МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

Інститут інженерії та інформаційних технологій

Кафедра комп'ютерної інженерії та електромеханіки

ДИПЛОМНА БАКАЛАВРСЬКА РОБОТА

на тему

МУЛЬТИСЕРВІСНА КОРПОРАТИВНА МЕРЕЖА ПІДПРИЄМСТВА

Виконав: студент групи БКІ-19

спеціальності 123 «Комп'ютерна інженерія »

Савісько В.О. _____
(прізвище та ініціали)

Керівник к.т.н., доц. Стаценко Д.В. _____
(прізвище та ініціали)

Рецензент_____ _____
(прізвище та ініціали)

Київ 2023

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
Інститут інженерії та інформаційних технологій
Кафедра комп'ютерної інженерії та електромеханіки
Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма «Комп'ютерні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри КІЕМ

_____проф. Злотенко Б.М.

"_____" _____2023 року

З А В Д А Н Н Я

НА ДИПЛОМНУ БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Савіську Вячеславу Олександровичу

(прізвище, ім'я, по батькові)

1. Тема дипломної бакалаврської роботи Мультисервісна корпоративна мережа підприємства

Науковий керівник роботи Стаценко Д.В., к.т.н., доцент

затверджені наказом вищого навчального закладу від _____ № _____

2. Строк подання студентом роботи 1 червня 2023 року

3. Вихідні дані до дипломної бакалаврської роботи: структура та підрозділи підприємства; основні сервіси корпоративної мережі.

4. Зміст дипломної бакалаврської роботи (перелік питань, які потрібно розробити): 1. Аналіз концепцій та рішень побудови корпоративних комп'ютерних мереж виробничих підприємств. 2. Структура мультисервісної корпоративної мережі. 3. Вибір мережевого обладнання. 4. Вибір сервісів.

5. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної бакалаврської роботи	Терміни виконання етапів	Примітка про виконання
1	Вступ	01.02.2023	
2	Розділ 1. Аналіз концепцій та рішень побудови корпоративних комп'ютерних мереж виробничих підприємств	15.02.2023	
3	Розділ 2. Структура мультисервісної корпоративної мережі	15.03.2023	
4	Розділ 3. Вибір мережевого обладнання	05.04.2023	
5	Розділ 4. Вибір сервісів	20.04.2023	
6	Висновки	10.05.2023	
7	Оформлення дипломної бакалаврської роботи (чистовий варіант)	20.05.2023	
8	Здача дипломної бакалаврської роботи на кафедру для рецензування (за 14 днів до захисту)	25.05.2023	
9	Перевірка дипломної бакалаврської роботи на наявність ознак плагіату (за 10 днів до захисту)	28.05.2023	
10	Подання дипломної бакалаврської роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	05.06.2023	

Студент _____ Савісько В.О.
(підпис) (прізвище та ініціали)

Науковий керівник роботи _____ Стаценко Д.В.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Савісько В.О. Мультисервісна корпоративна мережа підприємства. – Рукопис.

Дипломна бакалаврська робота за спеціальністю 123 Комп'ютерна інженерія, освітньою програмою «Комп'ютерна інженерія». – Київський національний університет технологій та дизайну, Київ, 2023 рік.

Дипломну бакалаврську роботу присвячено аналізу та побудові мультисервісної корпоративної мережі підприємства.

При вирішенні поставлених завдань використано порівняльний аналіз, теоретичні знання та практичні надбання в галузі комп'ютерних мереж та програмного забезпечення.

В результаті роботи було запропоновано рішення мультисервісної корпоративної мережі підприємства з використанням технології *Huawei One Net*. Новизна полягає в порівняльному аналізі існуючих рішень побудови мультисервісних корпоративних мереж, сервісів відеоспостереження, *IP*-телефонії, відеоконференцій та обґрунтованні використання саме даних рішень.

Результати досліджень можуть бути застосовані при побудові мультисервісних корпоративних мереж підприємств.

Ключові слова: корпоративна мережа, сервіс, IP-телефонія, відеоспостереження, конференція, підприємство.

ABSTRACT

Savisko V.O. Multi-service corporate network of the enterprise. – Manuscript.

Bachelor’s thesis in specialty 123 "Computer Engineering", educational program "Computer Engineering". – Kyiv National University of Technologies and Design, Kyiv, 2023.

The bachelor thesis is devoted to the analysis and construction of a multi-service corporate network of the enterprise.

Comparative analysis, theoretical knowledge and practical assets in the field of computer networks and software were used to solve the tasks.

As a result of the work, a multi-service enterprise network solution using Huawei One Net technology was proposed. The novelty consists in the comparative analysis of existing solutions for building multi-service corporate networks, video surveillance services, IP-telephony, video conferencing and justified use of these solutions.

Research results can be applied in the construction of multi-service corporate networks of enterprises.

Keywords: corporate network, service, IP telephony, video surveillance, conference, enterprise.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 8
ВСТУП 9
РОЗДІЛ 1 АНАЛІЗ КОНЦЕПЦІЙ ТА РІШЕНЬ ПОБУДОВИ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ВИРОБНИЧИХ ПІДПРИЄМСТВ 13
1.1. Аналіз концепцій побудови мереж виробничих підприємств 13
1.2. Основні властивості та складові комп'ютерних мереж 14
1.3. Принципи створення корпоративних мереж виробничих підприємств 18
1.4. Багаторівневий підхід при побудові мультисервісних мереж 22
1.4.1. Трьохрівнева модель мережі 22
1.4.2. Двохрівнева модель мережі 25
1.5. Рішення побудови мультисервісної корпоративної мережі 25
1.5.1. Використання Cisco AVVID 25
1.5.2. Використання Huawei One Net 28
Висновки за розділом 1 30
РОЗДІЛ 2 СТРУКТУРА МУЛЬТИСЕРВІСНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ 32
2.1. Загальна структура мережі 32
2.2. Вибір та обґрунтування топології мережі 33
2.3. Аналіз віртуальних мереж 35
2.3.1. Віртуальна приватна мережа 35
2.3.2. Віртуальна локальна мережа 37
2.4. Забезпечення відмовостійкості ядра мережі 40
2.4.1. Сімейство протоколів FHRP 40
2.5. Аналіз вимог до корпоративної мережі 43
2.6. Побудова корпоративної мережі 45
2.7. Розподіл адресного простору та VLAN 48
Висновки за розділом 2 49
РОЗДІЛ 3 ВИБІР МЕРЕЖЕВОГО ОБЛАДНАННЯ 51
3.1. Вимоги до мережевого обладнання 51
3.2. Порівняльний аналіз та вибір мережевого обладнання 51

3.2.1. Комутатор Huawei S2700-26TP-PWR-EI 53
3.2.2. Комутатор Huawei S2700-26TP-SI-AC 54
3.2.3. Комутатор Huawei S5700-26X-SI-12S-AC 54
3.2.4. Маршрутизатор Huawei AR-1200E 56
3.2.5. Маршрутизатор Huawei AR-3200-SRU200 57
3.2.6. IP-телефон Fanvil X4 59
3.2.7. Сервер ARTLINE Business R25v10 60
3.2.8. IP-камера Huawei C2120-10-LU 61
Висновки за розділом 3 62
РОЗДІЛ 4 ВИБІР СЕРВІСІВ 63
4.1. Сервіс інтелектуального відеоспостереження 63
4.2. Сервіс IP-телефонії 67
4.2.1. Налаштування SIP користувачів 68
4.2.2. Безпека VoIP 70
4.2.3. Налаштування плану набору 71
4.2.4. Налаштування переадресації дзвінків 73
4.3. Сервіс відеоконференцій 74
4.3.1. Налаштування ConfBridge 75
4.3.2. Підвищення ефективності сервісу 78
Висновки за розділом 4 78
ВИСНОВКИ 80
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 83

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AGI – Asterisk Gateway Interface (Шлюзовий інтерфейс Asterisk)

AVVID – Architecture for Voice, Video and Integrated Data (Архітектура для голосу, відео та інтегрованих даних)

FHRP – First Hop Redundancy Protocol (Протокол резервування першого переходу)

SDC – Software-Defined Camera (Програмно-визначена камера)

SIP – Session Initiation Protocol (Протокол встановлення сеансу)

SRTP – Secure Real-time Transport Protocol (Безпечний протокол передачі даних в реальному часі)

TLS – Transport Layer Security (Протокол захисту транспортного рівня)

VLAN – Virtual Local Area Network (Віртуальна локальна мережа)

VoIP – Voice over IP (Голос через IP)

VPN – Virtual Private Network (Віртуальна приватна мережа)

VRRP – Virtual Router Redundancy Protocol (Протокол резервування віртуального маршрутизатора)

АТС – Автоматична Телефонна Станція

ВСТУП

Основою інфраструктури сучасних підприємств є корпоративні мережі передачі даних. Корпоративна мережа – це складна система, що забезпечує передачу різноманітної інформації між різними додатками та системами, що використовуються в єдиній мережі підприємства.

Мультисервісна корпоративна мережа може включати в себе такі сервіси та системи як: єдину для всіх підрозділів базу даних, електронний документообіг, організацію нарад, аудіо- та відеоконференції з віддаленими підрозділами, забезпечення всіх потреб організації в високоякісному телефонному місцевому, міжміському та міжнародному зв’язку. Все це зменшує час реакції на зміни, що відбуваються на підприємстві, та забезпечує раціональне управління процесами підприємства в реальному часі. Для організації конференцій та якісного телефонного зв’язку у корпоративних мережах використовують *IP*-телефонію, що знижує залежність організації від операторів мобільного зв’язку. Дане рішення в свою чергу дозволяє істотно скоротити витрати організації. Також, корпоративна мережа дає можливість передавати будь-яку конфіденційну інформацію фінансового або виробничого характеру з впевненістю, що ніхто, крім працівників підприємства, не має до неї доступу.

Мультисервісні корпоративні мережі приходять на зміну спеціалізованим мережам. З розвитком корпоративних мереж та сервісів, що вони надають, вимоги до мультисервісної корпоративної мережі безперервно зростають.

В даному підприємстві необхідне надання працівникам послуг передачі даних та медіа-даних в рамках створеної корпоративної мережі. Необхідно створення єдиного телефонного номерного простору компанії з можливістю гнучкого налаштування і доступом до телефонної мережі загального користування (ТМЗК). Також, необхідно забезпечення фізичної безпеки складу підприємства, шляхом відеоспостереження. Дана мультисервісна корпоративна мережа повинна включати в себе, також, сервіс відеоконференцій.

Ідея об’єднати в єдиній мережевій інфраструктурі, заснованій на пакетному протоколі, можливість передачі і даних, голосових потоків, і відеоінформації – є

дуже привабливою для підприємств, адже вона здатна істотно скоротити витрати і збільшити продуктивність праці.

Відомі рішення побудови корпоративних мереж досить специфічні, оскільки розглядають конкретні системи і наявні результати неможливо безпосередньо використовувати при побудові і аналізі інших мереж з відмінними параметрами. Це пояснюється сильною залежністю початкових параметрів мережі від пропонованих вимог до обробки, захисту, представлення інформації та сервісів, які дана мережа надає. У кожному конкретному випадку необхідне оригінальне рішення, що зумовлено специфікою мережі та сервісів.

Приймаючи рішення про побудову корпоративної мультисервісної мережі з інтеграцією в неї сервісу *IP*-телефонії, підприємство прогнозує значне зростання регіональних філій.

Корпоративна мережа, зазвичай, є територіально розподіленою, тобто об’єднує офіси, фабрики та інші підрозділи, що знаходяться на великій відстані один від одного. Іноді підмережі корпоративної мережі є розташованими в різних містах, а інколи і різних країнах. Підходи, за якими будується така мережа, досить сильно відрізняються від тих, які застосовуються при створенні локальної мережі. Основна відмінність полягає в тому, що територіально розподілені мережі використовують досить повільні орендовані лінії зв’язку. Якщо при створенні локальної мережі основні витрати припадають на закупівлю мережевого обладнання і прокладку кабелю, то в територіально-розподілених мережах найдорожчою складовою виявляється орендна плата за використання каналів, яка швидко зростає зі збільшенням якості і швидкості передачі даних. Це обмеження є принциповим, і при побудові корпоративної мережі слід вживати заходів для мінімізації обсягів даних, що передаються.

Перша проблема, яку доводиться вирішувати при створенні корпоративної мережі – об’єднання підрозділів підприємства. Якщо в межах одного міста можна розраховувати на оренду виділених ліній, в тому числі високошвидкісних, то при переході до географічно істотно віддалених вузлів вартість оренди каналів стає просто астрономічною, а якість і надійність часто виявляється досить низькою.

Очевидною альтернативою є використання вже існуючих глобальних мереж. У цьому випадку досить забезпечити канали від підрозділів до найближчих вузлів глобальної мережі. Завдання обміну інформації між вузлами глобальна мережа при цьому візьме на себе. Навіть при створенні невеликої мережі в межах одного міста слід закладати можливість подальшого розширення і використовувати технології, сумісні з існуючими глобальними мережами.

При використанні мережі Інтернет в якості основи для корпоративної мережі передачі даних з'ясовується дуже цікава річ. Якщо заглянути в структуру мережі Інтернет, можна побачити, що інформація проходить через безліч абсолютно незалежних і здебільшого некомерційних вузлів, пов'язаних через найрізноманітніші канали та мережі передачі даних. Звідси випливає нагальна проблема Інтернету – безпека. Якщо говорити про приватну мережу, інформацію, що передається досить просто захистити від чужого впливу. Непередбачуваність шляхів інформації між безліччю незалежних вузлів Інтернету не тільки підвищує ризик того, що інформація може бути перехоплена, але і робить неможливим визначення місця витоку інформації. Існують засоби шифрування інформації, що передається, які дозволяють частково вирішити цю проблему. Інший аспект проблеми безпеки знову ж пов'язаний з децентралізацією мережі Інтернет – немає нікого, хто міг би обмежити доступ до ресурсів вашої приватної мережі. Оскільки це відкрита система, де всі бачать всіх, то будь-який бажаючий може спробувати потрапити в вашу корпоративну мережу і отримати доступ до даних. Звичайно, є деякі засоби, такі як фаервол (*Firewall*), але це не дає повного захисту. Окрім того, потрібно враховувати ще забезпечення безпеки і до інформації, яка передається в рамках корпоративної мережі, щоб доступ до неї отримували лише співробітники, які повинні її побачити. Це досягається за допомогою поділу корпоративної мережі на віртуальні локальні мережі та застосування політик безпеки.

Створення віртуальних приватних мереж (*VPN*) дозволяє об'єднати усі підрозділи підприємства, що мають географічно-розгалужену структуру. Незалежно від взаємної віддаленості територіальних підрозділів та складів, *VPN* забезпечує їх повну зв'язність, роботу і взаємодію будь-яких сервісів, тому вона є

ефективним інструментом для створення єдиного інформаційного простору підприємства.

Мета дипломної роботи – аналіз та побудова мультисервісної корпоративної мережі підприємства.

Об’єктом дослідження є процес побудови мультисервісної корпоративної мережі підприємства.

Предмет дослідження: корпоративна мережа підприємства.

Методи дослідження. При вирішенні поставлених завдань використано порівняльний аналіз, теоретичні знання та практичні надбання в галузі комп’ютерних мереж та програмного забезпечення.

Для досягнення мети дипломної роботи поставлено такі **завдання:**

1. Аналіз теоретичних аспектів побудови сучасних комп’ютерних мереж підприємств.
2. Вибір та обґрунтування топології і структури мережі.
3. Аналіз та вибір мережевого обладнання.
4. Вибір сервісу відеоспостереження.
4. Вирішення питання *IP*-телефонії.
5. Вирішення питання аудіо- та відеоконференцій.

Дипломна робота бакалавра складається зі вступу, 4 розділів, висновків, списку використаних джерел. Основний текст роботи викладений на 85 сторінках, містить 30 рисунків, 12 таблиць, список джерел з 33 найменувань.

РОЗДІЛ 1
АНАЛІЗ КОНЦЕПЦІЙ ТА РІШЕНЬ ПОБУДОВИ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ВИРОБНИЧИХ ПІДПРИЄМСТВ

1.1. Аналіз концепцій побудови мереж виробничих підприємств

В основний перелік складових елементів телекомунікаційних технологій, присутніх на більшості виробничих підприємств, входять, у вигляді набору, паралельно діючих мереж: телефонної, комп'ютерної, охоронної сигналізації, пожежної сигналізації, диспетчерського зв'язку, управління технологічними процесами, гучномовний зв'язок і деякі інші типи мереж.

Для підтримки перерахованих мереж на нині діючих виробничих підприємствах прокладені тисячі кілометрів кабельних систем. Наймолодшим з них - близько 20 років, основна ж маса має вік більше 40 років [2]. Для цього є свої причини. При проектуванні і будівництві будь-якої промислової будівлі в ньому відразу закладають кабельні траси. У міру розвитку підприємства (будівництво нових цехів, запуск виробництв, створення додаткових служб) еволюціонує і його система комунікації: збільшується абонентська ємність, розгалужується мережа зовнішніх зв'язків.

Однак саме обладнання систем зв'язку зазвичай належить до того ж покоління, що і саме підприємство. Абонентська ємність телефонної мережі розширюється за рахунок прокладки кабелів і установки додаткового обладнання. Проте, рано чи пізно, абонентська ємність АТС досягає своєї межі: кабельна каналізація повністю забита, та й самі кабелі, давно прокладені, майже непрацездатні через важкі умови експлуатації (в каналах, як правило, присутні вода, емульсія, масла).

Виникають складнощі з організацією зовнішніх зв'язків, оскільки наявні автоматичні телефонні станції (АТС) практично не стикуються з новими АТС міського та міжміського зв'язку. Приходить пора заміни обладнання систем зв'язку підприємств. Причому нові АТС доводиться вводити так, щоб не зупиняти всю мережу відразу, таким чином, модернізуючи її поступово. Це відноситься і до кабелів: заміні підлягають тільки міжцехові кабелі, а внутрішня розводка по

будівлях повинна бути збережена.

Комп'ютерні мережі на підприємствах створювалися в такий спосіб. Якщо потрібно під'єднати комп'ютери, що знаходяться в сусідній кімнаті, туди підводився кабель, при необхідності охопити ще одну кімнату проводився інший кабель і т.д. В результаті виходила локальна мережа з досить заплутаною структурою. Описаний підхід до розгортання мережі обмежувався межами одного підприємства, а іноді і одного цеху, підрозділу.

У разі необхідності приєднання комп'ютерів, розташованих в інших будівлях або навіть в інших частинах цеху, словом, на відстані більш 200-300 м, проблеми ставали складнішими.

З появою потужних систем управління виробництвом (наприклад, на базі інтегрованих пакетів *SAP R/3* та *IFS System4*) ефективність використання мереж на виробничих підприємствах стала вкрай низькою.

Відомості про динаміку розвитку виробничих процесів надходять з різних джерел по каналах різної якості, тому часто запізнюються, в результаті чого оперативне управління і планування виявляються відірваними від фактичного стану виробничих об'єктів управління. Диспетчерські служби більшості підприємств працюють чи не на граничному рівні завантаження, вручну реалізуючи багато управлінських процедур, виконуючи великий обсяг рутинних облікових операцій і постійно відволікаючись на телефонні запити [1, 2].

1.2. Основні властивості та складові комп'ютерних мереж

Всеохоплюючий характер. Область дії КМ поширюється на підприємство в цілому. Немає такого підрозділу, який не був би підключений до неї.

Інтеграція. КМ надає можливість доступу її користувачів до будь-яких даних і додатків (в рамках політики інформаційної безпеки). Немає такого інформаційного ресурсу, доступ до якого не можна було б отримати по мережі.

Експлуатаційні характеристики. Мережа має властивість керованості і має високий рівень *RAS* (*reliability, availability, serviceability*) – безвідмовність, живучість, обслуговуваність за підтримки критично важливих для діяльності підприємства сервісів.

