, яка повністю покриває потреби голосового трафіку.

Сервери, що обслуговують бази даних і файлові сервіси, повинні мати підключення на швидкості від 1 до 4 Гбіт/с залежно від навантаження. Для IP-телефонії та інтерактивних сервісів критично важливою є затримка передачі — вона не повинна перевищувати 10 мс у межах локальної мережі та 150 мс від кінця до кінця для голосового трафіку, а варіації затримки (джитер) мають обмежуватися 30 мс. Втрати пакетів у нормальних умовах не повинні перевищувати 0,1% для загального трафіку та 0,01% для голосового, навіть при пікових навантаженнях допустимі втрати не більше 1% для не-голосових потоків.

Високий рівень надійності забезпечується резервуванням всіх критичних компонентів: комутатори ядра та розподілу підключаються

резервними лінками з автоматичним перемиканням протягом 30 секунд, для живлення використовуються резервні джерела (UPS, дизель-генератори), а обладнання має підтримувати гарячу заміну компонентів і мати MTBF не менше 100 000 годин. Навіть при повному відключенні електроенергії мережеве обладнання має працювати не менше 30 хвилин від UPS, а генератор запускатися автоматично за 60 секунд.

Архітектура мережі повинна бути масштабованою: з розрахунком на підключення щонайменше 150 робочих місць операторів із резервом на майбутнє (20% запасу), плюс мінімум 50 портів для серверів, телефонів, Wi-Fi точок, принтерів та іншої техніки. Всі комутатори мають підтримувати розширення портів та нарощування пропускної здатності, а IP-адресний простір — передбачати можливість масштабування до 500 пристроїв у кожному VLAN.

Серед ключових функціональних вимог: підтримка якості сервісу (QoS) з пріоритезацією трафіку (IEEE 802.1p на канальному рівні, DiffServ на мережевому), можливість створення мінімум 50 VLAN із підтримкою IEEE 802.1Q та динамічним призначенням VLAN за MAC-адресами чи 802.1X. Для відеоконференцій і розповсюдження оновлень необхідна підтримка мультикасту (IGMP snooping, PIM). Моніторинг та адміністрування мають здійснюватися через SNMP v3, sFlow/NetFlow, syslog, а віддалене управління — через SSH.

Безпека мережі повинна забезпечуватися автентифікацією 802.1X для всіх пристроїв, MAC-фільтрацією, захистом від DDoS через rate limiting, Dynamic ARP Inspection, DHCP snooping та port security, а також шифруванням трафіку (IPSec для VPN, TLS для веб-застосунків, SRTP для голосу). Централізоване управління, автоматизація рутинних операцій, резервне копіювання конфігурацій, автоматичне оновлення програмного забезпечення й ведення журналів змін входять до вимог до обслуговування. Важливим є також забезпечення сумісності з наявними системами, підтримка гібридних хмарних рішень (SD-WAN, SaaS) і політик BYOD, що включає

якісне Wi-Fi покриття та мобільне адміністрування.

Загалом, ці технічні та функціональні вимоги формують основу для проектування масштабованої, захищеної та ефективної мережі, яка відповідатиме як поточним, так і майбутнім потребам кол-центру, забезпечуючи надійну роботу критичних сервісів, швидке реагування на інциденти й можливість безболісного розширення.

3.3 Побудова логічної та фізичної топології мережі

Побудова логічної та фізичної топології мережі для кол-центру, розрахованого на 30 робочих місць, здійснюється із застосуванням двоярусної ієрархічної моделі, яка забезпечує оптимальний баланс між функціональністю, надійністю та вартістю. У якості логічної топології використовується принцип колапсованого ядра (Collapsed Core), де рівні ядра та розподілу об’єднані в одному вузлі. Для підприємств із кількістю користувачів до 100 це найкращий варіант: він дає достатню продуктивність і спрощує адміністрування мережі, знижуючи витрати на обладнання.

В об’єднаному рівні ядра/розподілу функції виконує пара L3-комутаторів, що працюють у режимі активний-активний. Вони забезпечують маршрутизацію між VLAN, підключення до зовнішніх мереж, реалізацію політик QoS та безпеки, а також агрегацію трафіку з рівня доступу. На цих пристроях налаштовано базовий міжмережевий екран і політики контролю доступу. Для резервування шлюзів впроваджено протокол HSRP, а для спрощення управління – стекування комутаторів. Завдяки цьому при відмові одного пристрою весь трафік автоматично перенаправляється через інший без втрати доступності для користувачів.

Рівень доступу призначений для підключення всіх кінцевих пристроїв кол-центру. Два комутатори доступу (основний на 24 порти для робочих місць операторів і додатковий на 12 портів для допоміжного обладнання й резерву) забезпечують підключення всіх необхідних пристроїв. Тут

впроваджено політики безпеки портів (802.1X, port security), класифікацію трафіку для QoS, призначення VLAN на основі портів, а також PoE для живлення IP-телефонів та точок доступу Wi-Fi.

Логічна сегментація мережі реалізується шляхом виділення окремих VLAN для різних типів трафіку: голосовий трафік IP-телефонії операторів, робочі станції, серверне обладнання, керування мережею, Wi-Fi для співробітників і окремий гостьовий сегмент. Для прикладу, голосовий трафік відокремлюється у VLAN 10, користувацькі робочі місця у VLAN 20, сервери – у VLAN 30, обладнання управління – у VLAN 40, Wi-Fi – у VLAN 50, а гостьовий доступ – у VLAN 60. Це дозволяє ізолювати трафік різних служб, застосовувати до кожної групи власні політики безпеки та пріоритети QoS, що особливо важливо для підтримки якості IP-телефонії.

