НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий інститут телекомунікаційних систем

Кафедра телекомунікацій

До захисту допущено:

Завідувач кафедри

_____ Сергій КРАВЧУК

«___»_____2024 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інженерія та програмування інфокомунікацій»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Побудова корпоративної мережі VoIP на основі відкритої платформи Elastix»

Виконав:
студент IV курсу, групи ТЗ-01
Черниш Микола Олександрович _____

Керівник:
Доцент кафедри ТК НН ІТС, к.т.н, доцент
Нестеренко Микола Миколайович _____

Рецензент:
Доцент кафедри ЕКІР НН ІТС, к.т.н, доцент,
Бердников Олег Михайлович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій КРАВЧУК
«___»_____2024 р.

ЗАВДАННЯ
на дипломну роботу студенту
Чернишу Миколі Олександровичу

1. Тема роботи «Побудова корпоративної мережі VoIP на основі відкритої платформи Elastix», керівник роботи Нестеренко Микола Миколайович, к.т.н, доцент, затверджені наказом по університету від «22» травня 2024 р. № 2064-с.

2. Термін подання студентом роботи 10 червня 2024 року

3. Вихідні дані до роботи:

1. Літературні джерела та наукові публікації, що описують принципи роботи та побудови VoIP-мереж.
2. Дослідження процесу розробки корпоративної мережі на основі платформи Elastix.
3. Аналіз необхідних для стабільної роботи системи аспектів забезпечення якості та безпеки VoIP-мереж.

4. Зміст роботи:

1. Оглянути базові принципи роботи технології VoIP, основні протоколи та стандарти.
2. Дослідити переваги та недоліки VoIP у порівнянні з традиційними методами зв’язку.

3. Дослідити відкриту платформу Elastix та спектр її функціональних можливостей.
4. Визначити вимоги, необхідні для впровадження корпоративної мережі на базі Elastix.
5. Проаналізувати аспекти забезпечення якості обслуговування та методи захисту від кібератак.
6. Зробити висновки щодо критеріїв тестування системи для стабільної роботи.

5. Перелік ілюстративного матеріалу
Слайд №1 Назва роботи
Слайд №2 Мета, об’єкт, предмет та завдання дослідження
Слайд №3 Вступ
Слайд №4-6 VoIP технології
Слайд №7 Платформа Elastix
Слайд №8 Аналіз вимог та планування мережі
Слайд №9 Забезпечення якості зв’язку QoS
Слайд №10 Безпека VoIP-мереж
Слайд №11 Резервне копіювання та відновлення
Слайд №12 Тестування системи на надійність
Слайд №12 Висновки

6. Дата видачі завдання 27 березня 2024 року

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Огляд літератури для аналізу принципу роботи VoIP	27.03.2024 – 14.04.2024	Виконано
2	Ознайомлення з платформою Elastix	15.04.2024 – 25.04.2024	Виконано
3	Ознайомлення з побудовою мережі VoIP	26.04.2024 – 11.05.2024	Виконано
4	Аналіз параметрів безпеки та якості обслуговування	12.05.2024 – 26.05.2024	Виконано
5	Підготовка та оформлення презентації для доповіді.	27.05.2024 – 10.06.2024	Виконано

Студент Микола ЧЕРНИШ

Керівник Микола НЕСТЕРЕНКО

РЕФЕРАТ

Дипломна робота на тему “Побудова корпоративної мережі VoIP на базі відкритою платформи Elastix” містить 57 сторінок, 6 таблиць. У роботі використано різноманітні джерела інформації, включаючи наукові публікації та електронні ресурси.

Актуальність дослідження полягає у тому, що традиційні системи телефонії стають все менш актуальними на фоні розширення та постійного розвитку мережі Інтернет, що досить ймовірно поступово буде призводити до повного витіснення традиційних систем.

Метою дипломної роботи є дослідження теоретичного підґрунтя, розгляд існуючих принципів побудови корпоративних мереж передачі даних на базі технології VoIP та вирішення побудови корпоративної мережі VoIP на базі відкритої платформи Elastix.

Об’єктом дослідження є корпоративна VoIP-мережа, побудована на базі відкритої платформи Elastix.

Предметом дослідження є процес створення корпоративної VoIP-мережі, побудованої на базі відкритої платформи Elastix.

Основними ключовими словами, пов’язаними з дипломною роботою, є “VoIP”, “Elastix”, “корпоративна мережа”, “якість обслуговування”, “критерії стійкості системи”.

ABSTRACT

The diploma thesis on the topic “Building a corporate VoIP network based on the Elastix open-source application” comprises approximately 57 pages, 6 tables. Various sources of information, including scientific publications and electronic resources, were used in the research.