Корпоративна мережа – це інфраструктура організації, що підтримує рішення актуальних завдань і забезпечує досягнення її цілей. Вона об’єднує в єдиний інформаційний простір всі об’єкти підприємства. КМ створюється як апаратно-технічна основа корпоративної мережі, як її головний системоутворюючий компонент, на базі якого конструюються інші системи та сервіси [3].

Корпоративну мережу необхідно розглядати в різних аспектах. Загальне уявлення про КМ складається з проекцій, що одержано в результаті її розгляду з різних точок зору.

Корпоративна мережа задумана і проектується в єдиній системі координат, основу якої складає поняття системно-технічної інфраструктури (структурний аспект), системної функціональності (сервіси та додатки) і експлуатаційних характеристик (властивості). Кожне поняття знаходить своє відображення в тому чи іншому компоненті мережі і реалізується в конкретних технічних рішеннях.

З функціональної точки зору КМ – це ефективне середовище передачі актуальною інформації, необхідної для вирішення завдань підприємства. З системно-технічної точки зору мережа являє собою цілісну структуру, що складається з декількох взаємопов’язаних і взаємодіючих рівнів:

- комп’ютерна мережа;
- телекомунікації;
- комп’ютерні платформи;
- ПЗ проміжного шару;
- додатки.

З точки зору системної функціональності КМ виглядає як єдине ціле, яке надає користувачам набір корисних в роботі сервісів, загальносистемних і спеціалізованих додатків, що володіє набором корисних якостей (властивостей).

Одним з принципів, покладених в основу створення КМ, є максимальне використання типових рішень, стандартних уніфікованих компонентів. Конкретизуючи цей принцип стосовно прикладного ПЗ, можна виділити ряд універсальних сервісів, які доцільно зробити базовими компонентами додатків.

Такими сервісами є:

- сервіс системи управління базою даних(СУБД);
- файловий сервіс;
- інформаційний сервіс;
- сервіс *VoIP* телефонії;
- сервіс відеоконференцій;
- мережевий друк і інші.

Відзначимо, що основним засобом для побудови прикладних і системних сервісів є ПЗ проміжного шару. Поняття сервісів ПО проміжного шару корисно при опрацюванні архітектури КМ. Фактично, програмна інфраструктура КМ є багатошаровою. Нижні шари складають низькорівневі сервіси, такі як сервіс імен, сервіс реєстрації, мережевий сервіс і т.д. Вищележачі шари включають сервіси управління документами, управління повідомленнями, подій. Верхній шар являє собою сервіси, до яких опосередковано (через додатки) звертаються користувачі.

КМ зручно описувати в термінах сервісів. Так, наприклад, політику інформаційної безпеки доцільно будувати, виходячи з потреби в захисті існуючих сервісів.

До загальносистемних додатків відносять засоби автоматизації індивідуальної праці, що використовуються різноманітними категоріями користувачів і орієнтовані на рішення типових офісних завдань. Це - текстові процесори, електронні таблиці, графічні редактори, календарі, записні книжки і т.д. Як правило, загальносистемні додатки представляють собою тиражовані локалізовані програмні продукти, нескладні в освоєнні і прості в використанні, орієнтовані на кінцевих користувачів.

Спеціалізовані додатки спрямовані на вирішення завдань, які неможливо або технічно складно автоматизувати за допомогою загальносистемних додатків. Як правило, спеціалізовані додатки або купуються у компаній-розробників, що спеціалізуються в своїй діяльності на конкретну сферу, або створюються компаніями-розробниками на замовлення підприємства, або розробляються силами самої організації. В більшості випадків спеціалізовані програми

звертаються в процесі роботи до загальносистемних сервісів, таких, наприклад, як файловий сервіс, СКБД і т.д. Власне, спеціалізовані додатки та сервіси, що розглядаються в сукупності в масштабах організації, і визначають весь спектр прикладної функціональності.

Як уже зазначалося, термін служби системно-технічної інфраструктури в декілька разів більше, ніж у додатків. КМ забезпечує можливість розгортання нових додатків і їх ефективне функціонування при збереженні інвестицій в неї, і в цьому сенсі повинна мати властивість відкритості, продуктивності і збалансованості, масштабованості, високої готовності, безпеки, керованості. Перераховані властивості, по суті, являють собою експлуатаційні характеристики корпоративної мережі і визначаються в сукупності якістю продуктів і рішень, покладених в її основу. Зрозуміло, хороші показники по конкретних властивостях будуть досягатися за рахунок грамотних технічних рішень системного конструювання. Так, система буде мати властивості безпеки, високої готовності та керованості за рахунок реалізації в проекті КС відповідних служб. Масштабованість в контексті комп'ютерних платформ (наприклад, для серверної платформи) означає можливість адекватного нарощування потужностей комп'ютера (потужності, обсягу інформації, що зберігається і т.д.) і досягається такими якостями лінії серверів, як плавне нарощування потужності від моделі до моделі, єдина ОС для всіх моделей, зручна і продумана політика модифікації молодших моделей в напрямку старших (*upgrade*).

Загальносистемні служби – це сукупність ПЗ, що не спрямовані безпосередньо на рішення прикладних задач, але необхідні для забезпечення нормального функціонування корпоративної мережі підприємства. В якості обов'язкових, в КМ повинні бути включені служби інформаційної безпеки, централізованого моніторингу і адміністрування.

Розглянутий набір понять є досить абстрактним для того, щоб сформулювати КМ поза прив'язкою до конкретних програмно-апаратних рішень і в той же час достатньо конкретний для визначення корисної функціональності (сервіси та додатки як засіб вирішення завдань користувача КМ) і

експлуатаційних характеристик (властивості і служби) корпоративної мережі [2, 3, 13].

Викладені вище поняття і принципи цілком конкретні. Будучи прийнятими в якості основоположних при побудові КМ, вони виливаються в конкретні кроки і технічні дії.

1.3. Принципи створення корпоративних мереж виробничих підприємств

Необхідність подальшого розвитку КМ виробничих підприємств диктується, перш за все, зростанням внутрішніх потреб різних служб підприємств в інформаційних сервісах. Існуюча інфраструктура в якийсь момент перестала справлятися із збільшеними навантаженнями, а спроби її розширення стали наштовхуватися на непереборні труднощі.

Телефонія все активніше використовує цифрову передачу даних. В результаті комп'ютерна та телефонна мережі виявилися тісно інтегрованими, якщо не сказати - невіддільними один від одного. Звідси можна зробити закономірний висновок про те, що проектування і монтаж обох мереж повинні здійснюватися як єдиний процес у рамках однієї кабельної системи, загальної інформаційної магістралі (ІМ). Інтеграція трафіку всіх існуючих мереж підприємства в єдину кабельну систему багаторазово скорочує витрати на побудову, розвиток і обслуговування. Формування єдиної ІМ робить проект дорожчим на 10-15% (в порівнянні з витратами на розгортання кожної мережі), тоді як будівництво всіх мереж окремо збільшує загальну вартість у стільки разів, скільки таких мереж створюється.

При проектуванні будь-якої мережі з точки зору потенційних витрат на подальший розвиток виробництва важливим є питання про відносну значущість телекомунікаційного середовища (базиса) і ПЗ (надбудови). Тут є доречною аналогія з фундаментом і дахом будівлі. Фундамент – основа будівлі, але з напівзруйнованим дахом жити неможливо. З цих позицій сперечатися про відносну значимість окремих компонентів можна дуже довго. Тим часом дилема однозначно вирішується на користь фундаменту, якщо поставити питання інакше:

що буде простіше розширити, надбудувати або модернізувати при виникненні такої необхідності в подальшому?

Фундаментом інформаційної інфраструктури будівлі є кабельна система. Прокладка кабелю, особливо в складних виробничих умовах, та його захист від зовнішнього впливу вимагають чималих разових витрат. У той же час з встановленою кабельною системою користувачеві доводиться працювати набагато довше, ніж з комп'ютерним обладнанням чи ПЗ. В умовах змін самого об'єкта автоматизації, постійного створення нових технологій і тенденцій важливо, щоб кабельна система забезпечила мережеву життєдіяльність організації на 20-30 років (за міжнародними стандартами не менше ніж на 10 років), не наражаючись на кардинальні зміни [2].

На розширення або модернізацію кабельної системи в будівлі, що експлуатується потрібно витрачати набагато більше коштів, ніж на її первинний монтаж. Забезпечити просту модифікацію і розширення кабельної системи в складних виробничих умовах, не перериваючи життєдіяльності підприємства, зовсім непросто. Щоб кабельна система була здатна працювати з з новими технологіями, її початкова пропускна здатність повинна значно перевищувати поточні потреби і передбачати високі швидкості передачі. Існуючу ж інтенсивність трафіку слід взяти до уваги тільки при виборі активного мережного обладнання, хоча і в цьому випадку доцільно передбачити деякий запас пропускної здатності.

Сьогодні найбільш поширеною технологією для створення інформаційної мережі будівлі є структурована кабельна система (СКС), побудована на мідних і оптичних кабелях, яка поєднує передачу різних видів трафіку (мовних сигналів, комп'ютерних даних, сигналів аварійної та пожежної систем, систем контролю за вентиляцією, кондиціонуванням, опаленням і т.і.) і дозволяє оперативно збільшувати кількість користувачів. Як показує досвід, початкові вкладення в розумно спроектовані СКС носять довготривалий характер, оскільки зводять до мінімуму подальші експлуатаційні витрати і витрати на розширення і модифікацію. У той же час доводиться констатувати, що багато організацій не в

змозі повністю або достатньо ефективно використовувати можливості технології СКС в своїх виробничих або адміністративних приміщеннях, які були спроектовані і обладнані без урахування потреб автоматизації.

Сама суть СКС – забезпечити доступ до інформації з кожного робочого місця вимагає охоплення всієї будівлі і наявності достатньої кількості розгалужених комунікаційних каналів. Будучи невід'ємною частиною систем життєзабезпечення виробництва, СКС повинна проектуватися одночасно з самою будівлею.

Одна з особливостей промислового виробництва, що позначається на засобах автоматизації, - сильні електромагнітні перешкоди від автоматичних підйомників, електропечі, верстатів та іншого цехового обладнання, значна запиленість приміщень і територій. Специфіка виробничого середовища вимагає підвищеної уваги до засобів захисту комунікаційного та комп'ютерного обладнання, а також певних витрат.

При цьому слід враховувати, що характер виробництва передбачає безперебійну роботу віддалених від заводоуправління основних служб (склади, адміністративні будівлі і таке інше). Розрив зв'язку цих служб з основними інформаційними базами підприємства більш ніж на короткотривалий термін неприпустимий. Це обумовлює необхідність введення в основних підмережах режиму реального часу, а значить, і високих швидкостей передачі (100-150 Мбіт/с і вище). До сказаного треба додати, що в сучасних умовах дуже важливо забезпечити конфіденційність та збереження комерційної інформації підприємства.

Вимоги надійного захисту і високій швидкості передачі даних диктують необхідність в використанні оптичних кабелів в якості ліній зв'язку. Крім усього іншого оптичне середовище дозволяє підняти швидкість передачі на 3-4 порядки, в порівнянні з мідними лініями, при дуже високій якості.

Існує думка, що рішення на основі оптоволокна дорогі і до того ж призначені для спеціальних додатків. Що стосується другої тези, уявлення про екзотичність волоконної оптики позбавлені будь-яких підстав. Досить сказати, що

в армії США оптоволокно застосовується для оперативного зв’язку нижчої ланки (до рівня взводу) в бойових умовах. В Японії – висить на стовпах, як у нас електропроводи.

З економічного боку початкові витрати на волоконну оптику дійсно вище, ніж на мідні системи, але ця різниця дуже швидко і багаторазово окупається. По-перше, витрати на обслуговування волоконно-оптичних систем набагато нижче, ніж в разі багатожильного мідного кабелю. По-друге, більш висока пропускна здатність пропорційно зменшує вартість передачі одиниці інформації.

По своїй фізичній природі самі оптоволоконні кабелі не випромінюють (що дозволяє забезпечити повну захищеність переданої інформації), несприйнятливі до будь-яких видів електромагнітних перешкод, мало схильні до дії вологи, кислот, солей і нафтохімічних забруднень, які характерні для умов експлуатації на виробничих підприємствах.

Передавати інформацію без ретрансляції можна на відстані до 2-5 км на багатомодовому і до 70 км на одномодовому волокні. Це дозволяє побудувати всю комунікаційну інфраструктуру підприємства без єдиної станції ретрансляції. Виходячи з вище сказаного, зроблені інвестиції залишаться актуальними протягом мінімум 20 років.

В умовах великої різноманітності кабельних систем і мережевого устаткування, яке часом погано між собою стикується, завжди залишається проблема вибору конкретного рішення з наявних на ринку. У складних умовах промислового виробництва прокладка і монтаж кабелю пов’язані з низкою проблем. Побудова мережі на основі оптоволокна вимагає високої кваліфікації. Так, для отримання оптимальної структури кабельної системи необхідно враховувати десятки параметрів (таких як дисперсія, апертура, довжина хвилі випромінення, смуга пропускання, модальність оптичного волокна, типи кінцевих роз’ємів, передавачів і приймачів, кількість і типи з’єднувальних муфт, діаметри волокон і метод їх з`єднання) і спеціально підбирати кабелі та обладнання для передачі на потрібну відстань (особливо якщо вона перевищує 2 км). Крім того, апаратура передачі повинна бути узгоджена з кабельною мережею [2-4].

Можна зробити висновок, що наскільки професійно буде побудована кабельна система, настільки гнучкими і надійними виявляться інформаційні зв’язки і комунікації.

1.4. Багаторівневий підхід при побудові мультисервісних мереж

При побудові корпоративних мультисервісних мереж величезну роль відіграє правильний вибір архітектури і топології мережі, який повинен передбачати багаторівневий підхід. Він полягає в поданні архітектури створюваної мережі у вигляді ієрархічних рівнів, кожен з яких вирішує певні для цього рівня завдання. Це дозволяє:

- безболісно для мережі додавати різні рівні, що розширюють функціональні можливості мережі;
- мінімізувати ресурсні витрати для пошуку і усунення несправностей в мережі.

1.4.1. Трьохрівнева модель мережі

Типовий ієрархічний дизайн мережі підприємств включає в себе наступні три рівні (рис 1.1):

- рівень ядра;
- рівень розподілу;
- рівень доступу.

Рівень ядра в буквальному сенсі є серцем всієї мережі. Розташовуючись на самій вершині ієрархії, рівень ядра відповідає за швидку і надійну передачу великих об’ємів трафіку. Головним завданням рівня ядра є максимально швидка передача трафіку. Трафік, що передається через ядро, є загальнодоступним для більшості користувачів. Однак необхідно запам’ятати, що дані користувачів обробляються на рівні розподілу, а рівень розподілу відправляє запити ядру тільки в мірі необхідності. Будь-яка відмова на рівні ядра може відбитися на всіх без винятку користувачів. З цього випливає, що проблема відмовостійкості для цього рівня є дуже важливою.

Через ядро, будуть проходити великі обсяги трафіку, тому швидкість і величина затримки є визначальними. Зрозумівши функції ядра, можна тепер

розглянути деякі особливості його створення. На рівні ядра небажано реалізовувати:

- не слід реалізовувати те, що уповільнювало б обробку трафіку. Сюди входить використання списків доступу, маршрутизація між віртуальними локальними мережами (*VLAN*) і фільтрація пакетів;
- на цьому рівні не слід підтримувати доступ для робочих груп.

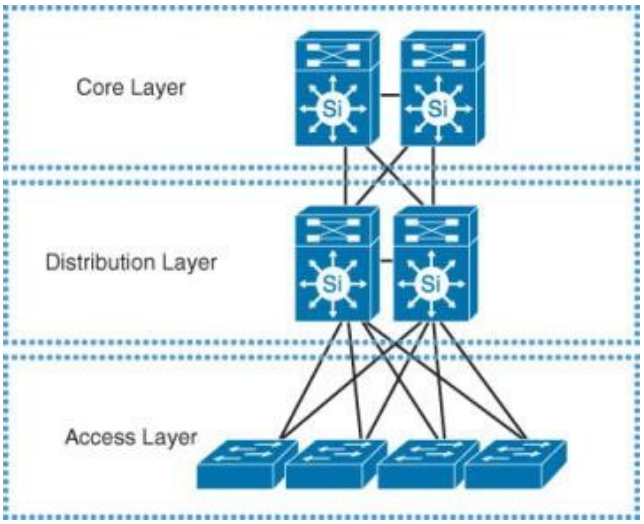

Рис. 1.1. Трьохрівнева модель мережі

Вимоги при розробці ядра:

- ядро має забезпечувати максимально високий рівень надійності;
- слід вибирати технології канального рівня, орієнтовані на високу швидкість при наявності резервних каналів - як, наприклад, *FDDI, Fast Ethernet* або *ATM;*
- слід вибирати протоколи з малим часом оповіщення. Наявність швидких з'єднань на канальному рівні і резервування з'єднань нічим не допоможе, якщо таблиці маршрутизації давно застаріли;

Рівень розподілу, який іноді називають рівнем робочих груп, - це рівень, що забезпечує взаємодію між рівнем доступу і рівнем ядра. Першочерговими функціями рівня розподілу є забезпечення маршрутизації, фільтрації і доступу до глобальної мережі, а також визначення того, яким чином пакет може отримати доступ до ядра при виникненні такої необхідності. Рівень розподілу повинен

визначати найбільш швидкий маршрут для користувача запитів, наприклад, маршрут, який повинен використовуватися пакетом запиту файлу при його відправці на сервер. Після того як рівень розподілу вибере найкращий маршрут, він відправляє запит на рівень ядра.

Тепер уже рівень ядра відповідальний за швидку пересилку запиту відповідній службі.

Рівень розподілу – це місце, де повинні застосовуватися мережеві політики. Саме тут є можливість використовувати значну гнучкість при визначенні роботи мережі. На рівні розподілу як правило реалізовується:

- списки доступу, фільтрація пакетів і організація черг;
- забезпечення безпеки і реалізація правил роботи мережі, включаючи перетворення адрес і міжмережеві екрани;
- розсилка таблиць протоколів маршрутизації, включаючи статичну маршрутизацію;
- виконання маршрутизації між віртуальними локальними мережами та інші функції підтримки робочих груп;
- визначення областей груповий і широкомовної розсилок.

Єдине, чого слід уникати на рівні розподілу, - це виконання функцій, які повинні бути притаманні виключно одному з двох інших рівнів.

Рівень доступу здійснює контроль за доступом користувачів і робочих груп до мережевому комплексу. Рівень доступу іноді називається рівнем настільних систем. Мережеві ресурси, які необхідні більшості користувачів, можуть бути виділені локально. Будь-які звернення до віддалених служб здійснюються на рівні розподілу. Функції, які повинні бути представлені на цьому рівні, включають в себе:

- створення окремих колізійних доменів (сегментація);
- забезпечення взаємодії робочих груп з рівнем розподілу;
- управління доступом користувачів і політиками мережі.

На рівні доступу можуть використовуватися такі технології, як комутація *DDR* (*Dialon-Demand Routing* – маршрутизація з викликом у міру необхідності) і

Ethernet. Не слід додавати нові маршрутизатори нижче рівня доступу. Такі дії призводять до збільшення діаметра мережі, що порушить передбачуваність топології [8, 37].

1.4.2. Двохрівнева модель мережі

Двохрівнева модель (рис. 1.2) підходить для невеликих і середніх мереж, де функції ядра та функції розподілу можуть бути об’єднані в один рівень.

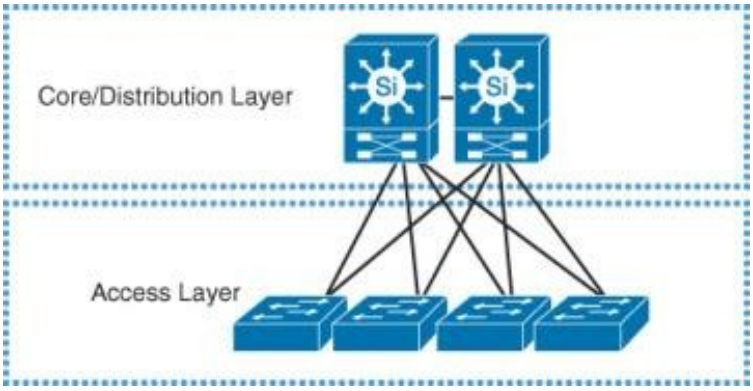

Рис. 1.2. Двохрівнева модель мережі

Відома, також, як згорнута архітектура розподілу ядра.