Фізична топологія мережі визначається компактним розміщенням обладнання у межах невеликого офісу. У виділеній серверній зоні, обладнаній настінною стійкою 12U, встановлено пару L3-комутаторів ядра/розподілу (у стеці), 2–3 сервери (файловий сервер/контролер домену, сервер CRM, сервер IP-АТС, резервний сервер, часто у вигляді віртуальних машин), патч-панель, систему безперебійного живлення (UPS), а також окремий мережевий комутатор для виходу в Інтернет. Між L3-комутаторами прокладено stacking-кабелі для об’єднання їх у єдиний логічний пристрій із незалежним живленням від UPS для кожного.

Комутатори доступу розташовані в різних частинах операторської зали: основний комутатор обслуговує 20 ключових робочих місць, а додатковий – 10 допоміжних місць і периферійне обладнання. Кожен комутатор підключається до стецьованих комутаторів ядра через два Gigabit Ethernet-канали для резервування й балансування навантаження. Всі робочі місця операторів підключені через кабелі Cat6A до інформаційних розеток. Серверна інфраструктура, крім фізичних серверів, може містити хост віртуалізації (наприклад, VMware vSphere) з кількома віртуальними машинами для файлових і CRM сервісів, серверу IP-АТС, а також виділений

або віртуальний backup-сервер.

Магістральні з’єднання виконано через мідні кабелі Cat6A: stacking між ядром – 10G, від ядра до доступу – 2×1GE, від комутаторів доступу до робочих місць – 1GE на порт. Горизонтальна кабельна система має зіркоподібну топологію з центром у серверній; усі кабелі Cat6A прямують від комутаторів доступу до розеток на робочих місцях, з максимальною довжиною не більше 70 метрів.

Для покриття Wi-Fi у приміщенні до 200 м² достатньо двох точок доступу, розміщених у залі операторів і в переговорних чи загальних зонах. Вони підключені до PoE-портів найближчих комутаторів доступу та налаштовані на різні канали для зниження взаємних завад.

Для забезпечення доступу до Інтернету використовується два незалежні канали: основний (100 Мбіт/с від провайдера А) та резервний (50 Мбіт/с від провайдера Б), які підключені до різних портів на ядрових комутаторах. Автоматичне перемикання (failover) гарантує безперервність доступу у випадку відмови основного каналу.

Електроживлення організовано таким чином, щоб при зникненні напруги UPS потужністю 3 кВА забезпечував безперебійну роботу всього мережевого обладнання і серверів протягом 20–30 хвилин. IP-телефони та точки доступу Wi-Fi живляться через PoE з комутаторів, а комутатори доступу мають власні адаптери живлення. Для компактності й зручності організації в серверній встановлено один 24-портовий patch panel із кольоровим маркуванням кабелів за VLAN, а всі з’єднання документуються у простій схемі.

Фізична безпека реалізована через закриту серверну стійку з контролем доступу, систему відеоспостереження в серверній зоні, сигналізацію при відкритті стійки та контроль температури й вологості для запобігання перегріву обладнання. Така топологія дозволяє забезпечити високу надійність і масштабованість мережі, простоту адміністрування, підтримку сучасних вимог до сегментації трафіку й безпеки, а також гнучкість щодо

майбутнього розширення.