The relevance of the research lies in the fact that traditional telephony systems are becoming less relevant against the background of the expansion and continuous development of the Internet, which will likely gradually lead to the complete displacement of traditional systems.

The aim of the thesis is to research the theoretical foundation, consider the existing principles of building corporate data transmission networks based on VoIP technology, and solve the construction of a corporate VoIP network based on the Elastix open-source application.

The object of the research is a corporate VoIP network built on the open Elastix platform. **The subject** of the research is the process of creating a corporate VoIP network based on the Elastix open-source application.

The key terms related to the thesis are "VoIP", "Elastix", "corporate network", "quality of service", "system stability criteria".

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

2FA	Two-Factor Authentication (двофакторна аутентифікація)
API	Application Programming Interface (інтерфейс прикладного програмування)
CLI	Command Line Interface (інтерфейс командного рядка)
DHCP	Dynamic Host Configuration Protocol (протокол динамічної конфігурації хостів)
DNS	Domain Name System (система доменних імен)
DoS	Denial of Service (атака на відмову в обслуговуванні)
GUI	Graphical User Interface (графічний інтерфейс користувача)
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System (система виявлення вторгнень)
IP	Internet Protocol
IPS	Intrusion Prevention System (система запобігання вторгнень)
LAN	Local Area Network (локальна мережа)
MITM	Man-In-The-Middle (атака типу "людина посередині")
PBX	Private Branch Exchange (приватна телефонна станція)
QoS	Quality of Service
RTP	Real-time Transport Protocol (протокол реального часу)
SIP	Session Initiation Protocol
SRTP	Secure Real-time Transport Protocol
SSL	Secure Sockets Layer (рівень захищених сокетів)
TCP	Transmission Control Protocol (протокол керування передачею)
TLS	Transport Layer Security
UDP	User Datagram Protocol (протокол користувацьких дейтаграм)
VLAN	Virtual Local Area Network (віртуальна локальна мережа)
VoIP	Voice over Internet Protocol

VPN	Virtual Private Network (віртуальна приватна мережа)

ВСТУП

З розвитком інформаційних технологій ефективна комунікація стає однією з ключових складових успіху будь-якої організації. Сучасні підприємства все більше звертають увагу на технології, що забезпечують зручність, гнучкість і економічність у сфері зв'язку. Однією з таких передових технологій є VoIP (Voice over Internet Protocol), яка дозволяє здійснювати голосові дзвінки через інтернет, обходячи традиційні телефонні мережі.

Актуальність теми

Тема побудови корпоративної VoIP-мережі на основі платформи Elastix є надзвичайно актуальною з кількох причин. По-перше, використання VoIP дозволяє суттєво знизити витрати на зв'язок. Це особливо важливо для компаній з великою кількістю міжнародних дзвінків або розгалуженою структурою, оскільки дзвінки через інтернет значно дешевші. По-друге, VoIP-системи легко налаштовуються під потреби організації. Платформа Elastix дозволяє швидко масштабувати мережу, додаючи нових користувачів або функції, що робить її ідеальною для динамічних бізнес-середовищ.

Метою дослідження є розробка та впровадження корпоративної VoIP-мережі на основі відкритої платформи Elastix.

Завдання дослідження

1. Аналіз технологій VoIP та платформи Elastix
2. Планування корпоративної VoIP-мережі
3. Впровадження та налаштування платформи Elastix
4. Інтеграція та налаштування VoIP-обладнання
5. Забезпечення якості зв'язку та безпеки в VoIP-мережі
6. Оцінка ефективності впровадженої VoIP-мережі

Предметом дослідження є процес створення корпоративної VoIP-мережі на основі відкритої платформи Elastix.

Об'єктом дослідження є корпоративна VoIP-мережа, побудована на базі відкритої платформи Elastix.

Методи дослідження

1. Аналіз літератури та джерел інформації
2. Проектні методи
3. Методи моделювання та симуляції
4. Методи аналізу та синтезу
5. Методи забезпечення якості та безпеки

РОЗДІЛ 1

ОГЛЯД ТЕХНОЛОГІЙ VOIP ТА ПЛАТФОРМИ ELASTIX

1.1 Вступ до технологій VoIP

VoIP (Voice over Internet Protocol) є технологією, що дозволяє передавати голосові дані через IP-мережі, включаючи Інтернет, замість використання традиційних телефонних ліній. Основний принцип роботи VoIP полягає в перетворенні голосових сигналів у цифрові дані, які потім передаються по мережі як пакети даних. Це забезпечує значну гнучкість і економічну ефективність у порівнянні з традиційними аналоговими телефонними системами.