1.5. Рішення побудови мультисервісної корпоративної мережі

Побудова сучасної корпоративної мережі тісно пов’язана з необхідністю забезпечення успішного функціонування існуючих і планованих бізнес-додатків, а також організацією сучасної багатофункціональної системи корпоративної телефонії та впровадженням відеододатків (відеоконференцій, програми дистанційного навчання).

1.5.1. Використання Cisco AVVID

Для вирішення цих завдань, компанія *Cisco* розробила архітектурну модель побудови мережі, що забезпечує можливість інтеграції різних додатків даних, голосу і відео в рамках єдиної інтелектуальної мережевої інфраструктури (рис. 1.3).

Архітектура систем з інтеграцією голосу, відео і даних, запропонована компанією *Cisco Systems* (*Cisco Architecture for Voice, Video and Integrated Data*)

складається з чотирьох основних компонентів, таких як:

1. Інтелектуальна мережева інфраструктура на базі протоколу *IP*, що включає в себе маршрутизатори, комутатори, шлюзи та інше мережеве обладнання. *IP* інфраструктура є основою для подальшого впровадження призначених для користувача додатків і повинна забезпечувати підтримку таких життєво важливих для мережі сервісів, як безпека, мережеве управління і механізмів гарантії якості сервісу *Quality of Service*(*QoS).*

2. Інтелектуальні клієнтські місця з підтримкою протоколу *IP*, в тому числі цифрові *IP*-телефони *Cisco*, персональні комп'ютери із спеціалізованим програмним забезпеченням для вирішення різних бізнес-задач, програмні емулятори телефонів (наприклад, *Cisco IP SoftPhone*), відео клієнти та ін.

3. Службові серверні додатки, в тому числі сервери *Cisco CallManager*, щоб забезпечити управління корпоративною системою *IP* телефонії, корпоративна система директорій, відео сервери.

4. Сучасні користувальницькі додатки, які отримали завдяки розвитку інтегрованих систем з підтримкою голосу, відео і даних, - наприклад, система уніфікованої обробки повідомлень (*Unified Messaging*) або інтелектуальні центри обробки викликів. Впровадження подібних програм дозволяє забезпечити додаткові можливості для користувачів/абонентів корпоративної мережі, підвищити зручність і ефективність використання системи.

Характерною рисою даної архітектури є її розподілена природа, завдяки якій система легко масштабується. Мережа на базі архітектури *Cisco AVVID* може охоплювати одну будівлю або кілька поруч розташованих будинків, об'єднаних високошвидкісною кампусовою мережею. Також можна забезпечити сервіси телефонії, відео і даних для користувачів віддалених офісів і підрозділів, об'єднаних корпоративною *IP* мережею. Інша відмінна риса архітектури *Cisco AVVID* – це її відкритість, орієнтація на використання відкритих стандартів (зокрема, стандартних протоколів *H.323* і *MGCP* для передачі голосу і відео в мережах *IP*). Це дозволяє забезпечити поєднання з цілим рядом інших систем, як традиційної, так і пакетної телефонії, а також з системами передачі даних і відео.

Підтримка відкритих стандартних протоколів і відкритих інтерфейсів для розробки додатків (таких як *TAPI* і *JTAPI*), забезпечує можливість написання нових додатків, що інтегруються в системи на базі *Cisco AVVID*, а також можливість інтеграції додатків, написаних сторонніми виробниками.

Забезпечення послуг телефонії на базі мережі передачі даних дозволяє позбутися від необхідності експлуатації роздільних мереж для передачі даних і телефонного зв'язку і забезпечує можливість більш повного задоволення потреб підприємств в послугах телефонії. Продукція *Cisco IP* телефонії дозволить замовнику зменшити витрати на впровадження, підтримку і розширення об'єднаної мережі і, як наслідок, підвищити рентабельність телекомунікаційної мережі [5].

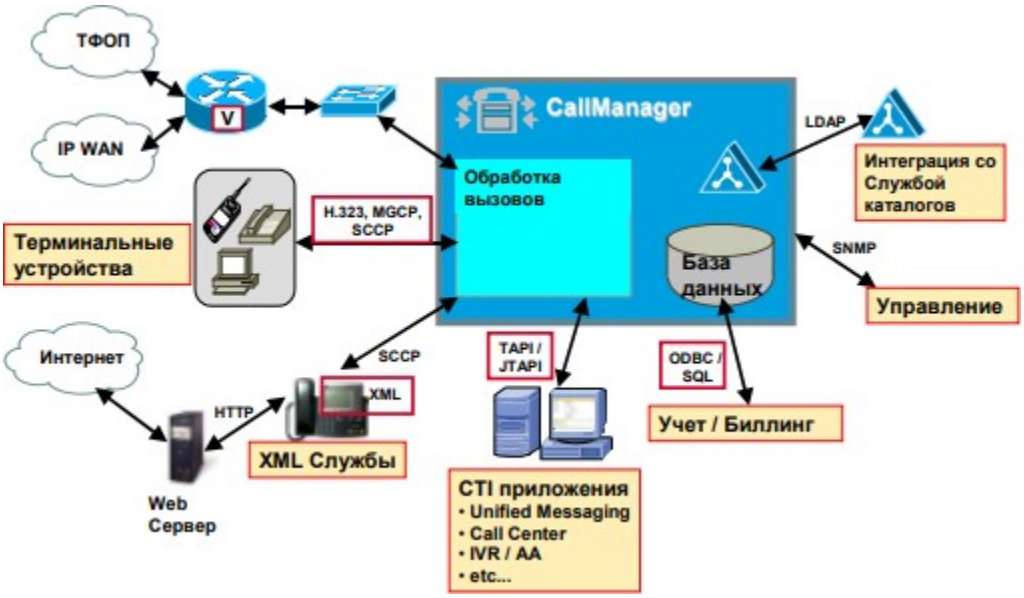

Рис. 1.3. Інтеграція з додатками на основі відкритих протоколів та інтерфейсів для розробки додатків (*API*)

Переваги технології *Cisco AVVID*:

- можливість побудови єдиної телекомунікаційної інфраструктури на базі корпоративної *IP* мережі;
- простота побудови розподілених телефонних і телекомунікаційних систем за рахунок розподіленої природи архітектури *Cisco AVVID*;
- зниження загальної вартості володіння системою;
- скорочення витрат на канали за рахунок можливості ефективного

використання каналів для спільної передачі голосового трафіку, даних і трафіку відеододатків;

- скорочення витрат на оплату міжміських переговорів;
- спрощення налаштування, підтримки і адміністрування телекомунікаційної інфраструктури.
- можливість використання додатків, що використовують переваги інтеграції голосу, відео і даних в рамках єдиної телекомунікаційної інфраструктури;
- орієнтація на підтримку відкритих протоколів та інтерфейсів для розробки додатків (*API*), що забезпечує можливість інтеграції з широким спектром додатків, пропонованих в даний час різними виробниками.

Недоліки:

- неможливість використання стороннього обладнання, окрім продуктів *Cisco Systems;*
- висока вартість системи;
- застарілі інтерфейси для розробки додатків.

Як бачимо, дане рішення від *Cisco Systems* підходить далеко не усім підприємствам. Впершу чергу, воно є актуальним для великих компаній, які сильно зав'язані на використанні *IP*-телефонії та обробці великої кількості вхідних дзвінків. У компаніях, де *IP*-телефонія використовується лише працівниками підприємства, дане рішення буде надлишковим. Не менш важливим моментом є те, що рішення *Cisco Systems* вимагають досить великих фінансових затрат.

1.5.2. Використання Huawei One Net

Компанія *Huawei* розробляючи рішення побудови мультисервісних корпоративних мереж *One Net* (рис. 1.4), поставила перед собою наступні вимоги:

- розвиток мережевих сервісів: філіальна мережа повинна розвиватися з послугами, які вона надає;
- мультисервісність: підвищені вимоги до призначених для користувача додатків, при цьому забезпечуючи якість для кожного сервісу окремо;

- безпека користувача: повна мережева захист повинен бути забезпечена по всьому периметру філіальної мережі;

- управління та обслуговування: управління та обслуговування повинно бути простим і доступним для зниження управлінських витрат і експлуатаційних витрат (*OPEX*).

Філії можуть отримати прямий доступ до мультисервісної корпоративної мережі головного офісу, використовуючи:

- інтегрований доступ: надає дротовий і бездротовий доступ до корпоративной мережі через різні типи інтерфейсів, такі як *Ethernet, WLAN, PON, XDSL, E1 / T1, ISDN, POS, і 3G;*

- сервіси: користувачі можуть спілкуватися використовуючи інтерактивні сервіси в режимі реального часу, такі як телефонія, відеоконференція і відеоспостереження;

- інтегровану платформу: формується єдина мультисервісна корпоративна мережа і корпоративні мережеві політики на базі маршрутизаторів, комутаторів і міжмережевих екранів до кінцевої станції, що значно знижує експлуатаційні витрати на мережу.

В деяких випадках термінали повинні мати доступ до корпоративних ресурсів з відкритих доступних незахищених мереж, такі мережі як в готелях, аеропортах, які мають потенційно високі ризики з точки зору безпеки для корпоративних мереж. Рішення з безпеки *One Net* для філій допомагає захистити корпоративні мережі та ресурси одним із таких способів:

- *VPN* з'єднання: організація гнучких, масштабованих і зашифрованих *VPN* туннелей для забезпечення зв'язку в межах мультисервісної корпоративної мережі;

- прикордонна безпека: забезпечення надійної мережевої безпеки по периметру корпоративної мережі, до складу якої входять фаерволи, *Intrusion Protection System (IPS) і Intrusion Detection System (IDS)*;

- безпека рівня доступу: аутентифікація користувачів терміналів, керування політиками доступу, а також управління правами користувачів для забезпечення віддаленого доступу.

Рис. 1.4. Типова топологія корпоративної мережі

Рішення *One Net* поставляється з програмним забезпеченням (система управління) *eSight* для мультисервісної корпоративної мережі, що спрощує віддалене керування та обслуговування мережі та надає [6]:

- безперервне управління;
- простоту розгортання;
- підтримку відкритих стандартів.

Висновки за розділом 1

Корпоративна мережа – це інфраструктура організації, що підтримує рішення актуальних завдань і забезпечує досягнення її цілей. Вона об’єднує в єдиний інформаційний простір всі об’єкти підприємства. КМ створюється як апаратно- технічна основа корпоративної мережі, як її головний системоутворюючий компонент, на базі якого конструюються інші системи та сервіси.

Термін служби системно-технічної інфраструктури в декілька разів більше, ніж у додатків та сервісів. КМ забезпечує можливість розгортання нових сервісів і

їх ефективне функціонування при збереженні інвестицій в неї, і в цьому сенсі повинна мати властивість продуктивності, масштабованості та керованості.

Рекомендується використання багаторівневого підходу при побудові мультисервісної корпоративної мережі, а саме трьохрівневої моделі. Такий підхід полягає в поданні архітектури створюваної мережі у вигляді ієрархічних рівнів, кожен з яких вирішує певні для цього рівня завдання. Це дозволяє безболісно для мережі додавати різні рівні, що розширюють функціональні можливості мережі та мінімізувати ресурсні витрати для пошуку і усунення несправностей в мережі.

Розглянуто та проаналізовано існуючі рішення побудови мультисервісних корпоративних мереж таких як *Cisco AVVID* та *Huawei One Net*. Рішення від *Cisco Systems* підходить далеко не усім підприємствам. В першу чергу, воно є актуальним для великих компаній, які сильно зав’язані на використанні *IP*-телефонії та обробці великої кількості вхідних дзвінків. У компаніях, де *IP*-телефонія використовується лише працівниками підприємства, дане рішення буде надлишковим. Не менш важливим моментом є те, що рішення *Cisco Systems* вимагають досить великих фінансових затрат. Рішення від *Huawei* в свою чергу не має прив’язки до конкретних виробників мережевого обладнання, має централізовану систему управління мережею *eSight* та постачає власні різноманітні сервіси, в тому числі із використанням штучного інтелекту.

РОЗДІЛ 2
СТРУКТУРА МУЛЬТИСЕРВІСНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1. Загальна структура мережі

Структурно дане підприємство складається з наступних підрозділів:

- головний офіс;
- виробництво;
- склад;
- офіс.

Усі вони є географічно віддаленими та мають вихід у мережу *Internet*, тому доцільно буде використати її для з'єднання сегментів корпоративної мережі. Таким чином, загальна структура мультисервісної корпоративної мережі підприємства матиме наступний вигляд (рис. 2.1):

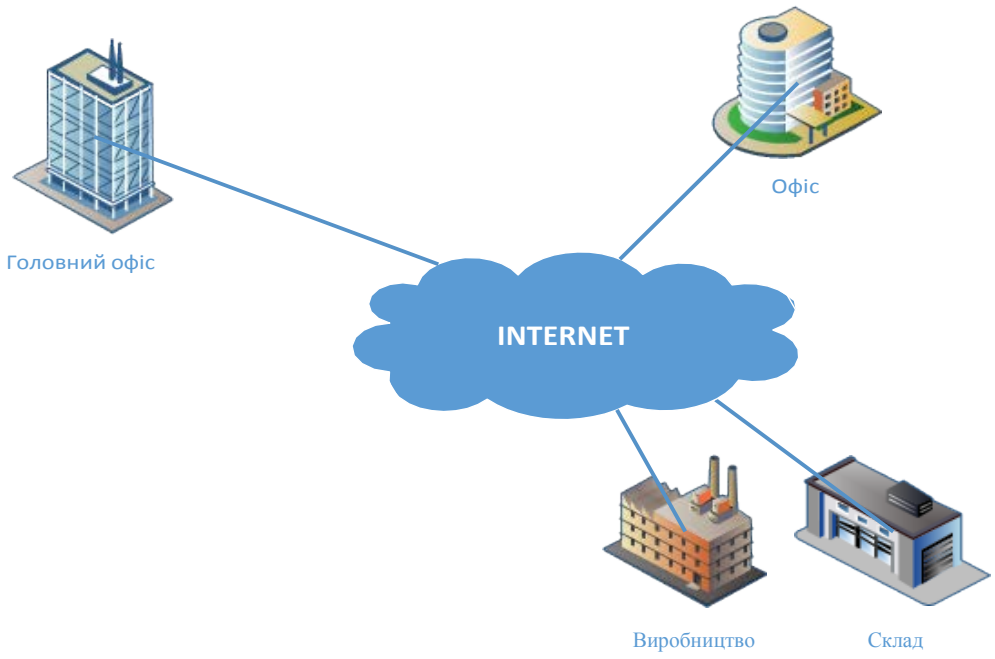

Рис. 2.1. Загальна структура мультисервісної корпоративної мережі

Об'єднуючи в мережу кілька (більше двох) комп'ютерів, необхідно вирішити, яким чином з'єднати їх один з одним, іншими словами, вибрати конфігурацію фізичних зв'язків, або їх топологію.

2.2. Вибір та обґрунтування топології мережі

Під топологією мережі розуміється конфігурація графа, вершинам якого відповідають кінцеві вузли мережі (наприклад, комп'ютери) і комунікаційне обладнання (наприклад, маршрутизатори), а ребрам – інформаційні зв'язки між вершинами. Від вибору топології зв'язків істотно залежать характеристики мережі. Наприклад, на відмінність між вузлами декількох шляхів підвищує надійність мережі і робить можливим розподіл завантаження між окремими каналами. Простота приєднання нових вузлів, що властива деяким топологіям, робить мережу легко масштабованою. Економічні міркування часто приводять до вибору топологій, для яких характерна мінімальна сумарна довжина ліній зв'язку. Серед безлічі можливих конфігурацій розрізняють повнозв'язні (рис. 2.2, а) і неповнозв'язні (рис. 2.2, б).

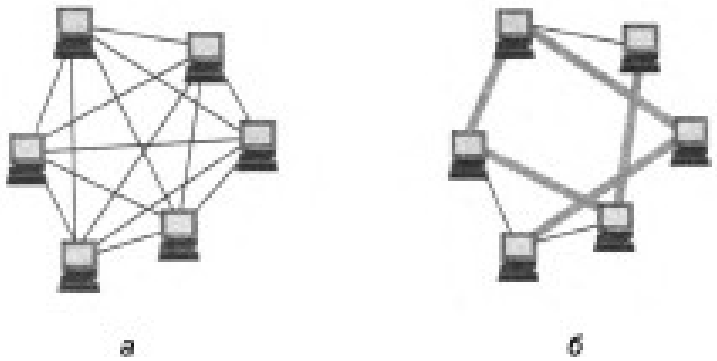

Рис. 2.2. Конфігурація мережі: а – повнозв'язна, б – неповнозв'язна

Повнозв'язна топологія відповідає мережі, в якій кожен комп'ютер безпосереднім чином пов'язаний з усіма іншими. Незважаючи на логічну простоту, цей варіант виявляється на практиці громіздким і неефективним. Дійсно, в такому випадку кожен комп'ютер в мережі повинен мати велику кількість комунікаційних портів, достатню для зв'язку з кожним з інших комп'ютерів мережі. Для кожної пари комп'ютерів повинна бути виділена окрема фізична лінія зв'язку (в деяких випадках навіть дві, якщо неможливе використання цієї лінії для двосторонньої передачі).

Повнозв'язні топології в великих мережах застосовуються рідко, так як для зв'язку N вузлів потрібно $N(N - 1)/2$ фізичних дуплексних ліній зв'язків, тобто має

місце квадратична залежність від числа вузлів. Зазвичай цей вид топології використовується в багатомашинних комплексах або в мережах, які об’єднують невелику кількість комп’ютерів.

Всі інші варіанти засновані на неповнозв’язних топологіях, коли для обміну даними між двома комп’ютерами може знадобитися транзитна передача даних через інші вузли мережі.

В даному випадку структури підприємства, доцільно буде використати топологію ієрархічної зірки(дерева). Сама по собі, зіркоподібна топологія утворюється в разі, коли кожен комп’ютер підключається безпосередньо до загального центрального пристрою, що зветься концентратором. У функції концентратора входить передача переданої комп’ютером інформації одному або всім іншим комп’ютерам мережі. В ролі концентратора може виступати як універсальний комп’ютер, так і спеціалізований пристрій.

Ієрархічна зірка (рис. 2.3), будується ж з використанням декількох концентраторів, що ієрархічно з’єднанні між собою зіркоподібними зв’язками [7].

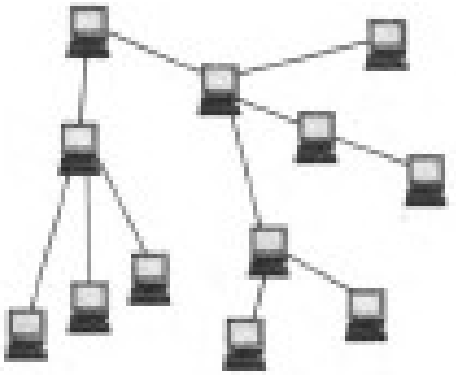

Рис. 2.3. Топологія «ієрархічна зірка»

Перевагами обраної топології є:

- масштабованість;
- легкий пошук проблемних вузлів;
- висока продуктивність мережі.

Недоліки:

- вихід з ладу концентратора впливає на роботу всієї мережі;

- високі витрати кабелів.

Можна побачити, що обрана топологія мережі найкраще підходить для даного підприємства. Збільшені витрати на додаткові кабелі легко нівелюються її перевагами. А вразливість концентраторів вирішується за допомогою технологій стекування комутаторів.