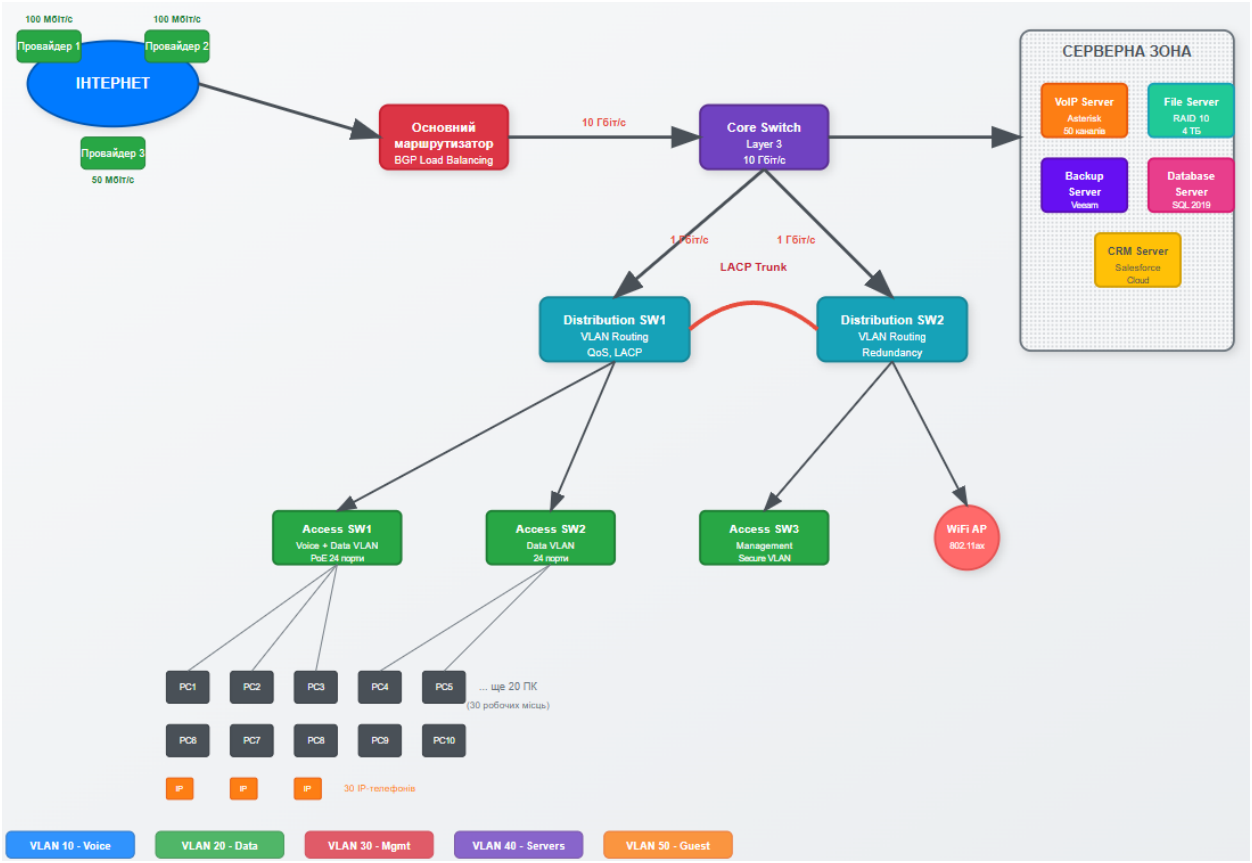

Рисунок 3.1 – Схема мережі кол-центру

3.4 Розрахунок і моделювання навантаження на мережеву інфраструктуру

Розрахунок і моделювання навантаження на мережеву інфраструктуру кол-центру з 30 робочими місцями передбачає комплексний підхід до аналізу всіх основних джерел трафіку, їх динаміки та впливу на різні сегменти мережі в різних режимах роботи. Оскільки навіть у невеликому кол-центрі одночасно функціонують системи IP-телефонії, CRM, відеоконференцій, файлового обміну, віддаленого моніторингу та доступу до Інтернету, важливо оцінити як типовий, так і піковий рівень навантаження для забезпечення стабільної роботи критичних сервісів.

У сфері IP-телефонії, яка є стратегічно важливою для кол-центру,

найбільше навантаження припадає на пікові години, коли одночасно може вестися до 28 голосових сесій — це враховує роботу 25 операторів і ще 3 резервних каналів для супервайзерів або внутрішніх консультацій. Використання кодеку G.729 дає можливість економити пропускну здатність без втрати якості, тому для одного каналу необхідно близько 31 кбіт/с. З урахуванням сигналізації SIP і резерву, загальна потреба для 28 дзвінків становить приблизно 1 Мбіт/с. Це означає, що навіть під час масових звернень система легко витримує голосовий трафік, не впливаючи на інші сервіси.

CRM-системи формують другий за обсягом тип трафіку. Для 30 операторів середнє фонове навантаження зазвичай не перевищує 45–60 Мбіт/с, проте під час пікових звернень, одночасного завантаження великих масивів даних або запуску масових запитів навантаження може зростати до 90–100 Мбіт/с. CRM також генерує трафік через web-інтерфейс, який, навіть при одночасній роботі всіх операторів, не створює критичного навантаження — близько 15 Мбіт/с. Додатково до CRM додається сегмент трафіку віддаленого моніторингу, коли до 8 операторів можуть одночасно здійснювати підключення до клієнтських систем для технічної підтримки через VPN або спеціалізовані протоколи, що створює навантаження в діапазоні від 24 до 64 Мбіт/с у залежності від типу обслуговування та обсягу переданої інформації.

Відеоконференції займають важливе місце в мережевій активності, особливо під час навчальних сесій для нових співробітників або планових нарад. Для невеликого кол-центру типові показники — це 8–15 учасників у HD-форматі, що потребує від 16 до 32 Мбіт/с. Якщо одночасно проходить кілька групових сесій, навантаження на мережу може зрости, проте завдяки ізольованості трафіку у власних VLAN та пріоритезації QoS цей сегмент не створює загроз для роботи основних сервісів.

Файловий трафік у кол-центрі є нерівномірним і формується як під час щоденної роботи (копіювання документів, обмін файлами), так і в процесі

резервного копіювання та синхронізації CRM. За типовий день кожен оператор передає близько 50 МБ даних, що дає сумарно понад 1,5 ГБ — середнє навантаження тут незначне, але під час пікових завантажень (наприклад, одночасна синхронізація даних чи запуск резервного копіювання обсягом 20 ГБ) пропускна здатність мережі повинна бути достатньою для підтримки передачі на рівні 10–15 Мбіт/с і вище, не створюючи затримок у роботі інших додатків.

Інтернет-трафік у сучасному кол-центрі формується в основному за рахунок веб-серфінгу, роботи з хмарними додатками, електронної пошти та месенджерів, а також періодичних оновлень програмного забезпечення. Загальне середнє навантаження становить 45–50 Мбіт/с, у години пік може досягати 60 Мбіт/с, особливо якщо одночасно проходить масове оновлення ПЗ або користувачі працюють з великими обсягами даних у SaaS-сервісах.

Моделювання різних сценаріїв дозволяє оцінити стабільність і потенціал інфраструктури до подальшого масштабування. У стандартному робочому режимі (типова завантаженість, середній трафік усіх сервісів) сумарне навантаження на мережу становить близько 110–120 Мбіт/с, що для сучасної гігабітної інфраструктури є незначним. У пікові періоди, наприклад, під час проведення масових інформаційних кампаній, навчання чи діагностики складних інцидентів із залученням усіх ресурсів, навантаження може сягати 230–250 Мбіт/с. Критичні сценарії, коли задіяні всі канали (максимальна кількість дзвінків, активна робота CRM, відеоконференції, інтенсивний моніторинг і передачі даних), дають навантаження до 300 Мбіт/с — це легко обслуговується інфраструктурою з гігабітними портами і навіть залишає запас для подальшого зростання.