Процес передачі голосу через VoIP починається з аналогово-цифрового перетворення. Коли користувач говорить у мікрофон, аналоговий голосовий сигнал перетворюється на цифровий сигнал за допомогою спеціального пристрою, званого кодеком (codec). Кодек виконує дві основні функції: кодування та декодування. Кодування передбачає перетворення аналогового сигналу в цифровий, а декодування - зворотний процес, перетворення цифрового сигналу назад у аналоговий, який може бути почутий через динамік[7].

Після кодування голосовий сигнал розбивається на невеликі пакети даних, кожен з яких містить частину голосового повідомлення разом з інформацією про адресу відправника і отримувача, а також службові дані, необхідні для правильної передачі пакету через мережу. Ці пакети передаються через IP-мережу за допомогою протоколів, таких як RTP (Real-Time Protocol) для передачі мультимедійних даних і SIP (Session Initiation Protocol) для встановлення, управління та завершення сеансів зв'язку.

SIP є одним з найважливіших протоколів у VoIP-технологіях. Він використовується для встановлення з'єднання між двома або більше кінцевими точками, а також для управління сеансами зв'язку, такими як дзвінки, конференції та відеозв'язок. Протокол SIP відповідає за ініціалізацію, зміну та завершення сеансу зв'язку, забезпечуючи таким чином гнучкість і можливість інтеграції з іншими мережевими сервісами.

RTP, у свою чергу, забезпечує передачу аудіо- та відеоданих у режимі реального часу. Цей протокол працює поверх транспортного протоколу UDP (User Datagram Protocol), який забезпечує швидку передачу даних без гарантій доставки, що є важливим для реального часу, де затримка є критичним фактором. RTP забезпечує синхронізацію та контроль якості передачі мультимедійних даних, що дозволяє підтримувати високу якість звуку та відео під час сеансу зв'язку[2].

Коли пакети досягають кінцевої точки, вони збираються у вихідний цифровий сигнал і декодуються назад у аналоговий голосовий сигнал за допомогою кодека. Цей аналоговий сигнал потім відтворюється через динамік, дозволяючи користувачеві почути оригінальне повідомлення. Процес перетворення та передача даних займає дуже малий час, забезпечуючи майже миттєву комунікацію.

VoIP також використовує додаткові технології для забезпечення якості обслуговування (QoS) та безпеки передачі даних. QoS дозволяє управляти пріоритетами трафіку, зменшуючи затримки і втрати пакетів, що критично для підтримки високої якості звуку. Безпека VoIP забезпечується за допомогою шифрування даних, аутентифікації користувачів і захисту від несанкціонованого доступу.

Завдяки своїм перевагам, таким як зниження витрат на зв'язок, гнучкість у налаштуванні та використанні, інтеграція з іншими мережевими сервісами і висока якість зв'язку, VoIP технології стали невід'ємною частиною сучасних комунікаційних систем. Вони знаходять застосування в бізнесі, освіті, охороні здоров'я і багатьох інших галузях, забезпечуючи ефективну та надійну комунікацію по всьому світу.

Таблиця 1.1

Основні протоколи та стандарти VoIP

Протокол/Стандарт	Опис
SIP (Session Initiation Protocol)	SIP (Session Initiation Protocol) є сигнальним протоколом, який відповідає за встановлення, управління та завершення сеансів зв'язку між двома або більше кінцевими точками в мережі. SIP використовує простий текстовий формат для повідомлень, що дозволяє легко інтегруватися з іншими інтернет-протоколами, такими як HTTP та SMTP. SIP-повідомлення можуть містити різну інформацію, включаючи адреси учасників сеансу, параметри з'єднання та інші метадані, необхідні для встановлення зв'язку.
RTP (Real-Time Transport Protocol)	RTP (Real-Time Transport Protocol) є протоколом, який використовується для передачі аудіо- та відеоданих у режимі реального часу. RTP працює поверх транспортного протоколу UDP (User Datagram Protocol), який забезпечує швидку передачу даних без гарантій доставки. RTP пакети містять корисні дані, такі як аудіо- або відеозаписи, а також заголовки, які включають інформацію про синхронізацію, номер послідовності та таймстамп. RTP часто використовується разом з RTCP (Real-Time Control Protocol), який забезпечує зворотний зв'язок про якість передачі, дозволяючи адаптувати параметри з'єднання для покращення якості обслуговування.
H.323	H.323 є набором рекомендацій, розроблених ITU (International Telecommunication Union), що визначають протоколи для аудіо-, відео- та даних у мережах з перемиканням пакетів, таких як Інтернет. H.323 включає кілька компонентів, включаючи H.225 для сигналізації та управління викликами, H.245 для управління медіа-каналами, H.235 для безпеки, а також кодеки для стиснення аудіо- та відеоданих. H.323 використовує архітектуру на основі зон, де кожна зона керується Gatekeeper (шлюзовим сервером), який забезпечує управління викликами, адресацію та контроль доступу. H.323 підтримує інтероперабельність з традиційними телефонними системами та іншими VoIP-протоколами, що робить його гнучким і масштабованим рішенням для різних типів мереж.