2.3. Аналіз віртуальних мереж

2.3.1. Віртуальна приватна мережа

Віртуальна приватна мережа (*VPN*) - це приватна мережа передачі даних, яка використовує загальнодоступний комп'ютерну мережу, наприклад Інтернет, шляхом додавання процедур безпеки над незахищеними канали зв'язку. Це досягається, використовуючи комбінацію шифрування, автентифікації та тунелювання. "Тунелювання" (іноді його називають інкапсуляцією) відноситься до процесу інкапсуляції або вбудовування одного мережевого протоколу, який буде передаватися, в пакети іншого [9].

Технологія *VPN* надає компанії можливості дорогої приватної орендованої лінії за набагато нижчою вартістю, використовуючи спільну мережу, таку як Інтернет (рис. 2.4, а).

Існує кілька різних реалізацій протоколів *VPN*. Найбільш вживані протоколи віртуальних приватних мереж наступні [10]:

- *Point-to-Point Tunneling Protocol (PPTP);*
- *Layer 2 Tunneling Protocol (L2TP);*
- *Internet Protocol Security (IPSec);*
- *SOCKS.*

Перевага використання Інтернету для зв'язку в тому, що тунелі можуть бути бути створеним за вимогою та включати, наприклад, працівника, який знаходиться вдома або подорожує, та має з'єднання з Інтернетом. Гнучкість є вищою, чим у виделенних ліній, та з точки зору користувачів топологія даної приватної мережі виглядає як локальна мережа, що показано на рис. 2.4, б.

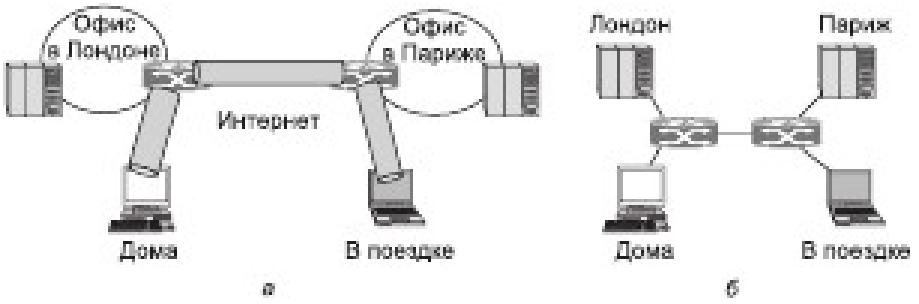

Рис. 2.4. Віртуальна приватна мережа:
а – приклад топології, б – топологія з точки зору користувачів

Захист інформації в процесі передачі її по відкритих каналах засновується на побудові захищених віртуальних каналів зв’язку, що називаються криптозахищеними тунелями. Кожен такий тунель представляє собою з’єднання, що проходить через відкриту мережу, по якому передаються криптографічно захищені пакети повідомлень.

Створення захищеного тунеля виконують компоненти віртуальної мережі, що функціонують на вузлах, між якими формується тунель. Ці компоненти прийнято називати ініціатором і термінатором тунеля. Ініціатор тунеля інкапсулює пакети в новий пакет, що містять новий заголовок з інформацією про відправлення та отримання. Хоча всі пакети, що передаються по каналу є пакетами *IP*, інкапсульовані пакети можуть належати до будь-якого протоколу. Маршрут між ініціатором і термінатором тунеля визначає звичайна *IP*-мережа, якою може бути мережа Інтернет або будь-яка інша. Термінатор тунеля виконує процес зворотній інкапсуляції – він видаляє нові заголовки і направляє кожен вхідний пакет у локальному стеці протоколів адресату в локальної мережі.

Сама по собі інкапсуляція ніяк не впливає на захист пакетів повідомлень, що передаються по тунелю. Але завдяки інкапсуляції з’являється можливість повного криптографічного захисту інкапсульованих пакетів. Конфіденційність інкапсульованих пакетів забезпечується шляхом криптографічного закриття, тобто зашифрування, а цілісність і справжність – за допомогою формування цифрового підпису. Так як існує велика кількість методів криптозахисту даних, дуже важливо, щоб ініціатор і термінатор тунеля використовували одні і ті ж

методи і могли узгодити дані методи. Крім того, для можливості розшифрування даних та перевірки цифрового підпису при прийомі ініціатор та термінатор тунеля повинні підтримувати функції безпечного обміну ключами. Ну і нарешті, щоб тунелі створювались лише між уповноваженими користувачами, кінцеві сторони взаємодії потрібно аутентифікувати [11].

2.3.2. Віртуальна локальна мережа

Віртуальна локальна мережа це група вузлів мережі, трафік якої, що включає в себе і широкомовний, на канальному рівні повністю ізольований від трафіку інших вузлах мережі.

Основне призначення технології *VLAN* в полегшенні процесу створення ізолювання мереж, які потім зазвичай зв’язуються між собою за допомогою маршрутизаторів. Така побудова мережі створює потужні бар’єри на шляху небажаного трафіку з однієї мережі в іншу. Сьогодні вважається очевидним, що будь-яка велика мережа повинна включати маршрутизатори, інакше потоки помилкових кадрів, наприклад широкомовних, будуть періодично «затоплювати» всю мережу через прозорі для них комутатори, приводячи її в неробочий стан.

Перевагою технології віртуальних мереж є те, що вона дозволяє створювати повністю ізольовані сегменти мережі шляхом логічної конфігурації комутаторів, не вдаючись до зміни фізичної структури. При створенні віртуальних мереж на основі одного комутатора зазвичай використовується механізм групування портів комутатора (рис. 2.5). При цьому кожен порт відноситься тій чи іншій віртуальній мережі. Кадр, що прийшов на порт, що належить, наприклад, віртуальній мережі 1, ніколи не буде переданий порту, який не належить цій віртуальній мережі. Втім, порт можна приписати декільком віртуальним мережам, хоча на практиці так роблять рідко – зникає ефект повної ізоляції мереж.

Якщо вузли будь-якої віртуальної мережі підключені до різних комутаторів, то для підключення кожної такої мережі на комутаторах повинна бути виділена спеціальна пара портів. В іншому випадку, якщо комутатори будуть пов’язані тільки однією парою портів, інформація про приналежність кадру тієї чи іншої віртуальної мережі при передачі з комутатора в комутатор буде загублена. Таким

чином, комутатори з групуванням портів вимагають для свого з'єднання стільки портів, скільки віртуальних мереж вони підтримують.

Порти і кабелі використовуються в цьому випадку дуже марнотратно. Крім того, при з'єднанні віртуальних мереж через маршрутизатор для кожної віртуальної мережі виділяються окремі кабель і порт маршрутизатора, що також призводить до великих накладних витрат.

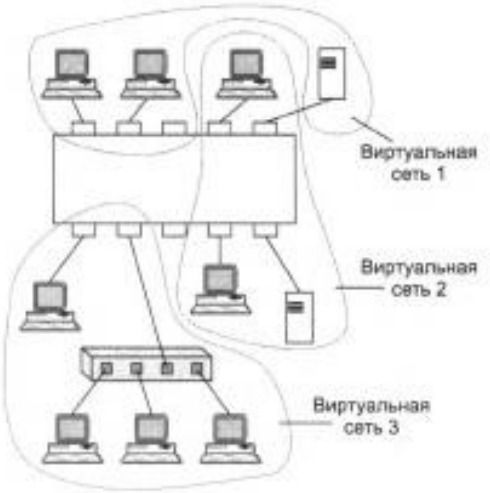

Рис. 2.5. Віртуальні мережі, побудовані на одному комутаторі

Групування MAC-адрес у віртуальну мережу на кожному комутаторі позбавляє від необхідності пов'язувати їх з кількох портів, оскільки в цьому випадку MAC- адреса стає міткою віртуальної мережі. Однак цей спосіб вимагає виконання великої кількості ручних операцій по маркуванню MAC-адрес на кожному комутаторі мережі.

Обидва підходи засновані тільки на додаванні додаткової інформації до адресних таблиць комутатора і в них відсутня можливість передачі в кадрі інформації про приналежність кадру до віртуальної мережі. Тому широке поширення отримав інший підхід, заснований на введенні в кадр додаткового поля, яке зберігає інформацію про приналежність кадру тієї чи іншої віртуальної локальної мережі при його переміщеннях між комутаторами мережі. При цьому немає необхідності пам'ятати в кожному комутаторі про приналежність всіх MAC-адрес до віртуальних мереж. Додаткове поле з позначкою про номер віртуальної мережі використовується тільки тоді, коли кадр передається від

комутатора до комутатора, а при передачі кадру кінцевому вузлу воно зазвичай видаляється. При цьому модифікується тільки протокол взаємодії «комутатор - комутатор», а програмне і апаратне забезпечення кінцевих вузлів залишається незмінним.

До прийняття стандарту *IEEE* 802.1*Q* існувало багато вендорних протоколів цього типу, але всі вони мали один недолік - обладнання різних виробників створенні *VLAN* виявлялося несумісним. Стандарт *IEEE* 802.1*Q* вводить в кадрі *Ethernet* додатковий заголовок - тег віртуальної локальної мережі [7].

Існує 4 режима призначення *VLAN*:

- на основі інтерфейсу;
- на основі *MAC*-адреси;
- на основі протоколу;
- на основі політик.

При використанні *VLAN* на основі інтерфейсів мережевий адміністратор попередньо налаштовує *Port VLAN Identifier*(*PVID*) для кожного інтерфейсу комутатора. Коли нетегований кадр приходить на інтерфейс, комутатор додає *PVID* інтерфейсу до кадру. Перевага в тому, що учасників *VLAN* легко призначати, хоча з іншого боку, адміністратор повинен переналаштувати *VLAN* при зміні учасників. Рекомендується використовувати до мереж будь-якого масштабу і пристроїв в фіксованих місцях розташування.

В режимі призначення *VLAN* на основі *MAC*-адреси адміністратор попередньо налаштовує зіставлення між *MAC*-адресами і ідентифікаторами *VLAN*. При отриманні нетеговованого кадру комутатор додає тег *VLAN*, що відповідає *MAC*-адресі кадру, до кадру. При зміні фізичного розташування користувачів адміністратору не потрібно перенастроювати *VLAN*. Це підвищує безпеку і гнучкість доступу в мережі. Адміністратор повинен попередньо визначити *VLAN* для всіх учасників в мережі. Часто використовується в невеликих мережах, де призначені для користувача термінали часто змінюють фізичне місцеположення, але їх *Network Interface Card*(*NIC*) рідко змінюються, наприклад, на ноутбуках.

Наступний режим *VLAN*, що призначається на основі типів протоколів

(стеків) і форматів інкапсуляції кадрів. Адміністратор попередньо налаштовує зіставлення між типами протоколів і ідентифікаторами *VLAN*. При отриманні нетегованого кадру комутатор додає тег *VLAN*, відповідний типу протоколу кадру, до кадру. Потім кадр передається у зазначений *VLAN*. Цей режим прив'язує типи послуг до *VLAN*, полегшуючи управління і обслуговування. Адміністратор повинен попередньо конфігурувати зіставлення між усіма типами протоколів і ідентифікаторами *VLAN*. Комутатор повинен аналізувати формати адрес протоколу і перетворювати формати, які споживають надмірні ресурси. Тому цей режим уповільнює час відгуку комутатора. Застосовується до мереж, що використовують кілька протоколів.

Останній режим *VLAN*, що призначаються на основі таких політик, як комбінації інтерфейсів, *MAC*-адрес і *IP*-адрес. Адміністратор попередньо налаштовує політики. При отриманні нетегованого кадру, який відповідає налаштованій політиці, комутатор додає тег зазначеної *VLAN* до кадру. Потім кадр передається в зазначений *VLAN*. Цей режим забезпечує високу ступінь безпеки. *MAC*-адреси або *IP*-адреси користувачів, прив'язаних до *VLAN*, не можуть бути змінені. Адміністратор може гнучко вибирати, які політики використовувати відповідно до режиму управління і вимогами. Кожна політика повинна бути налаштована вручну [20].

2.4. Забезпечення відмовостійкості ядра мережі

2.4.1. Сімейство протоколів FHRP

Корпоративна мережа вимагає врахування того, як мережа справляється з несправністю. Для збільшення відмовостійкості маршрутизаторів, було розроблено сімейство протоколів *FHRP*. З точки зору працівника підприємства, поза їх локальною мережею, наступним важливим елементом, з яким вони мають справу, є шлюз за замовчуванням. Якщо шлюз зламається, тоді доступ до цілої підмережі зникне.

Для боротьби з даною проблемою саме і застосовується *FHRP*. Існує ряд цих технологій, з яких найбільш популярні:

- *Hot Standby Redundancy Protocol (HSRP);*

- *Virtual Router Redundancy Protocol (VRRP);*
- *Gateway Load Balancing Protocol (GLBP).*

Так як, *HSRP* та *GLBP* розроблені компанією *Cisco Systems* та доступні лише на пристроях даної компанії, розглянемо *VRRP* який є відкритим протоколом.

VRRP працює, групуючи резервні маршрутизатори разом у єдиний віртуальний маршрутизатор. Цей віртуальний маршрутизатор має власну *IP*-адресу. Замість відправлення трафіку до окремого маршрутизатора, трафік надсилається до адреси віртуального маршрутизатора (рис. 2.6). Головний маршрутизатор обробляє трафік, адресований віртуальному маршрутизатору адресу та переадресує її належним чином. Головний маршрутизатор також регулярно надсилає *hello*-пакет на резервний маршрутизатор. Якщо основний маршрутизатор зламався, тоді резервний маршрутизатор не отримує ці пакети відповідно. У такому випадку резервний маршрутизатор бере на себе роль головного маршрутизатора і починає обробку трафіку. Коли зламаний маршрутизатор відновився, він знову приймає на себе роль головного маршрутизатора. Поки хоча б один фізичний маршрутизатор доступний в віртуальному маршрутизаторі, досі існуватиме доступ до даної підмережі [12].

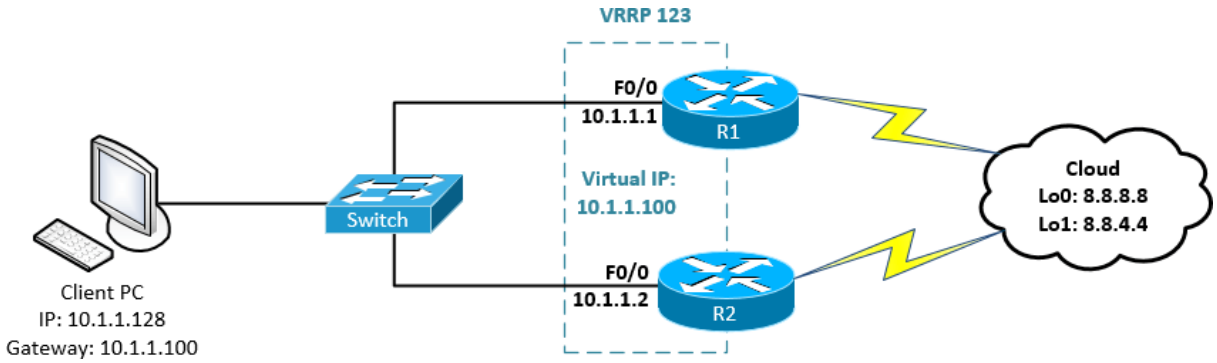

Рис. 2.6. Приклад мережі з використанням *VRRP*

Стекування комутаторів

При фізичному стекуванні комутатори представляють собою один логічний пристрій, що забезпечує зручність керування і моніторингу їх параметрів. Для

керування комутаторами можна використовувати інтерфейс командного рядка (*CLI*), *Web*-інтерфейс, *Telnet*, протокол *SNMP*. Комутатори можуть бути об’єднані в стек за кільцевою топологією або лінійною топологією (рис. 2.7). Перевагою топології "кільце" є те, що при виході одного пристрою з ладу або обриві зв’язку інші пристрої стека будуть продовжувати функціонувати в звичайному режимі.

Враховуючи те, що топологія “кільце” забезпечує роботу стеку при виході з ладу частини з комутаторів, доцільно буде використовувати дану топологію стекування при побудові даної корпоративної мережі.

Кожному комутатору стека присвоюється певна роль. Ці ролі можуть бути вручну налаштовані адміністратором мережі на кожному комутаторі або визначені стеком автоматично.

Існують три ролі, які можуть бути призначені комутаторам стека.

Основний майстер (*Primary Master*) – основний майстер-комутатор є головним пристроєм стека і єдиною точкою управління. Він стежить за нормальною роботою стека, топологією, призначає ідентифікатори пристроїв стека (Box *ID*), синхронізує конфігурації і передає команди іншим комутаторам. Роль основного майстра може бути присвоєна комутатору вручну, шляхом призначення найвищого пріоритету адміністратором мережі, або визначена автоматично в процесі виборів.

Резервний майстер (*Backup Master*) – резервний майстер дублює основний майстер-комутатор і в разі його виходу з ладу бере на себе функції основного майстра. Резервний майстер комутатор стежить за станом сусідніх комутаторів стека, основного майстра комутатора і виконує його команди. Роль резервного майстра може бути призначена комугатору вручну, шляхом присвоєння йому другого за значенням пріоритету до фізичного об’єднання пристроїв в стек або автоматично під час виборів.

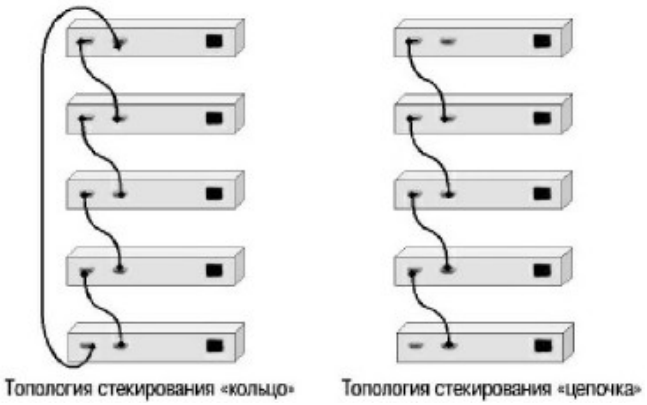

Рис. 2.7. Топології стекування комутаторів

Ведений (*Slave*) – веденими є всі інші комутатори стека. Ведені комутатори виконують команди, що дає основний майстер, стежать за станом сусідніх комутаторів стека і топологією, слідують командам резервного майстра, коли він стає основним. Ведені комутатори беруть участь в процесі вибору нового резервного майстра, в разі якщо:

- резервний майстер став основним майстром;
- резервний майстер вийшов і з ладу або видалений зі стеку;
- обидва, і основний, і резервний майстер, вийшли з ладу або видалені зі стеку.

2.5. Аналіз вимог до корпоративної мережі

Головний офіс включає в себе наступні складові: адміністрація, бухгалтерія, IT-відділ, відділ маркетингу та серверну. Загальна кількість необхідного обладнання подано у таблиці 2.1. Для зменшення навантаження на мережу, окремим модулем (підмережею) запропоновано винести серверну.

Таблиця 2.1

Мережеве обладнання головного офісу

Найменування	Кількість
Персональний комп’ютер	17
Сервер	3
Комутатор	6
Маршрутизатор	3
IP-телефон	6

Виробництво складається з підрозділів: адміністрація, цех №1, цех №2, цех №3.

Необхідне обладнання подано в табл.2.2.

Таблиця 2.2

Мережеве обладнання виробництва

Найменування	Кількість
Персональний комп’ютер	4
Комутатор	3
Маршрутизатор	1
IP-телефон	4

В таблиці 2.3 подано обладнання для створення мережі на складі.

Таблиця 2.3

Мережеве обладнання складу

Найменування	Кількість
Персональний комп’ютер	1
Сервер	1
Комутатор	1
Маршрутизатор	1
IP-телефон	1
IP-камера	4

Філіальний офіс включає в себе наступні підрозділи: адміністрацію, бухгалтерію та ІТ-відділ. Обладнання подано в таблиці 2.4.

Таблиця 2.4

Мережеве обладнання філіалу

Найменування	Кількість
Персональний комп’ютер	7
Комутатор	3
Маршрутизатор	1
IP-телефон	4

2.6. Побудова корпоративної мережі

Згідно з трьохрівневою моделлю мережі пропонується реалізація серверної головного офісу окремою підмережею (рис. 2.8). Маршрутизатори продубльовано з використанням технології *VRRP* та комутатори ввімкнені в стек для збільшення відмовостійкості ядра корпоративної мережі.