Розподіл навантаження між сегментами відбувається наступним чином: комутатор доступу на 20 портів обслуговує до 180 Мбіт/с, другий комутатор на 10 портів — до 90 Мбіт/с. На рівні ядра агрегується весь трафік до 300 Мбіт/с, при цьому зовнішній канал використовується на рівні до 60 Мбіт/с, а маршрутизація між VLAN у пікові моменти досягає 100 Мбіт/с. Це

підтверджує достатню продуктивність гігабітної архітектури й можливість агрегації каналів для резервування та балансування навантаження.

Загальний висновок моделювання полягає в тому, що навіть у критичних сценаріях пікове навантаження у 300 Мбіт/с не перевищує можливостей гігабітної інфраструктури з запасом. Ядро мережі повинно мати канали 1GE з можливістю агрегації до 2GE, рівень доступу — 1GE на кожне підключення, а для IP-телефонії цілком достатньо портів зі швидкістю 100 Мбіт/с. Такий підхід забезпечує надійність, швидкодію і гнучкість мережі, дозволяє легко масштабуватися в разі зростання кількості користувачів або збільшення обсягу сервісів, а також гарантує якість обслуговування в усіх режимах роботи кол-центру.

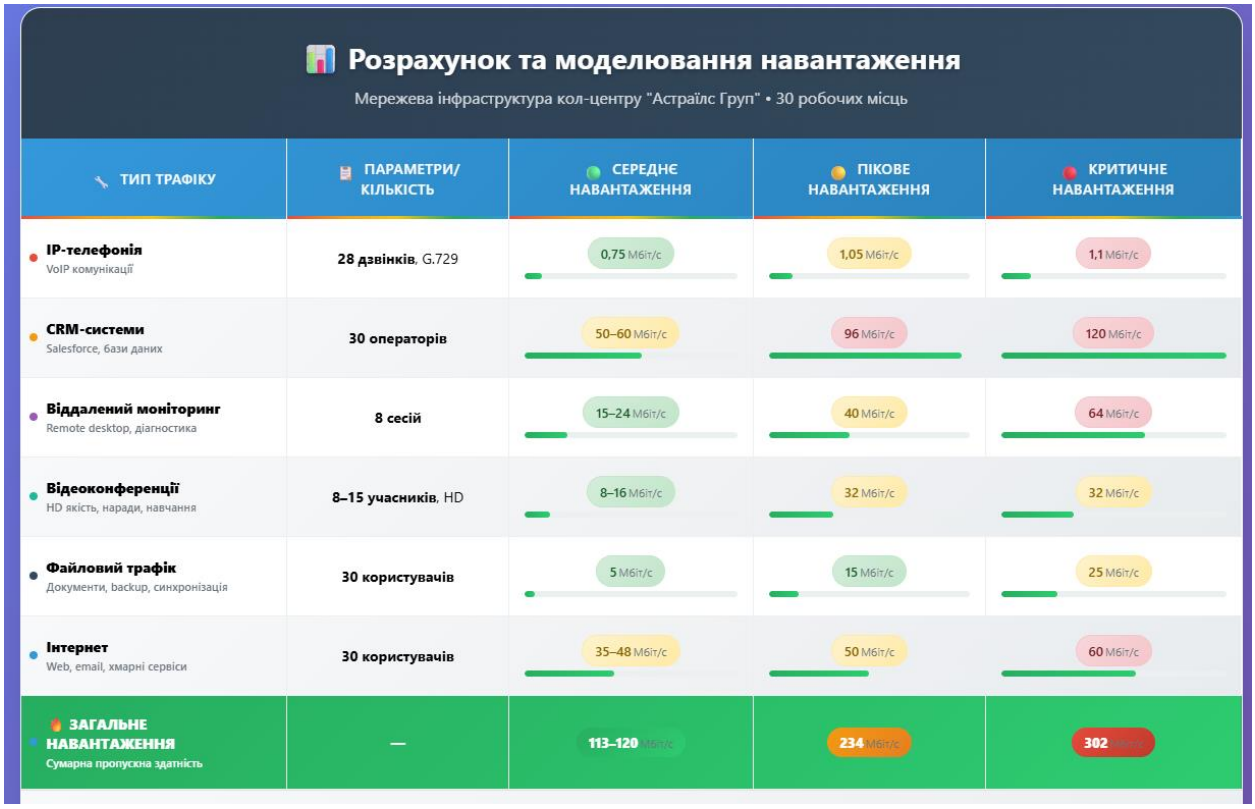

Рисунок 3.2 – Розрахунок та моделювання навантаження

3.5 Архітектура сегментації трафіку та планування IP-адрес (VLAN, Voice/Data/Management)

У мережі кол-центру з 30 робочими місцями використовується спрощена, але повноцінна архітектура VLAN, яка відповідає вимогам ізоляції, безпеки та оптимізації мережевого трафіку. Основні принципи сегментації трафіку реалізуються через виділення логічних підмереж для різних категорій пристроїв і служб, що забезпечує надійний розподіл ресурсів, централізоване управління, а також чіткий контроль доступу між сегментами.

Для голосового трафіку організовано VLAN 10 (Voice) з підмережею 192.168.10.0/26, яка дозволяє розмістити до 62 пристроїв. Основний шлюз — віртуальний IP HSRP 192.168.10.1. Діапазон 192.168.10.10–40 призначено для IP-телефонів операторів, 192.168.10.41–50 — для телефонів керівництва, а статичні адреси 192.168.10.51–62 — для IP-АТС та SIP транків. DHCP-пул забезпечує динамічне видавання адрес телефонії, а сервер IP-АТС та інфраструктурні SIP-лінки мають статичні налаштування.