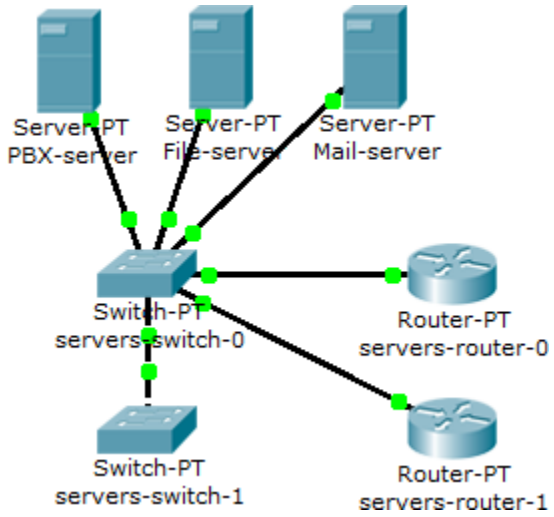

Рис. 2.8. Структура ядра корпоративної мережі

Головний офіс, який знаходиться в одній будівлі з серверною, має структуру, зображену на рис.2.9.

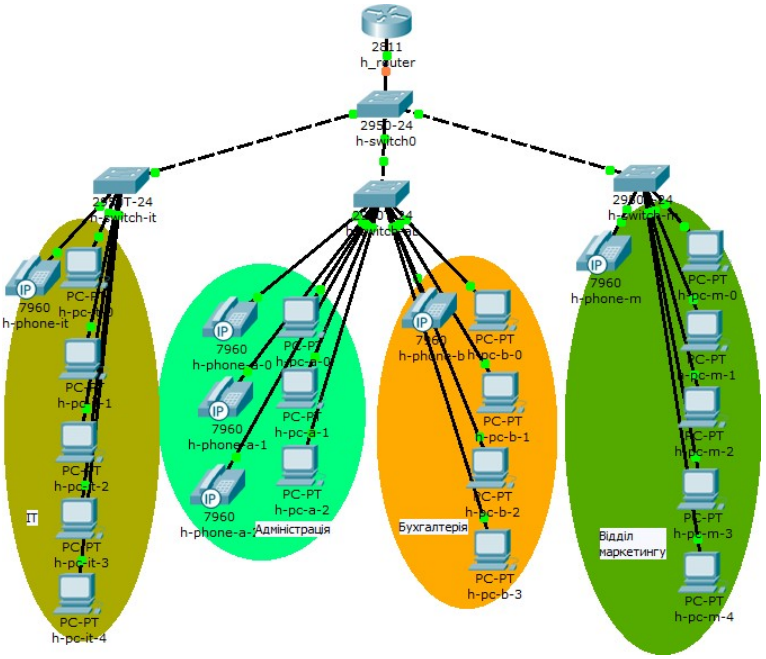

Рис. 2.9. Структура мережі головного офісу

Філіальний офіс має аналогічну структуру мережі до головного офісу (рис. 2.10).

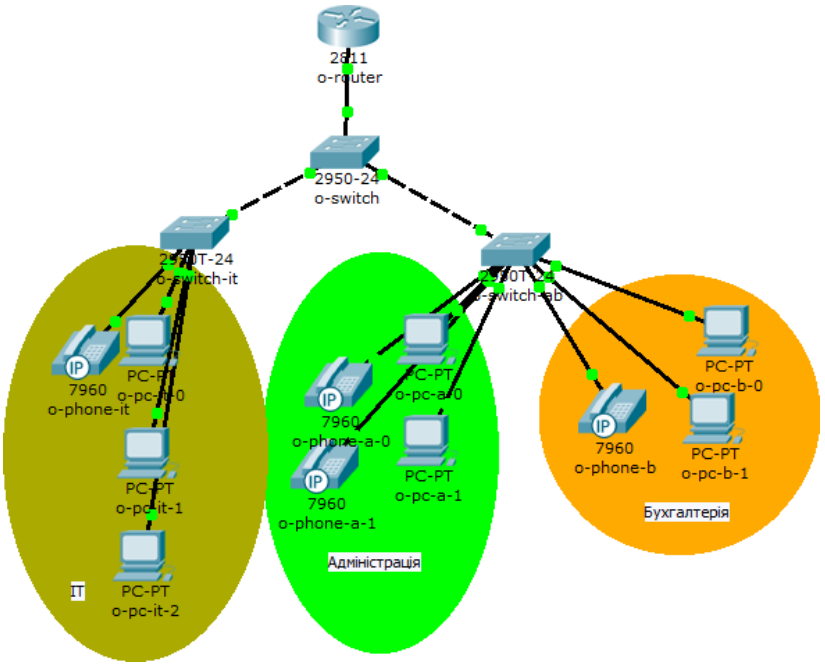

Рис. 2.10. Структура мережі філіального офісу

Незважаючи на те, що склад (рис. 2.11) та виробництво (рис. 2.12) знаходяться територіально близько(в межах 100м між будівлями), що дозволяє об’єднати дві ці підмережі, доцільніше залишити їх окремими для збільшення надійності, та спрощення переміщення чи розширення даних підрозділів.

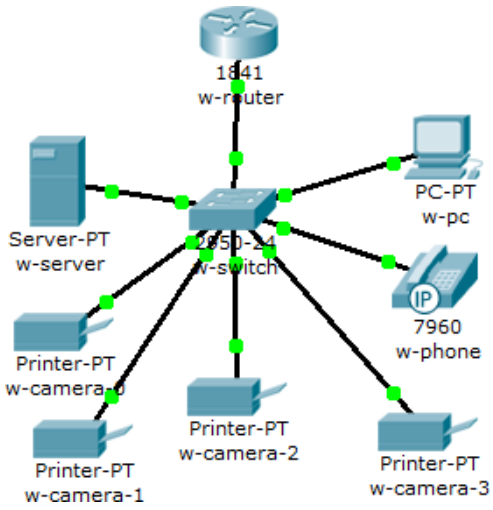

Рис. 2.11. Структура мережі складу

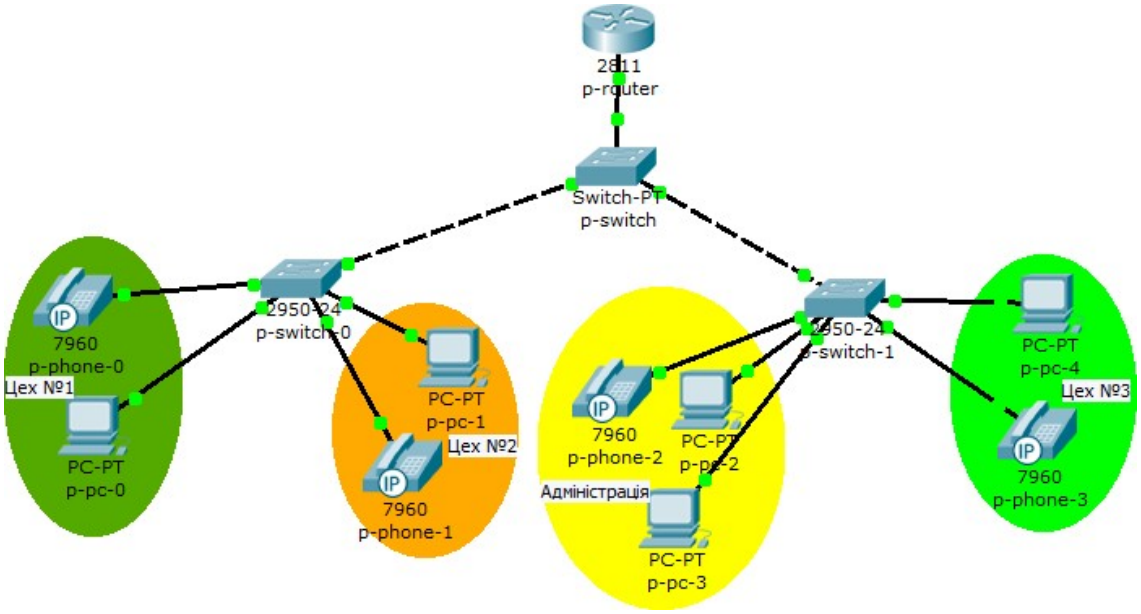

Рис. 2.12. Структура мережі виробництва

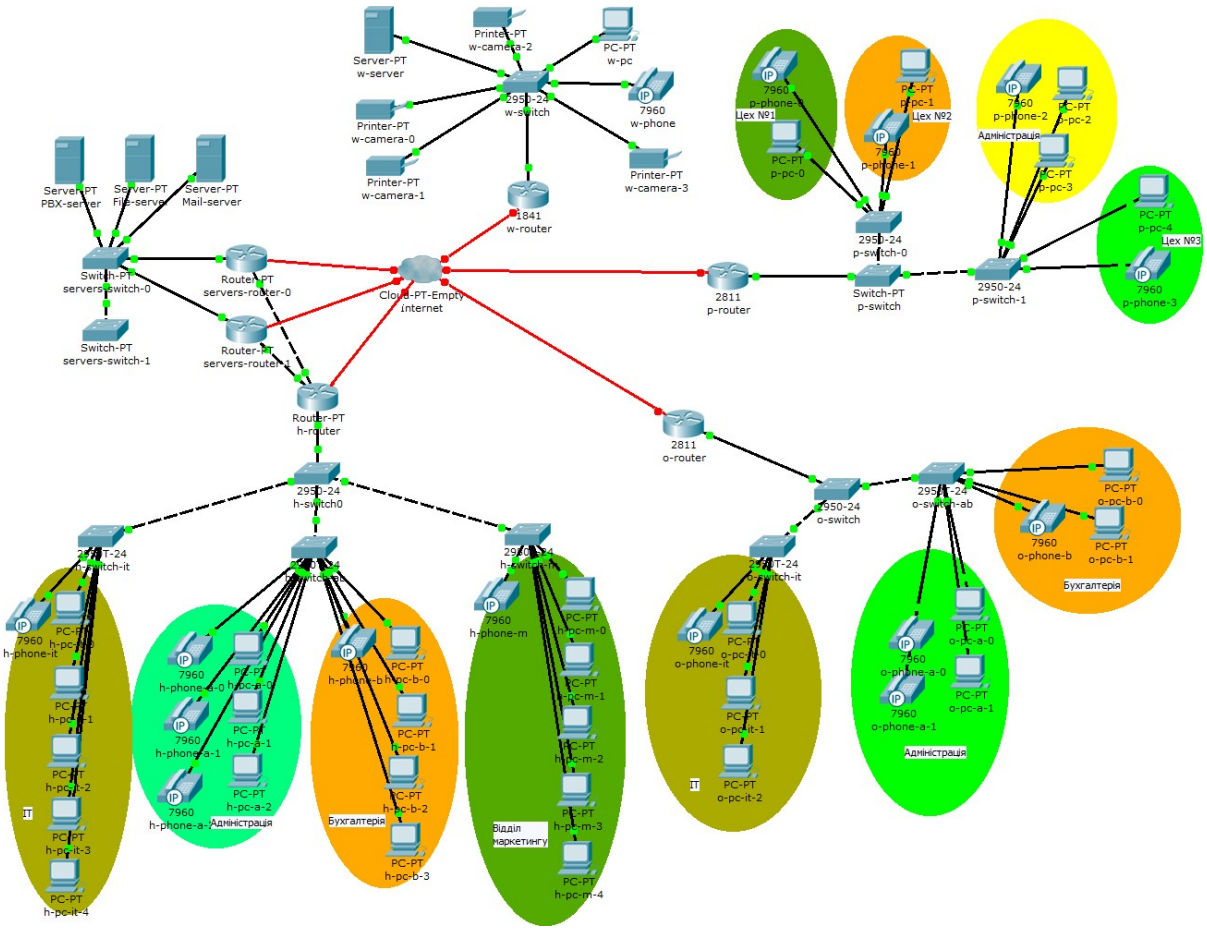

Рис. 2.13. Структура корпоративної мережі

Об’єднавши всі підмережі, отримаємо загальну структуру корпоративної мережі (рис. 2.13).

2.7. Розподіл адресного простору та VLAN

Проаналізувавши структуру корпоративної мережі підприємства, запропоновано наступний розподіл адресного простору підприємства з розбиттям на 14 підмереж, що показано у табл. 2.5.

Таблиця 2.5

Адресація мережі компанії

Підрозділ	**Ім'я *VLAN***	**Розмір**	**Адреса**	**Маска**	**Діапазон доступних адрес**	**Номер *VLAN***
Серверна головного офісу	*servers*	16	10.0.0.0	/28	10.0.0.1 - 10.0.0.14	100
Адміністрація головного офісу	*h-admin*	16	10.0.0.16	/28	10.0.0.17 - 10.0.0.30	101
IT-відділ головного офісу	*h-it*	16	10.0.0.32	/28	10.0.0.33 - 10.0.0.46	102
Бухгалтерія головного офісу	*h-finance*	16	10.0.0.48	/28	10.0.0.49 - 10.0.0.62	103
Відділ маркетингу головного офісу	*h-marketing*	16	10.0.0.64	/28	10.0.0.65 - 10.0.0.78	104
Склад	*warehouse*	32	10.0.1.0	/27	10.0.0.1 - 10.0.0.30	200
Цех №1	*Prod-1*	16	10.0.2.0	/28	10.0.2.1 - 10.0.2.14	302
Цех №2	*Prod-2*	16	10.0.2.16	/28	10.0.2.17 - 10.0.2.30	303
Цех №3	*Prod-3*	16	10.0.2.32	/28	10.0.2.33 - 10.0.2.46	304
Адміністрація виробництва	*p-admin*	16	10.0.2.48	/28	10.0.2.49 - 10.0.2.62	301
IT-відділ філіалу	*o-it*	16	10.0.3.0	/28	10.0.3.1 - 10.0.3.14	402
Адміністрація філіалу	*o-admin*	16	10.0.3.16	/28	10.0.3.17 - 10.0.3.30	401
Відділ маркетингу філіалу	*o-marketing*	16	10.0.3.32	/28	10.0.3.33 - 10.0.3.46	404
Бухгалтерія філіалу	*o-finance*	16	10.0.3.48	/28	10.0.3.49 - 10.0.3.62	403

Висновки за розділом 2

Підрозділи підприємства є географічно віддаленими та мають вихід у мережу *Internet*, тому доцільним буде її використання для з'єднання сегментів корпоративної мережі.

В ході аналізу структури підприємства, запропоновано використати топологію ієрархічної зірки(дерева). Сама по собі, зіркоподібна топологія утворюється в разі, коли кожен комп'ютер підключається безпосередньо до загального центрального пристрою, що зветься концентратором. Ієрархічна зірка, будується ж з використанням декількох концентраторів, що ієрархічно з'єднанні між собою зіркоподібними зв'язками.

Перевагами обраної топології є:

- масштабованість;
- легкий пошук проблемних вузлів;
- висока продуктивність мережі.

Недоліки:

- вихід з ладу концентратора впливає на роботу всієї мережі;
- високі витрати кабелів.

Збільшені витрати на додаткові кабелі легко нівелюються її перевагами. А вразливість концентраторів вирішується за допомогою технологій стекування.

Для підвищення відмовостійкості ядра корпоративної мережі використовувались технології стекування комутаторів та протокол *VRRP*. Даний протокол працює, групуючи резервні маршрутизатори разом у єдиний віртуальний маршрутизатор. Цей віртуальний маршрутизатор має власну *IP*-адресу. Замість відправлення трафіку до окремого маршрутизатора, трафік надсилається до адреси віртуального маршрутизатора.

Для зв'язку підрозділів підприємства використовується *VPN*. Технологія *VPN* надає компанії можливості дорогої приватної орендованої лінії за набагато нижчою вартістю, використовуючи спільну мережу, таку як Інтернет. Перевага використання Інтернету для зв'язку в тому, що тунелі можуть бути створеним за вимогою та включати, наприклад, працівника, який знаходиться вдома або

подорожує, та має з’єднання з Інтернетом. За рахунок цього гнучкість даного рішення є вищою, чим у виділених ліній.

Мережу поділено на 14 віртуальних локальних мереж для зменшення трафіку в мережі(наприклад, широкомовного), можливості застосування політик безпеки для окремих *VLAN*.

РОЗДІЛ 3
ВИБІР МЕРЕЖЕВОГО ОБЛАДНАННЯ

3.1. Вимоги до мережевого обладнання

Відповідно до обраної структури мережі необхідно використовувати наступне обладнання:

- два маршрутизатора ядра з наявністю портів *GigabitEthernet/ 10GigabitEthernet (GE/10GE);*
- чотири маршрутизатора рівня агрегації з наявністю портів *GE;*
- два комутатора рівня ядра з наявністю портів *10GE;*
- десять комутаторів рівня агрегації та доступу з наявністю портів *GE;*
- один комутатор рівня доступу з наявністю портів *GE* та технологією живлення пристроїв по витій парі (*PoE*) для підключення камер;
- чотири сервери;
- чотири *IP*-камери;
- п’ятнадцять *IP*-телефонів.

3.2. Порівняльний аналіз та вибір мережевого обладнання

Згідно з рейтингом та долею в світовому ринку, до найбільших постачальників мережевого обладнання належать *Cisco Systems* та *Huawei* [18]. Порівняння даних виробників у табл. 3.1.

Таблиця 3.1

Порівняння обладнання *Huawei* та *Cisco*

Параметр	*Huawei*	*Cisco*
Відповідність стандартам	Всі продукти повністю відповідають міжнародним	Рішення *Cisco* найчастіше використовують технології *Cisco*
Відповідність стандартам	стандартам, що забезпечує найкращу сумісність в галузі	з метою прив’язки замовника до вендора
Операційна система	Всі продукти працюють на уніфікованій операційній системі (*VRP*), що має 17 років розвитку	Операційні системи продуктів *Cisco* стали різнорідними (*IOS* / *IOS-XR* / *IOS-XE* /*NX-OS*)

Продовження таблиці 3.1

Параметр	*Huawei*	*Cisco*
Повнота мережевого рішення	Повне рішення для мережі підприємства з широким набором продуктів, включаючи *IP*, оптичний і РРЛ транспорт, 3*G*, і *PON*	Відсутні рішення *PON* для *FTTx*, *SDH*, РРЛ.
Економія електроенергії та екологічність	Технологія *SmartEnergy*	Технологія *EnergyWise*
Уніфікована система управління мережею (*NMS*)	Єдина *NMS* керує всією мережею підприємства. Не потрібно перемикатися між різними системами *NMS* для конфігурації різного устаткування	У технічній експлуатації використовується більше 30 різних продуктів *NMS* (результат безлічі злиттів і поглинань)
Сервіси	Телекомунікація, сервіси з використанням штучного інтелекту (комп'ютерного зору) та інші	Телекомунікація
Вартість	Помірна	Висока

Також, *eSight* (*NMS* від *Huawei*), завдяки відповідності стандартам, може керувати більш ніж 140 пристроями *Cisco*, більш 130 пристроїв *H3C*, більше чим 100 пристроїв інших вендорів, а також більш ніж десятьма типами принтерів та серверів. Мережеві адміністратори можуть використовувати *eSight* для управління всіма пристроями мережі. Дана система управляння значно покращує ефективність мережевого управління та може автоматично виявляти нові типи пристроїв існуючих постачальників, ідентифікувати виробника пристроїв, повідомляти адміністратора системними попередженнями та повідомленнями про поломки чи можливі проблеми в мережі. Крім того, *eSight* може контролювати такі параметри пристроїв, як дані з лицевих панелей та індикаторів, завантаження процесора**,** кількість трафіку та інше.

Провівши дане порівняння, у випадку мультисервісної корпоративної

мережі підприємства, вибір падає на продукцію *Huawei*.

3.2.1. Комутатор Huawei S2700-26TP-PWR-EI

Комутатори *Huawei* серії *S*2700 для корпоративних мереж є інтелектуальними енергозберігаючими комутаторами доступу наступного покоління (рис. 3.1, 3.2).

Рис. 3.1. Комутатор *Huawei S*2700-26*TP-PWR-EI*

Серія *S*2700 використовує передові технології комутації та програмне забезпечення універсальної платформи маршрутизації (*VRP*) компанії *Huawei*. Устаткування легко встановлюється і обслуговується. Завдяки гнучким можливостям роботи в мережі, продуманій політиці забезпечення безпеки, якості обслуговування та енергозберігаючим технологіям, *S*2700 дозволяє будувати мережі наступного покоління [14]. Характеристики комутатора наведено у табл. 3.2.

Таблиця 3.2

Характеристики комутатора *Huawei S2700-26TP-PWR-EI*

Характеристика	Значення
Комутаційна ємність	32 Гбіт/с
Порти	24 порта 10/100 Base-TX Ethernet з підтримкою PoE 2 порта Gigabit Ethernet (GE)
Таблиця *MAC*-адрес	8000 *MAC*-адрес Ручне видалення динамічних MAC-адрес Налаштування часу старіння MAC-адреси Контроль розпізнавання MAC-адрес на базі портів *MAC*-адреси типу "чорної діри"
VLAN	4000 *VLANs*, що відповідають *IEEE* 802.1*Q* Призначення мереж *VLAN* на основі портів Призначення на базі MAC-адреси

Продовження таблиці 3.2

QoS	Обмеження швидкості на базі порту 4 або 8 черг різних пріоритетів на кожному порту Відповідність між пріоритетами 802.1*p* і чергами Алгоритми *SP*, *WRR* і *SP* + *WRR*
Безпека і доступ	Аутентифікація 802.1*x* і обмеження на число користувачів в інтерфейсі Придушення шторму Захист джерела *IP* Підтримка різних методів аутентифікації, включаючи *AAA*, *RADIUS* і *TACACS* +
Безпека і доступ	Відстеження *DHCP*-пакетів Ізоляція порту і закріплений MAC Підтримка фільтрації пакетів по MAC-адресами Обмеження кількості відомих *MAC*-адрес

3.2.2. Комутатор Huawei S2700-26TP-SI-AC

*Huawei S*2700-26*TP-SI-AC* відноситься до лінійки *S*2700 і є ідентичним до попереднього (див. рис. 3.2).

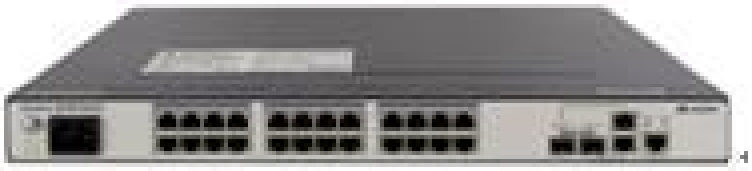

Рис. 3.2. Комутатор *Huawei S*2700-26*TP-SI-AC*

Окрім наявності підтримки *PoE* на вихідних 10/100 *Base-TX Ethernet* портах.

3.2.3. Комутатор Huawei S5700-26X-SI-12S-AC

Гігабітні корпоративні комутатори *Huawei Quidway* серії *S*5700 – це енергозберігаючі комутатори наступного покоління, розроблені компанією *Huawei* для задоволення потреб високошвидкісного доступу (рис. 3.3). Базується на сучасній апаратурі і програмному забезпеченні універсальної платформи

маршрутизації (*VRP*). *Huawei S*5700 надає високу комутуючу здатність і порти *GE* високої щільності для реалізації передачі даних в вузол зі швидкістю 10 Гбіт /с. Комутатор *S*5700 може використовуватися в різних сценаріях корпоративної мережі.

Рис. 3.3. Комутатор *Huawei S*5700-26*X*-*SI*-12*S*-*AC*

Наприклад, він може функціонувати як комутатор ядра в мережі кампусного типу, як гігабітний комутатор доступу в Інтернет-центрі обробки і зберігання даних або як настільний комутатор для надання доступу 1000 Мбіт/с до терміналів [15]. Характеристики комутатора наведено у табл. 3.3.

Таблиця 3.3

Характеристики комутатора *Huawei S5700-26X-SI-12S-AC*

Характеристика	Значення
Комутаційна ємність	256 Гбіт/с
Порти	12 портів 10/100/1000 Base-TX Ethernet, 12 портів 100/1000 Base-X 2 порта 10 Gigabit Ethernet (10GE)
Слоти розширення	Слот розширення для стекування
Таблиця *MAC*-адрес	Підтримка стандарту *IEEE* 802.1*d* Розпізнавання і старіння *MAC*-адрес Статичні, динамічні *MAC*-адреси і *MAC*-адреси типу «чорна діра» Фільтрація пакетів на базі *MAC*-адрес джерела 16 000 *MAC*-адрес
VLAN	4 000 мереж *VLAN* Гостьова *VLAN* і голосова *VLAN Super VLAN, MUX VLAN, GVRP* Побудова мереж *VLAN* на базі *MAC*-адрес, протоколів, *IP*-підмереж, політик і портів

Продовження таблиці 3.3

Характеристика	Значення
QoS	Обмеження швидкості на базі порту 4 або 8 черг різних пріоритетів на кожному порту Відповідність між пріоритетами 802.1*p* і чергами Алгоритми *SP*, *WRR* і *SP* + *WRR*
Безпека і доступ	*STP*, *RSTP* і *MSTP* Деревоподібна топологія *Smart Link* і *Smart Link multi-instance*, підтримка перемикання на резерв протягом мілісекунд Кільцева топологія *RRPP* і *RRPP multi-instance* Підтримка *G*.8032 *ERPS* технологія *SEP* Підтримка захисту *BPDU* (*BRDU protection*), кореня (*root protection*) і шлейфу (*loop protection*) *BPDU*-тунель
Адміністрування	Інтелектуальна технологія об’єднання в стеки (*iStack*) Віртуальна перевірка кабелю Дистанційний моніторинг мережі (*RMON*) *eSight* і *NMS* на базі веб-інтерфейсу *SNMP v*1 / *v*2*c* / *v*3 Системні логи і багаторівнева сигналізація

3.2.4. Маршрутизатор Huawei AR-1200E

Інтегровані функції комутації та маршрутизації забезпечують передачу голосу та даних, а також бездротовий зв’язок в офісах невеликих підприємств або віддалених офісах за допомогою 3*G*, *WLAN* або *LTE*. Неблокуюча архітектура *AR*1200 і багатоядерний процесор гарантують стабільну смугу пропускання для передачі даних (рис. 3.4).

Рис. 3.4. Маршрутизатор *Huawei AR*-1200*E*

Можливе використання кабельних і волоконно-оптичних інтерфейсів. Повний набір функцій забезпечення безпеки, виявлення несправностей і можливість динамічної заміни в «гарячому» режимі забезпечують безпечний та надійний зв'язок. Також, містить вбудований фаервол та АТС, що забезпечує основні голосові функції [16]. Характеристики маршрутизатора наведено у табл. 3.4.

Таблиця 3.4

Характеристики маршрутизатора *Huawei AR-1200E*

Характеристика	Значення
WAN порти	2 *GE*
LAN порти	8 портів *GE* (можливість настройки як *WAN*-інтерфейсів)
Слоти	Слоти *SIC*: 2 Слоти *WSIC* (за замовчуванням / максимум): 0/1
Телефонія	Основні голосові функції забезпечуються вбудованою АТС, *SIP*-сервером та *SIP*-шлюзом доступу Голосові послуги включають багатосторонній зв'язок, автоматичне підключення, *IVR*, мелодію дзвінка, паралельний дзвінок, послідовний дзвінок, управління абонентами Інтелектуальна маршрутизація дзвінків означає виняткову надійність голосових послуг Взаємозв'язок з терміналами *NGN* / *IMS* / *PBX* / основних постачальників
Пам'ять	1Гб
Техобслуговування	Підтримка заміни в «гарячому» режимі будь-яких телекомунікаційних плат Підтримка розгортання *U*-диска
VPN	*IPSec VPN, GRE VPN, DSVPN* та *L2TP VPN*

3.2.5. Маршрутизатор Huawei AR-3200-SRU200

Високопродуктивні масштабовані маршрутизатори доступу з інтегрованими функціями комутації і маршрутизації, а також універсальними функціями управління і безпеки для великомасштабних корпоративних мереж дозволяють знизити сукупну вартість мережі (рис. 3.5).

Рис. 3.5. Маршрутизатор *Huawei AR*-3200-*SRU*200

Неблокуюча архітектура з двома платами управління забезпечує надійний даних. Виявлення неполадок і динамічне резервування каналів забезпечують підвищену відмовостійкість, а плати з можливістю заміни в «гарячому» режимі дозволяють проводити модернізацію без відключення користувачів.

Підтримка відкритої сервісної платформи (*Open Service Platform*, *OSP*) забезпечує сумісність з продуктами сторонніх виробників, захист вкладених інвестицій і подальше підвищення коефіцієнта окупності інвестицій (*ROI*) [17]. Характеристики маршрутизатора наведено у табл. 3.5.

Таблиця 3.5

Характеристики маршрутизатора *Huawei Ar-3200-SRU200*

Характеристика	Значення
WAN порти	4 порта *GE*, 2 порта 10 *GE*
Слоти	Слоти *SIC*: 4 Слоти *WSIC* (за замовчуванням / максимум): 2/4 Слоти *XSIC* (за замовчуванням / максимальна кількість): 4/6
QoS	Апаратне прискорення, ієрархічна система *QoS*
Пам’ять	4Гб
VPN	*IPSec VPN*, *GRE VPN*, *DSVPN*, *L2TP VPN*
Техобслуговування	Підтримка заміни в «гарячому» режимі всіх інтерфейсних плат

3.2.6. IP-телефон Fanvil X4

*Fanvil X*4 – багатофункціональний *SIP*-телефон для бізнесу (рис. 3.6).

Рис. 3.6. *IP*-телефон *Fanvil X*4

Телефон підтримує широкий набір функцій, а саме: утримання виклику, відключення мікрофона, режим очікування, переведення виклику, повтор виклику, автовідповідь, режим "Не турбувати", голосова пошта, відеоконференція, гаряча лінія. Пристрій оснащений вбудованою телефонною книгою на 500 записів, а також дозволяє користуватися віддаленими телефонними книгами по *XML* або *LDAP*. Журнал викликів, який дозволяє дізнатися інформацію про всі зроблені, прийняті та пропущені виклики, що не дозволить пропустити важливу інформацію. Телефон має зручний для користувача інтерфейс, чотири програмовані клавіші, п’ять функціональних клавіш, чотири клавіші навігації і одну клавішу підтвердження [19]. Характеристики телефону наведено у табл. 3.6.

Таблиця 3.6

Характеристики *IP*-телефону *Fanvil X4*

Характеристика	Значення
Порти	10/100 *Base-T Ethernet*
Кількість ліній	4
Підтримка кодеків	*G*.726-32, *G*.711*a*, *G*.729*a*, *G*.729*b*, *G*.711*u*, *G*723.1
Підтримка АТС	3*CX*, *Asterisk*, *Broadsoft*, *Elastix*, *Zycoo*
Телефонна книга	500 контактів

3.2.7. Сервер ARTLINE Business R25v10

Однією з особливостей сервера *ARTLINE Business R*25*v*10 (рис. 3.7) є рішення для організації віддаленої роботи по стандарту *IPMI* 2.0. Така можливість реалізована завдяки спеціальному інтегрованому модулю адміністрування *ASMB*9-*iKVM*. Віддалене підключення по локальній мережі через *Ethernet*-інтерфейс (технологія *KVM-over-IP*) дозволяє уникнути прямої присутності адміністратора в безпосередній близькості до сервера - це допомагає значно знизити операційні витрати. Програмна оболонка *ASWM Enterprise* забезпечує необхідний контроль і відстеження цілого ряду параметрів (показників напруги силових ланцюгів, температурних датчиків, роботи системи охолодження, підключеної периферії і т.д.).

Рис. 3.7. Сервер *ARTLINE Bussiness R*25*v*10

Зручний веб-інтерфейс працює незалежно від операційної системи сервера, що дозволяє організувати периферійний контроль роботи останнього: включення/виключення, моніторинг апаратних елементів, установку ОС, налаштування, оновлення, відеозапис, реєстрацію критичних помилок з веденням журналу логування. Характеристики сервера наведено у табл. 3.7.

Таблиця 3.7

Характеристики сервера *ARTLINE Bussiness R25v10*

Характеристика	Значення
Оперативна пам’ять	16*Gb DDR*4-2666
Процесор	*Intel* 4-*core Xeon E*-2224*G* 3.5-4.7*GHz*;
Накопичувач	250Гб *SSD* 2*x*1Тб *HDD*
Рівні *RAID*	0/1/5/10

Продовження таблиці 3.7

Форм-фактор	2*U*
Відеокарта	Інтегрована

3.2.8. IP-камера Huawei C2120-10-LU

Програмне забезпечення в традиційних камерах залежить від апаратної платформи, що сильно обмежує спектр їх застосування. Інноваційна програмно-налаштована камера (*Software-Defined Camera*, *SDC*) *Huawei* (рис. 3.8) створена на основі передових чипів штучного інтелекту, відкритої операційної системи (ОС) та орієнтованої на майбутнє екосистему.

Рис. 3.8. *IP*-камера *Huawei C*2120-10-*LU*

Алгоритми, що використовуються в даній камері, не залежать від апаратної платформи. Крім того, камера підтримує безперервне онлайн-оновлення алгоритмів та самонавчання. Таким чином, розробка алгоритмів ведеться на протязі всього життєвого цикла обладнання, придбаного лише одного разу [22].

Алгоритми, що підтримуються:

- теплова карта;
- аналіз поведінки людини;
- аналіз натовпу;
- розпізнавання людського обличчя;
- розпізнавання тіла людини;
- розпізнавання транспортного засобу;
- аналіз даних про дорожній рух.

Висновки за розділом 3

Вибір мережевого обладнання – це відповідальний етап побудови корпоративної мережі, від якого залежить простота налаштування, ефективність моніторингу та масштабованість мережі. В ході проведеного аналізу рекомендується використання обладнання *Huawei* тому, що воно має наступні переваги:

- відповідність обладнання міжнародним стандартам, що забезпечує хорошу сумісність з продукцією інших виробників;
- всі продукти працюють на уніфікованій операційній системі (*VRP*), що має 17 років розвитку;
- повне рішення для мережі підприємства з широким набором продуктів, включаючи *IP*, оптичний і РРЛ транспорт, 3*G*, і *PON*;
- економічність, завдяки технології *SmartEnergy;*
- єдина уніфікована система управління мережею керує всією мережею підприємства. не потрібно перемикатися між різними системами для конфігурації різного устаткування;
- надає сервіси телекомунікації, сервіси з використанням штучного інтелекту (комп’ютерного зору) та інші;
- має низьку вартість, в порівнянні з обладнанням від *Cisco Systems.*

В якості інтелектуальної *IP*-камери використовується програмно-налаштована камера *Huawei SDC*, що немає прив’язки до алгоритму розпізнавання, як традиційні інтелектуальні камери. Крім того, камера підтримує безперервне онлайн-оновлення алгоритмів та самонавчання. Таким чином, розробка алгоритмів ведеться на протязі всього життєвого цикла обладнання, придбаного лише одного разу.

РОЗДІЛ 4
ВИБІР СЕРВІСІВ

4.1. Сервіс інтелектуального відеоспостереження

Штучний інтелект(ШІ) та аналіз даних не оминув таку індустрію, як відеоспостереження. Сьогодні камери вже не просто знімають, вони виконують багатовимірний, інтелектуальний аналіз даних, розпізнаючи відеозображення та прогнозуючи тенденції зміни ситуації.

Перевагою використання ШІ є те, що така система є точнішою і надійнішою за традиційну систему з оператором. В першу чергу, це пов’язано з втомою оператора, тому , що з протягом роботи оператор втрачає пильність, і може не помітити можливу загрозу. Система з використанням ШІ в свою чергу, буде однаково «пильною» незалежно від тривалості роботи. Це гарантує, що жодна деталь чи загроза не залишаться непоміченими, а отже, безпека організації буде гарантована.

Алгоритми машинного навчання значно спрогресували, що дає значний ріст точності розпізнавання. Нейронні мережі дозволяють комп’ютеру застосовувати ряд оцінок до тієї чи іншої ситуації, навчаючись виявляти все більш складні функції (краї, кольори, форми та тони об’єктів), на відміну від рішень, заснованих на правилах, які обмежуються початковим програмуванням [21, 22]. Також, оскільки обчислювальна потужність продовжує зростати, що дозволить нейронним мережам обробляти більшу кількість інформації і, відповідно, піднімати точність.

До інтелектуальної системи відеоспостереження можуть ставитись різні задачі розпізнавання:

- виявлення проникнення на територію, руху (рис. 4.1);
- виявлення підозрілих об’єктів в аеропортах та громадських приміщеннях;
- розпізнавання лиць;
- розпізнавання людини в натовпі за обличчям або певними рисами поведінки;
- безлике розпізнавання за фізичними характеристиками людини (зріст,

постава і т.д).

Обробка зображень штучним інтелектом дозволяє покращити аналіз ситуації. Хоч і існує можливість зйомки зображень високої роздільної здатності за допомогою камер високої чіткості, доля їх використання як частини рішень для відеоспостереження залишається низькою. Як результат, більшість зображень, зроблених такими рішеннями, низької якості, особливо в умовах недостатнього освітлення. Це виступає перешкодою під час проведення змістовного аналізу таких кадрів зображення. Штучний інтелект можна використовувати для покращення якості таких зображень, щоб співробітники служби безпеки могли отримувати з них необхідну інформацію.

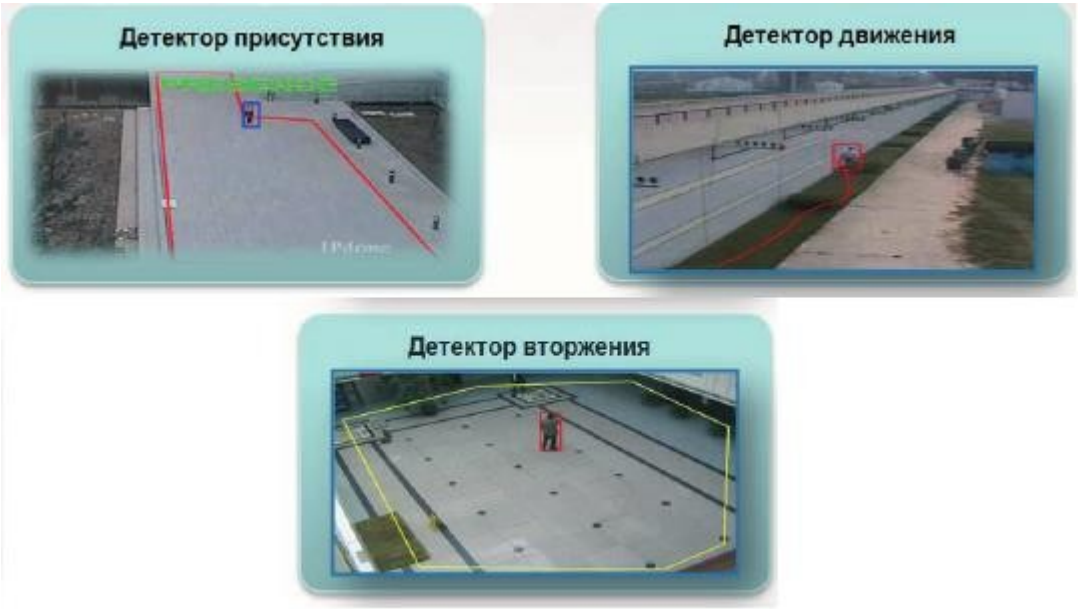

Рис. 4.1. Приклад результату роботи алгоритмів присутності, руху та вторгнення

Використання ШІ в системах відеоспостереження значно підвищує ефективність даних систем, роблячи операторів безпеки більш результативними на своїх робочих місцях. Усунувши необхідність постійно переглядати монітори та автоматизуючи функцію «виявлення» штучний інтелект дозволяє операторам зосередитись на тому, що вони роблять найкраще: на перевірці та дії в критичній ситуації. Це не тільки прискорює розслідування, але й забезпечує реакцію в реальному часі на небезпеку.