Вся робота з даними операторів і адміністрації відбувається у VLAN 20 (Data), що функціонує на підмережі 192.168.20.0/26. Шлюзом виступає 192.168.20.1, а DHCP-пул охоплює 192.168.20.10–45 для робочих станцій та додаткових пристроїв. Статичні адреси призначено для принтерів, багатофункціональних пристроїв і спеціалізованого обладнання, що спрощує контроль і аудит підключень.

Серверне обладнання ізольовано у VLAN 30 (Servers) — підмережа 192.168.30.0/27. Тут використовується лише статичне адресування для ключових систем: серверу віртуалізації, контролеру домену, CRM/Database серверу, файловому, email і backup серверам, моніторинговому серверу та віртуальним машинам. Це підвищує керованість, безпеку і стабільність серверної інфраструктури.

Окремо виділена VLAN 40 (Management) на підмережі 192.168.40.0/28,

призначена виключно для адміністрування мережевого обладнання. В цій VLAN статичні IP отримують стек комутаторів ядра, комутатори доступу та точки доступу Wi-Fi, що забезпечує ізольований і захищений канал для керування та моніторингу інфраструктури.

Для бездротових пристроїв співробітників організовано VLAN 50 (WiFi) — підмережа 192.168.50.0/27. DHCP-пул налаштований на динамічну видачу адрес усім корпоративним Wi-Fi пристроям, а шлюз HSRP гарантує надійний вихід у корпоративну мережу.

Гостьовий доступ забезпечує VLAN 60 (Guest), що працює на підмережі 192.168.60.0/28 з обмеженою кількістю динамічних IP для відвідувачів, ізоляцією від внутрішніх сегментів та чіткими правилами міжвланового доступу.

Маршрутизація між VLAN організована так, що трафік Voice VLAN має доступ до серверів (для роботи IP-АТС), Data VLAN підключається до серверів для виконання службових задач, а WiFi VLAN отримує обмежений доступ до корпоративних сервісів. Управлінська VLAN має повний доступ до всіх інших сегментів для адміністрування. Натомість гостьова VLAN повністю ізольована від внутрішніх служб, а прямий обмін між Voice та Data VLAN блокується для зниження ризику компрометації.

DHCP-сервер централізовано розташований на стеку комутаторів ядра, він обслуговує всі активні VLAN із видачею необхідних опцій: Option 66 для TFTP (автоматичне налаштування IP-телефонів), Option 6 для DNS (контролер домену), Option 15 для домену callcenter.local. Така архітектура дозволяє ефективно масштабувати мережу, гарантувати надійність і безпеку доступу, чітко контролювати розподіл адрес і сегментацію трафіку, спрощує адміністрування, моніторинг і резервування ресурсів для всіх категорій користувачів та пристроїв кол-центру.

Таблиця. Сегментація трафіку та IP-адресація у мережі кол-центру

VLAN	Призначення	IP-підмережа	DHCP-пул	Статичні адреси	Типові пристрої	Шлюз (HSRP)
10	Voice (Голосова мережа)	192.168.10.0/26	192.168.10.10–192.168.10.50	.51–.52 (IP-АТС), .53–.54 (SIP)	IP-телефони, IP-АТС	192.168.10.1
20	Data (Робочі місця)	192.168.20.0/26	192.168.20.10–192.168.20.45	.46–.50 (принтери), .51–.55 (інше)	ПК операторів, принтери	192.168.20.1
30	Servers (Сервери)	192.168.30.0/27	*DHCP вимкнено*	.10–.20	Сервери, віртуальні машини	192.168.30.1
40	Management (Управління)	192.168.40.0/28	*DHCP вимкнено*	.10–.14	Комутатори, точки доступу Wi-Fi	192.168.40.1
50	WiFi (Бездротова мережа)	192.168.50.0/27	192.168.50.10–192.168.50.25	—	Корпоративні Wi-Fi пристрої	192.168.50.1
60	Guest (Гості)	192.168.60.0/28	192.168.60.10–192.168.60.14	—	Гостьові пристрої	192.168.60.1

Рисунок 3.3 – Сегментація трафіку та IP-адресація у мережі кол-центру

3.6 Мережева політика безпеки та контроль доступу

Мережева політика безпеки та контроль доступу для кол-центру з 30 робочими місцями базується на принципі максимального захисту при мінімальній складності адміністрування. Головним завданням є зменшення ймовірності інцидентів за рахунок багаторівневого підходу до безпеки та чіткої ізоляції критичних сервісів і сегментів. Периметровий захист будується на використанні інтегрованого міжмережевого екрану в комутаторах ядра, який здійснює фільтрацію вхідного і вихідного трафіку, застосування NAT для маскування внутрішньої адресації й обмежений port forwarding лише для тих сервісів, які мають бути доступними ззовні (наприклад, веб-сервіси, IP-телефонія, VPN). Усі вхідні з’єднання за замовчуванням блокуються, а винятки чітко регламентовані: дозволяється лише доступ до портів HTTP/HTTPS для внутрішніх і зовнішніх веб-додатків, SIP для IP-телефонії, VPN для віддалених співробітників, при цьому P2P-трафік повністю блокується для зменшення ризиків.