Традиційні камери мають такі проблеми, як фіксовані методи

розпізнавання, низька обчислювальна потужність та труднощі з оновленням, оскільки вони поєднані між собою програмним та апаратним забезпеченням та обмеженою продуктивністю центрального процесора.

Програмно-конфігурована камера (*Software-Defined Camera, SDC*) *Huawei* створена на основі чипів штучного інтелекту та відкритої операційної системи. Традиційні інтелектуальні пристрої спостереження зазвичай мають окремий чіп центрального процесора (*CPU*) – для виконання алгоритмів інтелектуального аналізу на самій камері. Хоча така конструкція відповідає сучасним вимогам, простір для оновлення камери обмежений. У міру того, як виклики безпеці стають дедалі складнішими, необхідний глибший та ширший аналіз людей, транспортних засобів та об’єктів. Підвищення точності алгоритмів та підтримка одночасної роботи декількох алгоритмів стали пріоритетом. У цьому контексті *Huawei* випустила процесор штучного інтелекту, *Ascend* 310, наприкінці 2018 року. Він має високу обчислювальну потужність (16 *TOPS*) і низьке споживання енергії (лише 8 Вт). Завдяки обчислювальній потужності, одна *Huawei SDC* може обробляти відеопотік з трьох- чотирьох звичайних камер поблизу.

Крім того, камера підтримує безперервне, практично миттєве онлайн-оновлення алгоритмів і самонавчання. Таким чином, розробка алгоритмів ведеться протягом усього життєвого циклу обладнання, придбаного тільки один раз.

Камера *Huawei SDC* має відкриту програмну архітектуру, яка дозволяє інтегрувати нові алгоритми від партнерів по екосистемі, забезпечуючи ефективну роботу штучного інтелекту. Крім того, відкрита апаратна архітектура передбачає можливість підключення різних датчиків сторонніх виробників, допомагаючи створювати додаткову соціальну і комерційну цінність для клієнтів в різних секторах економіки.

Для інтелектуальних продуктів відеоспостереження обчислювальні можливості на основі штучного інтелекту мають ключове значення, так як вони забезпечують адаптацію до різних вимог безпеки і обробку величезних обсягів інформації і даних.

Таким чином, камери *Huawei SDC* безпосередньо долають обмеження, пов’язані із забезпеченням безпеки**,** з якими стикаються традиційні камери.

З відкритою операційною системою *SDC OS* для розробників доступні інструменти для підключення, навчання та розгортання алгоритмів та додатків відповідно до стандартів.

Huawei SDC застосовує алгоритм синтезу зображень за допомогою штучного інтелекту та інфрачервоне світло. Ці функції забезпечують повнокольорові зображення вдень і вночі без втрати інтенсивності світла або світлового забруднення. Завдяки цим особливостям *Huawei SDC* фіксує дрібні деталі з більшою ефективністю, особливо вночі. Також, камера *Huawei SDC,* вивчаючи особливості різних сцен, може ідентифікувати зміни світла та погоди в режимі реального часу та динамічно регулювати налаштування зображення для отримання чітких зображень.

Завдяки високій обчислювальній здатності процесорів штучного інтелекту, таких як *Ascend*, *Huawei SDC* може захоплювати до 100 облич на кадр у густонаселених сценах на основі алгоритму трасування та збігу, як на рис. 4.2.

Рис. 4.2 Приклад роботи алгоритму трасування та збігу *Huawei*

Згідно поставлених задач, які включають в себе відеоспостереження на

складі, та проведеного аналізу, пропонується використання в якості сервісу інтелектуального відеоспостереження систему на базі камер *Huawei SDC*.

4.2. Сервіс IP-телефонії

Існує безліч рішень в області програмних АТС, розглянемо найбільш поширені з них.

Asterisk – програмна АТС, здатна комутувати як *VoIP* виклики, так і виклики,

які здійснюються між *IP*-телефонами і традиційної телефонною мережею загального користування. Підтримує протоколи: *IAX*, *SIP*, *H*.323, *Skinny*, *UNIStim*. Підтримує кодеки: *G*.711(*ulaw* і *alaw*), *G*.722, *G*.723, *G*.729, *GSM*, *iLBC*, *LPC*-10, *Speex*. Призначена для малого бізнесу, кількість абонентів обмежена можливостями сервера. Весь необхідний функціонал може бути дописаний самостійно без фінансових витрат за короткий часовий інтервал, тому що на одну задачу застосовується один модуль. У порівнянні з *Cisco* або *Avaya*, *Asterisk* має низьку вартість розгортання. Програма є безкоштовною і всі витрати йдуть на покупку телефонів і сервера, необхідного для нормальної роботи АТС.

Asterisk не вимагає ніякої прив'язки до певного типу обладнання, так як продукт працює на операційних системах *Linux*, *FreeBSD*, *OpenBSD* і *Solaris* і ін. Є дуже гнучким рішенням. *Asterisk* в комплексі з необхідним обладнанням має всі можливості класичної АТС, підтримує безліч *VoIP*-протоколів і надає багаті функції управління дзвінками, серед яких:

- голосова пошта;
- конференція;
- *IVR* (інтерактивне голосове меню);
- центр обробки дзвінків (постановка дзвінків в чергу і розподіл їх по абонентам, використовуючи різні алгоритми);
- *Call Detail Record* (детальна інформація про виклик).

Для створення додаткової функціональності можна скористатися власною мовою *Asterisk* для написання плану дзвінків, написав модуль на мові С, або скориставшись *AGI* – гнучким і універсальним інтерфейсом для інтеграції з

зовнішніми системами обробки даних. Модулі, що виконуються через *AGI*, можуть бути написані на будь-якій мові програмування. *Asterisk* поширюється на умовах подвійний ліцензії, завдяки якої одночасно з основним кодом, поширюваним по відкритій ліцензії *GNU GPL*, можливе створення закритих модулів, що містять ліцензований код: наприклад, модуль для підтримки кодека *G*.729.

Cisco Unified Communication Manager (*Call Manager*). Призначений для мереж, що включають до 30000 абонентів. Програмно-апаратний комплекс забезпечує надійність функціонування системи і дозволяє конфігурувати безліч параметрів. Існує *Express* версія, призначена для невеликих компаній. Однією з переваг є технічна підтримка *Cisco*. При наявності договору на технічну підтримку всі проблеми вирішує корпорація *Cisco*. *Cisco Call Manager* призначений для компаній, яких цікавить відмінну якість зв'язку за немалі гроші.

Avaya IP Office. Система *IP Office* призначена для середніх мереж. Число користувачів обмежена потужністю сервера і кількістю ліцензій. Плати розширення, додатки повинні бути ліцензовані. *Avaya* має широкий спектр програм для керування сервером. *Avaya IP Office Manager* досить вдале рішення, тому що програма проста в використанні та можливе консольне керування за допомогою *Avaya Terminal Emulator*.

Asterisk є кращим рішенням тому, що підтримує безліч функцій, має можливість їх самостійного доповнення, не має прив'язки до конкретного виробника обладнання і є безкоштовним продуктом.

4.2.1. Налаштування SIP користувачів

Конфігурація *SIP* користувачів відбувається в файлі *sip.conf*. Об'єкти конфігурації – піри (*peers*), описуються в окремих секціях, які позначаються іменами в квадратних дужках. Діє принцип наслідування, як і в більшості файлів конфігурації *Asterisk*: все що задано після імені в квадратних дужках, відноситься до одного об'єкту, поки не буде оголошено наступного.

Категорія за замовчуванням - [general], задає глобальні налаштування драйвера

SIP Asterisk, які поширюються на всі об’єкти, але можуть бути перевизначені для окремих пірів в їхніх категоріях. За замовчуванням дана конфігурація має вигляд, як показано на рис. 4.3.

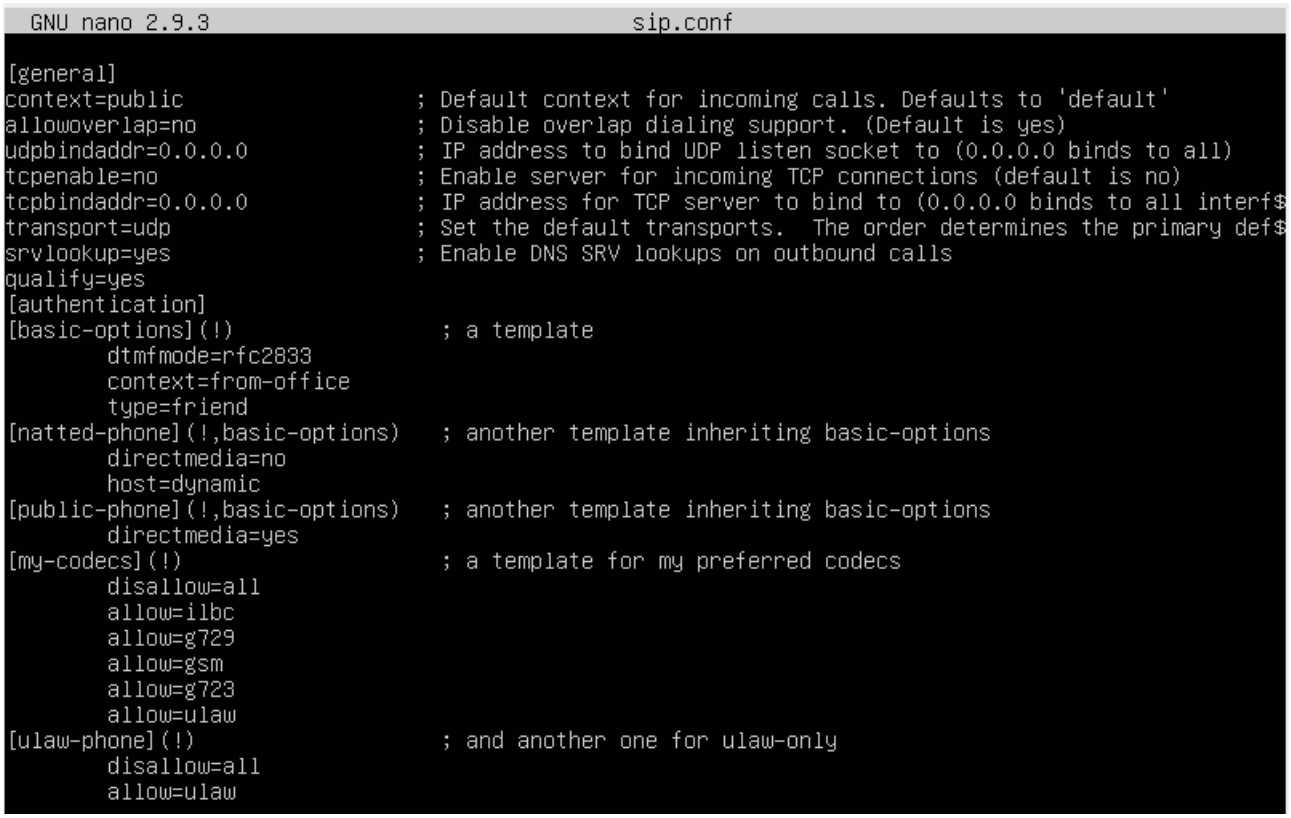

Рис. 4.3. Конфігурація *sip.conf* за замовчуванням

Замість використання пареметру *secret*, що містить пароль користувача у відкритому вигляді, рекомендується використання параметру *md*5*secret*, що зберігає *md*5-хеш паролю [25]. Для головного офісу пропонується наступне доповнення базової конфігурації *SIP*-користувачів:

[common-friend](!)

Type=friend Allow=ulaw,alaw Host=dynamic

[h-office](!)

context= headquarter

[h-secretary](common-friend, h-office)

md5Secret= 5f4dcc3b5aa765d61d8327deb882cf99 [h-it-1](common-friend, h-office)

md5Secret= 7c6a180b36896a0a8c02787eeafb0e4c [h-finance-1](common-friend, h-office)

md5Secret= c24a542f884e144451f9063b79e7994e [h-marketing-1](common-friend, h-office)

md5Secret= 482c811da5d5b4bc6d497ffa98491e38 [incoming]

host=sip.test.ua context= h-incoming insecure=port,invite type=user

username=749511377567 secret=Pa$$w0rd fromuser=74951234567 fromdomain=sip.test.ua qualify=yes

[outgoing]

host=sip.test.ua context= h-outgoing insecure=port,invite type=peer

username=749511377567 secret=Pa$$w0rd fromuser=74951234567 fromdomain=sip.test.ua qualify=yes

4.2.2. Безпека VoIP

Безпеку *VoIP* можна поділити на два аспекти: безпека сигналізації дзвінків та безпека в медіа (голосовій) сесії. Це досягається завдяки протоколам *TLS* та *SRTP*, які функціонують для забезпечення захисту сигналізації та шифрування аудіо/відео дзвінків [30].

Протокол *TLS* ставить собі за мету створення між двома вузлами мережі захищеного від прослуховування і підміни інформації каналу зв’язку, придатного для передачі довільних даних в обох напрямках, а також перевірку того, що обмін даними відбувається між саме тими вузлами, для яких канал і створено початково. Ці завдання називаються, відповідно, забезпеченням конфіденційності, цілісності та автентичності з’єднання (аутентифікації). З фундаментальних завдань захисту інформації, *TLS* не охоплюють тільки одну: забезпечення доступності інформації – і це завдання знаходиться за рамками даного протоколу [31].

Протокол *SRTP* ж в свою чергу, забезпечує конфіденційність, автентифікацію повідомлень та захист від відтворення як для одноадресних, так і для багатоадресних потоків *RTP* та *RTCP*. Він може досягти високої пропускної здатності та низького розширення пакетів навіть у середовищах, які є сумішшю дротових та бездротових мереж.

SRTP знаходиться в моделі *TCP*/*IP* між прикладним рівнем *RTP*/*RTCP* і транспортним рівнем, генеруючи захищені пакети *RTP* з потоку *RTP*/*RTCP* і пересилаючи їх на приймач. Подібним чином він також перетворює вхідні захищені пакети *SRTP* в пакети *RTP*/*RTCP* [32].

Проаналізувавши протоколи *TLS* та *SRTP*, рекомендується їхнє використання в даному сервісі телефонії корпоративної мережі для забезпечення захисту дзвінків.

4.2.3. Налаштування плану набору

Конфігурація плану набору(*Dialplan*) міститься в файлі конфігурації *Asterisk* - *extensions.conf*. Це один з найважливіших конфігураційних файлів. У ньому визначається обробка і маршрутизація вхідних і вихідних дзвінків. Цей файл керує поведінкою всіх з'єднань що проходять через систему *IP*-телефонії.

Діалплан ділиться на розділи, звані контекстами, для поділу різних частин діалплана (рис. 4.4). Розширення, визначене в одному контексті, повністю ізольовано від розширень в будь-якому іншому контексті, якщо взаємодія спеціально не дозволена. Обидва абонента знаходяться в одній і тій же системі, взаємодіючи з одним і тим же діалпланом, але оскільки вони прибули в різні контексти, то шлях обробки дзвінка буде різним для даних абонентів. Дії, що відбувається з кожним викликом, визначаються кодом діалплана в кожному контексті. Контексти визначаються у файлі *extensions.conf*. Ім'я контексту поміщається в квадратні дужки ([]). Ім'я може складатися з букв *A* - *z* (верхній і нижній регістр), чисел від 0 до 9, а також дефіса і підкреслення.

В телекомунікаційної галузі слово *extension* (розширення) зазвичай відноситься до числового ідентифікатора, який при наборі буде дзвонити на телефон (або викликати системний ресурс, такий як голосова пошта або черга). В *Asterisk* розширення представляє собою дещо більше потужне, оскільки воно визначає унікальну серію кроків (кожен крок, який містить додаток), через які *Asterisk* буде приймати цей виклик. У кожному контексті ми можемо визначити стільки розширень, скільки буде потрібно. Коли певне розширення запускається, *Asterisk* буде слідувати кроків, що визначені для нього. Тому, саме розширення

визначають що відбувається з викликами, коли вони проходять через діалплан.

Кожне розширення може мати кілька кроків, які називаються пріоритетами. Пріоритети нумеруються послідовно, починаючи з одиниці і кожен виконує один конкретний додаток.

Додатки – це «робочі конячки» діалплана. Кожна програма виконує певну дію в поточному каналі, таке як – відтворення звуку, прийом набору сигналів *DTMF*, пошук в базі даних, виконання виклику в канал, завершення виклику або щось інше [25, 26].

Рис. 4.4. Базовий прототип діалплану

Враховуючи вище сказане, пропонується використання наступного діалплану для головного офісу:

[h-admin]

exten => 10101,1, Dial(SIP/h-secretary, 30, T) same => n, Hangup

[h-it]

exten => 10201,1, Dial(SIP/h-it-1, 30) same => n,Hangup

[h-marketing]

exten => 10401,1, Dial(SIP/h-marketing-1, 30) same => n,Hangup

[h-finance]

exten => 10301,1, Dial(SIP/h-finance-1, 30) same => n,Hangup

[h-incoming]

exten => 5060,1,NoOp(Incoming call…)

same => n, GotoIfTime(9:00-18:00,mon-fri,,*?h-admin, 10101,1) same => n, Playback(home/asterisk/workOffTime)*

same => n, Hangup [h-outgoing]

exten => _0XXXXXXXXX,1,NoOp(Calling outside ${EXTEN}…) same => n, Dial(SIP/outside/${EXTEN})

[headquarter]

include => h-admin include => h-it

include => h-marketing include => h-finance

exten => _0XXXXXXXXX, 1, Goto(h-outgoing, {EXTEN}, 1)

В випадку головного офісу план набору складається з семи контекстів:

- контекст для адміністрації офісу;
- контекст для IT-відділу;
- контекст для відділу маркетингу;
- контекст для відділу бухгалтерії;
- контекст для вхідних дзвінків;
- контекст для вихідних дзвінків;
- загальний контекст для офісу, що об’єднує в себе усі відділи.

Запропонована структура діалплану дозволить легко змінювати особливості обробки дзвінка для конкретного відділу, не втручаючись в план обробки дзвінків інших відділів. Також, додана перевірка для часу вхідного дзвінка. У випадку дзвінка не у робочий графік, абоненту буде повідомлено про це наперед записаним повідомленням *workOffTime* та дзвінок буде завершено.

4.2.4. Налаштування переадресації дзвінків

Як відомо, в телефонії існує два основних види переадресації (або трансферу -*transfer*) вхідних дзвінків (рис. 4.5), це:

Attendant Transfer – переадресація дзвінка, при якому оператор, отримавши інформацію від абонента, ставить дзвінок на утримання, потім ініціює другий виклик третій стороні (абоненту, з яким хоче з’єднатися той, хто телефонує), повідомляє про вхідний дзвінок і лише після дозволу третьої сторони, з’єднує з абонентом. Після цього, оператор кладе трубку і більше ніяк не впливає на виклик. Таким чином, оператор залишається впевненим в тому, що той, хто телефонує з’єднаний з потрібним абонентом. У разі, якщо у оператора не

виходить додзвонитися до абонента або він повідомляє, що не може в даний момент прийняти дзвінок, оператор знімає дзвінок з утримання та просить його передзвонити пізніше.

Blind Transfer – з назви стає зрозуміло, що даний вид перекладу є "сліпим", тобто оператор переводить дзвінок, не повідомляючи третю сторону про вхідному виклику. Не важко здогадатися, що якщо абонент зайнятий або не відповідає, то виклик просто обривається.

Рис. 4.5. Налаштування доступу до переадресації в *features.conf*

Для початку потрібно налаштувати синтаксис, за яким буде розпочинатись переадресація. У функції *features.conf* потрібно налаштувати параметри *blindxfer* або *atxfer* в розділі *Featuremap*. Параметри налаштовуються за допомогою символьного рядка двотонального багаточастотного аналогового сигналу(*DTMF*), який буде використовуватись для доступу до трансферу. Для a*ttendant transfer* буде використовуватись *DTMF* символ «*», а для «сліпого» трансферу – «#» [27].