Контроль доступу на рівні доступу до мережі реалізовано через автентифікацію 802.1X, інтегровану з корпоративною Active Directory. Це дозволяє автоматично розподіляти пристрої користувачів у потрібні VLAN залежно від їхньої ролі, а невідповідні пристрої переміщати у quarantine VLAN для обмеження доступу до критичних ресурсів. Для IP-телефонів впроваджено MAC Authentication Bypass із “білим списком” MAC-адрес та автоматичним призначенням Voice VLAN. Будь-які невідомі MAC-адреси блокуються, що запобігає підключенню несанкціонованих пристроїв.

Для захисту портів комутаторів використовується портова безпека: на кожному порту дозволяється максимум дві MAC-адреси (наприклад, ПК і IP-телефон), із застосуванням sticky MAC-навчання. При виявленні порушень порт автоматично блокується. Додатково активовано DHCP snooping — лише порти, що ведуть до серверів, оголошуються довіреними, завдяки чому блокується можливість появи “шкідливих” DHCP-серверів у мережі; rate limiting обмежує кількість DHCP-запитів для запобігання DDoS-атакам.

Безпека Wi-Fi побудована на WPA3-Personal для корпоративних пристроїв і WPA2-Personal для гостьового сегменту, з виділенням окремих SSID і застосуванням MAC-фільтрації для найбільш критичних пристроїв. У гостьовій мережі обов’язково активується client isolation, що унеможливлює міжкористувацьку взаємодію навіть у межах одного SSID.

Моніторинг стану безпеки здійснюється за допомогою базової системи SIEM, що базується на зборі логів із усіх ключових пристроїв через syslog на файловий сервер. Впроваджені базові правила виявлення аномалій (наприклад, множинні невдалі спроби автентифікації, поява нових пристроїв у мережі, аномальний міжвлановий трафік, зміни у конфігураціях обладнання), а також автоматичні email-сповіщення про критичні події та щоденні звіти для адміністратора.

Політика керування паролями проста, але ефективна: для користувачів мінімальна довжина паролю складає 8 символів, для адміністраторів — не менше 12 символів, усі паролі оновлюються щонайменше раз на 180 днів,

при цьому забороняється використання останніх шести паролів. Це дозволяє уникнути простих сценаріїв підбору або компрометації паролів у разі витоку.

Резервне копіювання (backup) організовано у два етапи: щоденне копіювання на локальний NAS та щотижневе — у хмарне сховище із шифруванням. Перевірка працездатності відновлення виконується щомісяця, а усі процедури disaster recovery документуються й періодично оновлюються.

Фізична безпека досягається завдяки замкненій серверній стійці, відеореєстратору на кілька камер для контролю критичних зон, електронному контролю доступу до серверної й сигналізації при несанкціонованих спробах проникнення. Такий підхід дозволяє гарантувати високий рівень захисту даних і ресурсів кол-центру, водночас залишаючи адміністрування прозорим, керованим та максимально адаптованим до невеликої організації.

Рисунок 3.4 – Компоненти безпеки мережі кол-центру

4 АКТИВНЕ МЕРЕЖЕВЕ ОБЛАДНАННЯ

4.1 Комутатори (свічі) та їх характеристики

Комутатори, або мережеві свічі, є основними активними елементами будь-якої сучасної мережі кол-центру, і їхній правильний вибір безпосередньо впливає на продуктивність, відмовостійкість і безпеку всієї інфраструктури. Для організації мережі середнього масштабу, розрахованої на 30 робочих місць, оптимальним є впровадження двоярусної моделі з поєднанням функцій ядра та розподілу на одному класі обладнання. Для цієї ролі ідеально підходять комутатори серії Cisco Catalyst 9300-24P, які забезпечують високу комутаційну здатність (понад 200 Гбіт/с), мають вбудовані порти 1GE з підтримкою PoE+ для підключення критичних пристроїв, 10GE інтерфейси для магістральних з’єднань та стекові порти для резервування й об’єднання в єдину логічну систему. Задяки стекуванню можна отримати одну точку управління для кількох пристроїв, автоматичний розподіл навантаження, миттєве переключення у разі відмови master-комутатора та просту масштабованість без простою мережі.

Комутатори ядра виконують також роль маршрутизаторів між VLAN, підтримують повний набір протоколів динамічної маршрутизації (OSPF, EIGRP, BGP), резервування шлюзів за допомогою HSRP чи VRRP, а також ізоляцію та сегментацію за допомогою VRF-Lite для корпоративних сценаріїв. Для організації високоякісної IP-телефонії та надання пріоритету голосовому трафіку передбачено розвинену систему QoS — декілька черг на кожному порту, гнучка класифікація пакетів за DSCP, CoS або ACL, механізми rate limiting, а також автоматичне створення Voice VLAN і відповідне планування пріоритетів.

Ще одна перевага комутаторів цього класу — інтегровані засоби безпеки. До них належать портова аутентифікація 802.1X із динамічним

призначенням VLAN, MAC Authentication Bypass для обслуговування IP-телефонів, функції port security зі “sticky” MAC, захист від атак на мережевому рівні (Dynamic ARP Inspection, DHCP snooping, IP Source Guard), а також централізована інтеграція із сучасними платформами керування політиками доступу (Cisco TrustSec, AAA через Active Directory). Завдяки цьому підвищується контроль над підключеннями, знижується ризик компрометації, а мережа зберігає стійкість навіть під час атак чи внутрішніх збоїв.

Рисунок 4.1 – Cisco Catalyst 9300-24P

На рівні доступу для підключення кінцевих пристроїв застосовуються комутатори Cisco Catalyst 9200-24P, що поєднують доступну вартість, достатню продуктивність і розвинені можливості PoE+ для живлення IP-телефонів, точок доступу Wi-Fi та периферійного обладнання. Ці пристрої мають 24 порти 1GE, додаткові uplink-інтерфейси 1/10GE для підключення до ядра, підтримують створення до тисячі VLAN, 16 000 MAC-адрес у таблиці, сучасні протоколи захисту (802.1X, port security, storm control, DHCP snooping), автоматичне виявлення та класифікацію IP-телефонів, а також web-інтерфейс для простого первинного налаштування. Така архітектура дозволяє швидко підключати і масштабувати мережу відповідно до змін бізнес-процесів, забезпечуючи резервування й балансування навантаження за допомогою EtherChannel та Link Aggregation.

Розподіл портів між серверними, клієнтськими, магістральними і резервними підключеннями організовано таким чином, щоб забезпечити

максимум гнучкості: окремі порти відводяться під сервери (файловий сервер, контролер домену, CRM-система, резервний сервер, IP-АТС), підключення до комутаторів доступу й до провайдерів Інтернету. Uplink-з'єднання між рівнем доступу й ядром виконуються з агрегацією каналів для підвищення пропускної здатності й відмовостійкості, а сервери підключаються безпосередньо до ядра для мінімізації затримок.

Для підтримки якісної IP-телефонії на кожному порту, де встановлений телефон, впроваджується автоматичне розпізнавання пристрою й пріоритезація QoS на рівні Layer 2/3, відмітка голосових пакетів, визначення trust boundaries, суворі налаштування port security для обмеження кількості MAC-адрес і швидке реагування на несанкціоновані підключення. DHCP snooping та Dynamic ARP Inspection використовуються для захисту від основних типів атак на мережу, таких як rogue DHCP чи ARP spoofing. SNMP, NetFlow і syslog інтегруються у єдину систему моніторингу, яка дозволяє не лише бачити стан обладнання в реальному часі, а й аналізувати мережевий трафік, виявляти аномалії та оперативно реагувати на інциденти.

Управління обладнанням централізоване, завдяки стекуванню й вбудованим інструментам Cisco DNA Center, що дозволяє автоматизувати рутинні завдання, оновлення, резервування конфігурацій, запуск щоденних чи щотижневих резервних копій через планувальник Kron, а також здійснювати віддалене налаштування через CLI, SSH або REST API. Підвищена надійність досягається за рахунок резервування блоків живлення, вентиляторів, можливості "гарячої" заміни модулів, а також технологій Non-stop forwarding і graceful restart для мінімізації простоїв у разі збоїв.

Рисунок 4.2 – Cisco Catalyst 9200-24P

Завдяки такій архітектурі, навіть невеликий кол-центр отримує високий рівень продуктивності, безпеки, гнучкості та простоти масштабування, що дозволяє підтримувати всі сучасні бізнес-процеси, швидко розгортати нові сервіси і впроваджувати політику “zero trust” для всіх сегментів і користувачів без надлишкових витрат на адміністрування та підтримку.

4.2 Точки доступу Wi-Fi

Бездротовий доступ у сучасному кол-центрі відіграє важливу роль у підвищенні мобільності співробітників, підтримці роботи гостьових користувачів і оптимізації робочого простору. Для офісу на 30 робочих місць впровадження корпоративних точок доступу дозволяє не лише забезпечити стійке покриття по всьому периметру, а й централізовано управляти політикою доступу, контролем трафіку та безпекою мережі. Вибір Cisco Catalyst 9120AXI як основного обладнання гарантує підтримку новітнього стандарту Wi-Fi 6, що забезпечує високу щільність підключень, оптимальну пропускну здатність і мінімальні затримки навіть у найбільш завантажених офісних зонах.

Архітектура бездротової мережі передбачає встановлення двох точок доступу. Одна з них розміщується у центрі основного операторського залу, що дозволяє покривати основну робочу зону з 20-ма співробітниками та забезпечувати якісний рівень сигналу в радіусі 6–7 метрів. Друга точка орієнтована на додатковий зал, переговорні кімнати та суміжні офісні простори, що критично для підтримки зв’язку в розрізнених ділянках приміщення. Завдяки використанню технологій MIMO та beamforming пристрої автоматично підлаштовуються до найбільш оптимальної якості сигналу та мінімізують вплив інтерференції. Для уникнення взаємного впливу точок доступу використовується грамотне планування каналів, а зони перекриття (overlap) залишаються у межах 10–15%, що гарантує безперервний роумінг користувачів під час переміщення офісом.

Кожна точка доступу оснащена потужним Gigabit Ethernet портом із підтримкою PoE+, що дозволяє зручно організувати живлення пристроїв без окремих блоків. У випадку збою основного живлення точки доступу можуть залишатися функціональними завдяки резервному живленню від UPS системи. Точки доступу монтуються на стелі на висоті 3–3,5 метрів для рівномірного розподілу сигналу, а вибір антенної конфігурації забезпечує покриття навіть у важкодоступних кутах.

Безпека бездротової мережі організована на декількох рівнях. Для співробітників виділяється окремий SSID з обмеженим доступом до корпоративних ресурсів і підключенням до окремого VLAN. Захист трафіку забезпечується WPA2-PSK або WPA3 (залежно від підтримки клієнтських пристроїв), а доступ додатково обмежується MAC-фільтрацією для критичних пристроїв, такими як службові ноутбуки та IP-телефони з Wi-Fi-модулем. Гостьовий сегмент повністю ізольований від внутрішньої мережі: для гостей створюється окремий SSID із Captive Portal, який відкриває доступ лише до Інтернету після ідентифікації користувача, а швидкість підключення жорстко лімітується на рівні QoS.