4.3. Сервіс відеоконференцій

Відомі компанії пропонують безліч рішень для відеоконференцій із закритим кодом. Всі вони роблять приблизно одне і те ж, і все ж більшість вимагає встановлення власного програмного забезпечення, перш ніж ним користуватись.

Одним з найбільших рішень орієнтованих на бізнес-сектор є *Cisco WebEx,*

який є надійним рішенням для віддаленої співпраці та включає такі послуги, як кімнати для відеоконференцій з можливістю спільного використання файлів, демонстрація робочого столу. До недоліків відноситься те, що дане рішення вимагає встановлення власного ПЗ, висока вартість тарифів та суттєві обмеження безкоштовної версії(наприклад, обмеження часу конференції в 50 хвилин) [33].

За межами корпоративного сектора багато програм також дозволяють проводити відеоконференції. Популярні приклади – *Skype*, *Zoom* та *Google Meet*.

Skype належить *Microsoft* і використовує власний протокол для передачі потоків мультимедіа. Також для використання *Skype* потрібно встановлювати додаток.

Google Meet обмежує кількість учасників відеодзвінків лише 25 людьми за один дзвінок (10 найактивніших учасників відображаються внизу екрана) [21]. Запис відеоконференцій виходить за рамки безкоштовного тарифу. Як перевагу, *Meet* не має жодних відомих обмежень щодо тривалості дзвінків.

Zoom дозволяє користувачам брати участь у відеоконференції до ста учасників. Функція перегляду галереї дозволяє побачити до 49 з цих учасників на одному екрані. Хоча *Zoom* дозволяє здійснювати необмежену кількість дзвінків, кожен дзвінок може тривати лише до 40 хвилин в безкоштовній версії. Також, *Google Meet* та *Zoom* не потребують встановлення додаткового ПЗ так, як працюють через браузер.

Проаналізувавши вищезгадані рішення відеоконференцій та враховуючи те, що рекомендовано використання в якості сервісу *IP*-телефонії *Asterisk* та використання *IP*-телефонів *Fanvil X4,* що підтримують функцію відеоконференцій, пропонується використання *Astrerisk ConfBridge* в якості сервісу відеоконференцій. Це дозволить уникнути обмежень вищезгаданих рішень(такі як обмеження часу конференції чи кількості учасників), не потребує встановлення спеціалізованого ПЗ та не потребує звертання до сторонніх серверів.

4.3.1. Налаштування ConfBridge

ConfBridge має чотири внутрішні концепції:

- номер конференції;

- профіль конференції;
- профіль користувача;
- меню конференції.

Номер конференції – це числове представлення окремих “кімнат” у конференціях. Абоненти, що знаходяться на конференції з однаковим номером, потрапляють в одну і ту же конференцію та з’єднуються між собою. Абоненти, які входять у конференцію з різними номерами, знаходяться в різних конференціях і не можуть спілкуватися з іншими. Профіль конференції – це набір параметрів, що керують поведінкою конкретної “кімнати” конференцій. Кожна кімната конференції повинна мати власний профіль. Профіль користувача – це набір параметрів, які контролюють роботу та права користувачів, як члена певної конференції "кімнати". Меню конференції - це набір параметрів, дії, які може виконувати користувач конференції за допомогою *DTMF*. Профілі та меню *ConfBridge* налаштовуються у файлі конфігурації *confbridge.conf* [20, 21].

Для роботи відеоконференцій в *ConfBridge* необхідно створити два профіля користувача та меню(для адміністратора та звичайного користувача), та профіль конференції. Пропонується використання наступної конфігурації для профілю конференції:

[sample_bridge]

type=bridge max_members=50 mixing_interval=20 internal_sample_rate=auto record_conference=yes video_mode = follow_talker

Як можна побачити, вона дозволяє до 50 учасників, інтервал міксування аудіо 20мс, запис конференції та метод показу відео того, хто говорить в даний момент. В якості конфігурації профілів адміністратора та користувача рекомендується наступна:

[sample_user]

type=user announce_user_count_all=yes announce_join_leave=yes dsp_drop_silence=yes denoise=yes

pin=123

[sample_admin]

type=user admin=yes

announce_user_count_all=yes announce_join_leave=yes dsp_drop_silence=yes denoise=yes

pin=2277

В вищезгаданій конфігурації включено повідомлення про кількість учасників відеоконференції та повідомлення приєднання/від'єднання учасників, зменшення фонового шуму та вимикання передачі аудіо у випадку тиші, що значно підвищує продуктивність сервісу. Нище подана конфігурація меню конференції: *[sample_user_menu]*

type=menu

**=playback_and_continue(conf-usermenu)*

**1=toggle_mute 1=toggle_mute*

**4=decrease_listening_volume 4=decrease_listening_volume*

**6=increase_listening_volume 6=increase_listening_volume*

**7=decrease_talking_volume 7=decrease_talking_volume*

**8=leave_conference 8=leave_conference*

**9=increase_talking_volume 9=increase_talking_volume*

[sample_admin_menu] type=menu

**=playback_and_continue(conf-adminmenu)*

**1=toggle_mute 1=toggle_mute*

**2=admin_toggle_conference_lock 2=admin_toggle_conference_lock*

**3=admin_kick_last 3=admin_kick_last*

**4=decrease_listening_volume 4=decrease_listening_volume*

**6=increase_listening_volume 6=increase_listening_volume*

**7=decrease_talking_volume 7=decrease_talking_volume*

**8=leave_conference 8=leave_conference*

**9=increase_talking_volume 9=increase_talking_volume*

За допомогою *DTMF*, учасники конференції можуть: вмикати/вимикати мікрофон, регулювати власну гучність та гучність інших, виходити з конференції. Додатково, адміністратор може блокувати конференцію та змінювати склад

учасників. Також, необхідні мінімальні зміни в плані набору:

[conferences]

exten => _9XX,1,ConfBridge(${EXTEN})

Даний контекст описує що, адміністратор конференції, набравши трьохзначний номер, що починається з дев'ятки, зможе створити конференцію, а користувачі приєднатись до існуючої.

4.3.2. Підвищення ефективності сервісу

Для підвищення ефективності сервісу відеоконференцій на *Asterisk ConfBridge*

необхідно виконати наступні кроки:

- увімкнути *dsp_drop_silence* в профілі користувача. Увімкнення цього параметру означає, що звук користувачів, які не говорять, не передається;

- збільшити інтервал мікшування аудіо. Інтервал за замовчуванням - 20 мс. Інші варіанти - 10, 40 та 80 мс. Більш низькі значення забезпечують вищу якість звуку, але вимагають значно більшої потужності процесора сервера. Встановлення значення 80 забезпечує найбільшу кількість можливих учасників;

- підключити учасників з однаковою частотою дискретизації. Використання різної частоти дискретизації збільшує навантаження на сервер *Asterisk*;

- запустити *Asterisk* з вищим пріоритетом. За замовчуванням *Asterisk* працює з нормальним пріоритетом порівняно з іншими процесами в системі. Щоб максимізувати кількість можливих клієнтів, *Asterisk* слід запускати, використовуючи прапор *-p* (в реальному часі). Якщо навантаження стає занадто великим, це може негативно вплинути на продуктивність інших процесів, включаючи саму консоль, ускладнюючи віддалене адміністрування повністю завантаженої системи.

Дотримання вищевказаних рекомендацій дозволить збільшити кількість підключених клієнтів до того, як погіршиться якість звуку та відео [35].

Висновки за розділом 4

Вибір сервісів – це завершальний етап побудови мультисервісної корпоративної мережі. Згідно вимог, необхідно було обрати в ході аналізу три сервіси для корпоративної мережі:

- сервіс інтелектуального відеоспостереження;
- сервіс *IP*-телефонії;
- сервіс відеоконференцій.

В якості сервісу інтелектуального відеоспостереження обрана система на базі програмно-конфігурованих камер *Huawei*. Дане рішення має такі переваги, як: висока обчислювальна потужність, завдяки процесору *Ascend*, онлайн-оновлення алгоритмів і самонавчання, відкрита програмна архітектура, яка дозволяє інтегрувати нові алгоритми від партнерів по екосистемі, забезпечуючи ефективну роботу штучного інтелекту. Крім того, відкрита апаратна архітектура передбачає можливість підключення різних датчиків сторонніх виробників.

В ході аналізу рішень сервісу *IP*-телефонії вибір впав на рішення на базі *Asterisk* тому, що підтримує безліч функцій, має можливість їх самостійного доповнення, не має прив’язки до конкретного виробника обладнання і є безкоштовним продуктом. Запропоновано рішення безпеки у вигляді *TLS* та *SRTP,* налаштування *SIP* користувачів, плану набору та переадресації.

Проаналізувавши та порівнявши існуючі рішення відеоконференцій та враховуючи те, що рекомендовано використання в якості сервісу *IP*-телефонії *Asterisk* та використання *IP*-телефонів *Fanvil X4,* що підтримують функцію відеоконференцій, пропонується використання *Astrerisk ConfBridge* в якості сервісу відеоконференцій. Це дозволить уникнути обмежень відомих рішень(таких як обмеження часу конференції чи кількості учасників), не потребує встановлення спеціалізованого ПЗ та звертання до сторонніх серверів. Проаналізовано можливі рішення підвищення ефективності даного сервісу.

ВИСНОВКИ

Корпоративна мережа – це складна система, що забезпечує передачу різноманітної інформації між різними додатками та системами, що використовуються в єдиній мережі підприємства. Відомі рішення побудови корпоративних мереж досить специфічні, оскільки розглядають конкретні системи і наявні результати неможливо безпосередньо використовувати при побудові і аналізі інших мереж з відмінними параметрами. Це пояснюється сильною залежністю початкових параметрів мережі від пропонованих вимог до обробки, захисту, представлення інформації та сервісів, які дана мережа надає. У кожному конкретному випадку необхідне оригінальне рішення, що зумовлено специфікою мережі та сервісів.

Термін служби мережевої інфраструктури в декілька разів більше, ніж у додатків та сервісів. Мультисервісна корпоративна мережа забезпечує можливість розгортання нових сервісів і їх ефективне функціонування при збереженні інвестицій в неї. Рекомендується використання багаторівневого підходу при побудові структури корпоративної мережі, а саме трьохрівневої моделі. Такий підхід полягає в поданні архітектури створюваної мережі у вигляді ієрархічних рівнів, кожен з яких вирішує певні для цього рівня завдання. Також, це дозволяє додавати рівні до мережі, що розширюють функціональні можливості мережі та мінімізувати ресурсні витрати для пошуку і усунення несправностей в мережі.

Проаналізовано існуючі рішення побудови мультисервісних корпоративних мереж такі, як *Cisco AVVID* та *Huawei One Net*. Пропонується використання рішення від *Huawei* тому що, воно не має прив’язки до конкретних виробників мережевого обладнання, має централізовану систему управління мережею *eSight* та постачає власні різноманітні сервіси, в тому числі із використанням штучного інтелекту.

В ході аналізу структури підприємства, запропоновано використати топологію ієрархічної зірки(дерева).

Перевагами обраної топології є:

- масштабованість;
- легкий пошук проблемних вузлів;

- висока продуктивність мережі.

Недоліки:

- вихід з ладу концентратора впливає на роботу всієї мережі;
- високі витрати кабелів.

Збільшені витрати на додаткові кабелі легко нівелюються її перевагами. А вразливість концентраторів вирішується за допомогою технологій стекування.

Для зв'язку підрозділів підприємства використовується *VPN*. Технологія *VPN* надає компанії можливості дорогої приватної орендованої лінії за набагато нижчою вартістю, використовуючи спільну мережу, таку як Інтернет. Для підвищення відмовостійкості ядра корпоративної мережі використовувались технології стекування комутаторів та протокол *VRRP*. Мережу поділено на 14 віртуальних локальних мереж для зменшення трафіку в мережі(наприклад, широкомовного) та можливості застосування політик безпеки для окремих *VLAN*.

Від мережевого обладнання, яке використовується при побудові мультисервісної корпоративної мережі залежить простота налаштування, ефективність моніторингу та масштабованість мережі. В ході проведеного аналізу пропонується використання обладнання *Huawei* тому, що воно має наступні переваги:

- відповідність обладнання міжнародним стандартам, що забезпечує хорошу сумісність з продукцією інших виробників;
- всі продукти працюють на уніфікованій операційній системі (*VRP*), що має 17 років розвитку;
- повне рішення для мережі підприємства з широким набором продуктів, включаючи *IP*, оптичний і РРЛ транспорт, 3*G*, і *PON*;
- економічність, завдяки технології *SmartEnergy;*
- єдина уніфікована система управління мережею керує всією мережею підприємства. Не потрібно перемикатися між різними системами для конфігурації різного устаткування;
- надає сервіси телекомунікації, сервіси з використанням штучного інтелекту (комп'ютерного зору) та інші;
- має низьку вартість, в порівнянні з обладнанням від *Cisco Systems.*

В якості сервісу відеоспостереження запропоновано використання рішення на базі програмно-конфігурованих камер *Huawei* тому, що вони мають високу обчислювальну потужність, завдяки процесору *Ascend*, онлайн-оновлення алгоритмів і самонавчання, відкриту програмну архітектуру, яка дозволяє інтегрувати нові алгоритми від партнерів по екосистемі, забезпечуючи ефективну роботу штучного інтелекту.

Після аналізу та порівняння рішень сервісу *IP*-телефонії пропонується використання сервісу на базі АТС *Asterisk*. Він підтримує безліч телефонних функцій, має гнучке налаштування плану набору, можливість реалізації додаткового специфічного функціоналу шляхом програмування модулів, не має прив'язки до конкретного виробника обладнання та є безкоштовним ПЗ. Також, запропоновано рішення захисту дзвінків, що полягає в використанні протоколів *TLS* та *SRTP*.

Враховуючи використання в якості сервісу *IP*-телефонії *Asterisk* та *IP*-телефонів *Fanvil X4,* що підтримують функцію відеоконференцій, пропонується використання *Astrerisk ConfBridge* в якості сервісу відеоконференцій. Окрім спрощення налаштування сервісу, завдяки встановленому та налаштованому *Asterisk*, це дозволить уникнути обмежень відомих рішень відеоконференцій (таких як обмеження часу конференції чи кількості учасників), не потребує встановлення спеціалізованого ПЗ та звертання до сторонніх серверів.

В даній роботі були розглянуті принципи та рішення побудови корпоративних мереж підприємств, здійснено аналіз рішень побудови мультисервісної корпоративної мережі, запропоновано рішення структури корпоративної мережі даного підприємства, здійснено порівняння та вибір мережевого обладнання, вирішені питання сервісів відеоспостереження, *IP*-телефонії та відеоконференцій, надано рекомендації щодо покращення їхньої роботи.

Таким чином, дане рішення може використовуватись при побудові мультисервісних корпоративних мереж підприємств.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cisco AVVID Network Infrastructure Overview – URL: https://www.cisco.com/web/offer/CAT4500/toolkit/comin_ov.pdf

2. Huawei One Net – URL: https://support.huawei.com/enterprise/en/data-communication-common/one-net-campus- pid-7997341

3. Kizza J. M. Guide to Computer Network Security / Joseph Migga Kizza. Chattanooga: Springer, 2015. 550 p.

4. Canavan J. Fundamentals of network security / Jonh Canavan. Artech House telecommunications, 2001. 341 p.

5. Rajamohan P. An Overview of Virtual Router Redundancy Protocol Techniques and Implementation for Enterprise Networks / P. Rajamohan. Selangor: SEGi University Kota Damansara, 2018. 123 p.

6. Huawei S2700 – URL: https://e.huawei.com/ru/products/enterprise-networking/switches/campus-switches/s2700

7. Huawei S5700 – URL: https://e.huawei.com/ru/products/enterprise-networking/switches/campus-switches/s5700- si-model

8. Huawei AR1200 – URL: https://e.huawei.com/en/related-page/products/enterprise-network/routers/ar- g3/ar1200/Router_AR1200

9. Huawei AR3200 – URL: https://e.huawei.com/kz/products/enterprise-networking/routers/ar-g3/ar3200

10. IDC Trackers Show Moderate Growth in Worldwide Ethernet Switch and Router Markets in Q2 2019 – URL: https://www.idc.com/getdoc.jsp?containerId=prUS45487019

11. Fanvil X4 – URL: https://www.fanvil.com/Product/info/id/72.html

12. Reasons Why Video Surveillance Solutions Need AI to Evolve – URL: https://www.ifsec.events/india/visit/news-and- updates/5-reasons-why-video-surveillance-solutions-need-ai-evolve

13. Software-Defined Camera – URL: https://e.huawei.com/en/products/intelligent-vision/cameras/software-defined-camera/what-is-software-defined-camera

14. What Is a Software-Defined Camera? – URL: https://e.huawei.com/ua/products/intelligent-vision/cameras/software-defined- camera

15. Three Mission-Critical Features Make Huawei SDC Unique – URL: https://e.huawei.com/ua/products/intelligent- vision/cameras/software-defined-camera/software-defined-camera-vs-ip-camera

16. Meggelen J. V. Asterisk: The Definitive Guide / J. V. Meggelen, R. Bryant, L. Madsen. NY: O`REILLY, 2013. 845 p.

17. Google Meet pricing – URL: https://apps.google.com/meet/pricing/

18. Zoom pricing – URL: https://zoom.us/pricing

19. Asterisk Security using Transport Layer Security and Secure Real-Time Transport Protocol – URL: https://www.academia.edu/38306574/Asterisk_Security_using_Transport_Layer_Security_and_Secure_Real_Time_Transport_Protocol

20. The Secure Real-time Transport Protocol (SRTP) – URL: https://tools.ietf.org/html/rfc3711

21. Cisco Webex Plans and Pricing – URL: https://www.webex.com/pricing/index.html

22. Zoom vs Google Meet – URL: https://www.bustle.com/p/6-differences-between-zoom-google-hangouts-you-should-know- 22647281Asterisk ConfBridge – URL: https://wiki.asterisk.org/wiki/display/AST/ConfBridge

23. Адельштайн Т.М. Системе адміністрування в Linux / Т.М. Адельштайн, Б.Ю. Любанович ; [пер. с англ. А. Одноочко]. : Київ, 2018. 288 с.

24. Азаров О.Д. Комп’ютерні мережі: навчальний посібник / О.Д. Азаров, С.М. Захарченко, О.В. Кадук. Вінниця : Вінницький Національний Технічний Університет, 2013. 371 с. ISBN 978-966-641-543-4

25. Буров Є.В. Комп’ютерні мережі, Львів : Магнолія, 2016, 262 с.

26. Жуковицький І.В. Аналіз безпеки бездротових мереж Wi-Fi в автоматизованих системах залізничного транспорту / І. В. Жуковицький, І. О. Педенко // Наука та прогрес транспорту. 2020. № 4 (88). С. 7-21.

27. Комп'ютерні мережі. Підручник / Ю.О. Кулаков, Г.М. Луцький. Київ :

Вид-во "Юніор", 2015.

28. Комп'ютерні мережі. Технології, протоколи та моделювання: Навч. посібник / Ю.В. Стасєв, І.В. Рубан, С.В. Дуденко, Д.В. Сумцов, О.І. Тимочко. Харків : ХНУПС, 2015.

29. Кулаков Ю. О. Комп'ютерні мережі / Ю. О. Кулаков, Г. М. Луцький. Київ : Юніор, 2003. 400 с.

30. Николайчук Я.М., Возна Н.Я., Пітух І.Р. Проектування спеціалізованих комп’ютерних систем / Навчальний посібник Тернопіль : ТзОВ "Терног раф". 2010.

31. Особливості побудови локальних мереж – URL:: http://studopedia.org/13-100846.html

32. Романовський Ю.Р. Адміністрування комп’ютерних мереж і систем: Навч.пос. / Ю.Р. Романовський, В.В. Олексюк, А.В. Балик. Тернопіль : Навчальна книга Богдан, 2014. 196 с.

33. Яковина В.С. Основи безпеки комп’ютерних мереж: Навчальний посібник / За ред. Д.В. Федасюка. Львів : НВФ "Українські технології", 2015. 396 с.