Ще одним обов’язковим елементом політики є впровадження client isolation для гостьової мережі, що унеможливлює взаємодію між клієнтами навіть у межах одного SSID, а для персоналу діють більш лояльні правила, однак між VLAN налаштовуються Access Control Lists для суворого контролю доступу до серверів, служб і адміністративних ресурсів. Інтеграція з системою Cisco Identity Services Engine дозволяє централізовано управляти політиками доступу та сегментацією трафіку навіть для бездротових пристроїв.

Реалізація QoS дозволяє пріоритезувати голосовий та відеотрафік співробітників, що критично важливо для безперебійної роботи IP-телефонії та відеоконференцій. Адміністратори мають окремий прихований SSID із доступом лише для авторизованих пристроїв та посиленою автентифікацією, а також MAC-фільтрацією й підключенням до management VLAN для

віддаленого обслуговування інфраструктури.

Моніторинг і оптимізація бездротової мережі здійснюється через SNMP та централізовану платформу керування Cisco DNA Center, що дозволяє відслідковувати основні параметри якості сигналу, кількість активних підключень, рівень інтерференції, якість покриття та своєчасно реагувати на появу підозрілих пристроїв (rogue AP detection). Оновлення мікропрограм, регулярне тестування якості покриття (site survey), аудит налаштувань і періодична зміна паролів є стандартною процедурою для підтримки високого рівня безпеки й продуктивності.

Рисунок 4.3 – Cisco Catalyst 9120AXI

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи досягнуто головну мету дослідження — розроблено науково обґрунтовану архітектуру локальної комп'ютерної мережі кол-центру компанії "Астраїлс Груп" на тридцять операторських робочих місць, яка повністю відповідає сучасним вимогам до продуктивності, відмовостійкості та інформаційної безпеки контакт-центрів. Проведено комплексний аналіз предметної області, який дозволив виявити ключові особливості функціонування кол-центрів і сформулювати специфічні вимоги до мережевої інфраструктури: акцентовано критичну важливість якості VoIP-телефонії, стабільної роботи CRM-систем, захисту персональних даних клієнтів відповідно до регуляторних норм, а також ідентифіковано типи мережевого трафіку та їх характеристики — голосовий трафік з низькими затримками, дані CRM із піковими навантаженнями та трафік моніторингу із вимогами до стабільної пропускної здатності.

Системний аналіз теоретичних основ проектування локальних мереж забезпечив обґрунтований вибір технологічних рішень: досліджено стек протоколів TCP/IP із урахуванням їх специфіки в кол-центрах, аналізовано канальний і мережевий рівні, особливу увагу приділено механізмам забезпечення QoS для пріоритетності голосового трафіку й сучасним підходам до мережевої безпеки. На основі цього розроблено оптимальну архітектуру мережі, що спирається на двоярусну ієрархічну модель із колапсованим ядром, яка забезпечує баланс функціональності й економічної ефективності. Логічна сегментація за допомогою VLAN для різних типів трафіку (Voice, Data, Servers, Management, WiFi, Guest) гарантує їхню ізоляцію й покращує захищеність, а фізична топологія оптимізована для компактного офісу зі зручним розміщенням обладнання.

Математичне моделювання підтвердило, що навіть у пікових режимах (до 30 одночасних голосових з’єднань, активна робота з CRM і

відеоконференції) мережа не перевищує 300 Мбіт/с, що підтверджує достатність Gigabit-інфраструктури з резервом на майбутнє розширення до 50 робочих місць. Вибір обладнання обґрунтовано специфікою задач: комутатори Cisco Catalyst серії 9000 відповідають вимогам продуктивності, підтримують PoE+ для IP-телефонів, мають функції Layer 3 і сучасні засоби QoS, а точки доступу Wi-Fi 6 забезпечують ефективне бездротове покриття.

Розроблено комплексну систему безпеки: периметровий захист, сегментація з контролем міжвланового трафіку, автентифікація через 802.1X, портова безпека комутаторів, WPA3 для Wi-Fi і сегментація SSID, централізований моніторинг логів і виявлення аномалій. Запропоновано адаптацію принципів проектування корпоративних мереж під потреби контакт-центрів малого й середнього масштабу та розроблено методику розрахунку пропускної здатності для змішаного трафіку, що дозволяє точно визначити вимоги до обладнання й оптимізувати співвідношення продуктивності, надійності й економічної ефективності.

Розроблені технічні й організаційні рішення можуть бути безпосередньо впроваджені в компанії "Астраїлс Груп" для модернізації інфраструктури, а також застосовані в інших кол-центрах, службах підтримки та консалтингових компаніях. Напрацьовані рішення можуть бути використані як референтна модель для інтеграторів, а також у навчальному процесі для підготовки студентів з мережевих технологій. Запропонована архітектура забезпечує оптимальне використання інвестицій, мінімізує витрати на обладнання й обслуговування завдяки двоярусній топології та інтегрованим функціям PoE.

Результати кваліфікаційної роботи створюють підґрунтя для подальших досліджень з інтеграції штучного інтелекту для оптимізації трафіку, впровадження SDN для динамічного управління ресурсами, розробки гібридних хмарно-локальних рішень для масштабованості й відмовостійкості. Розроблена архітектура відповідає сучасним тенденціям цифровізації, вимогам до безпеки й якості сервісу, а впровадження QoS і

мобільних технологій забезпечує відповідність індустріальним стандартам. Таким чином, поставлені у кваліфікаційній роботі завдання повністю виконано, а результати мають як теоретичне, так і практичне значення для розвитку корпоративних мережевих технологій

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