Використання VoIP (Voice over Internet Protocol) має значний вплив на сучасні комунікаційні системи, забезпечуючи широкі можливості для зниження витрат, підвищення ефективності та гнучкості.

Переваги VoIP

Однією з найбільших переваг VoIP є економічна ефективність. Використання VoIP дозволяє значно знизити витрати на телефонний зв'язок, особливо для компаній, які здійснюють багато міжнародних дзвінків або мають розгалужену структуру з великою кількістю філій. Традиційні телефонні системи

зазвичай стягують високі тарифи за міжнародні дзвінки, тоді як дзвінки через інтернет є значно дешевшими або навіть безкоштовними, якщо обидва абоненти використовують одну й ту ж VoIP-платформу.

Гнучкість і масштабованість є іншою важливою перевагою VoIP. Ця технологія дозволяє легко додавати нових користувачів і розширювати мережу без значних додаткових витрат на обладнання та інфраструктуру. Це робить VoIP ідеальним рішенням для компаній, які швидко ростуть або мають сезонні коливання в чисельності працівників. Крім того, VoIP-системи легко інтегруються з іншими бізнес-додатками, такими як CRM-системи, що дозволяє покращити продуктивність і ефективність бізнес-процесів[1].

VoIP також пропонує широкий спектр додаткових функцій, які недоступні в традиційних телефонних системах. До них належать відеоконференції, автоматизовані голосові меню (IVR), голосова пошта, переадресація дзвінків, інтеграція з електронною поштою та багато інших. Ці функції дозволяють покращити якість обслуговування клієнтів, підвищити продуктивність працівників і забезпечити кращу координацію всередині організації.

Ще однією перевагою VoIP є мобільність. Оскільки VoIP-зв'язок здійснюється через інтернет, користувачі можуть здійснювати і приймати дзвінки з будь-якої точки світу, де є інтернет-з'єднання. Це особливо корисно для працівників, які часто перебувають у відрядженнях або працюють віддалено. VoIP дозволяє зберегти єдиний номер телефону і залишатися на зв'язку незалежно від місця перебування.

Недоліки VoIP

Незважаючи на численні переваги, VoIP має й свої недоліки, які слід враховувати при впровадженні цієї технології. Одним із головних недоліків VoIP є залежність від якості інтернет-з'єднання. Для забезпечення високої якості голосових дзвінків необхідне стабільне та швидке інтернет-з'єднання. Якщо інтернет-з'єднання нестабільне або має низьку швидкість, це може призвести до погіршення якості зв'язку, затримок або навіть розриву дзвінків[2].

Ще одним недоліком VoIP є вразливість до збоїв електроживлення. Традиційні телефонні системи зазвичай працюють навіть під час відключення електроенергії, тоді як VoIP-системи залежать від наявності електроживлення для маршрутизаторів, модемів та інших мережевих пристроїв. У разі відключення електроенергії VoIP-зв'язок може бути втрачено, що може бути критичним для деяких бізнесів.

VoIP також може бути вразливим до кіберзагроз. Оскільки VoIP-зв'язок здійснюється через інтернет, він піддається ризикам, пов'язаним із мережею, таким як хакерські атаки, віруси, фішинг та інші форми кіберзлочинності. Для захисту VoIP-мережі необхідно впроваджувати додаткові заходи безпеки, такі як шифрування даних, аутентифікація користувачів і використання міжмережевих екранів.

Затримки та втрати пакетів є ще одним потенційним недоліком VoIP. Оскільки голосові дані передаються у вигляді пакетів через IP-мережу, вони можуть піддаватися затримкам або втрачатись у процесі передачі. Це може призвести до розривів у розмовах, погіршення якості звуку та загального зниження якості обслуговування. Для мінімізації цих проблем необхідно налаштовувати мережеві пристрої на підтримку якості обслуговування (QoS).

В цілому, незважаючи на деякі недоліки, переваги VoIP значно перевищують його недоліки для більшості бізнесів. VoIP-технологія забезпечує значні економічні вигоди, підвищує гнучкість і ефективність комунікацій, надає широкий спектр додаткових функцій та забезпечує мобільність користувачів. Правильне впровадження та налаштування VoIP-системи дозволяє мінімізувати потенційні недоліки і забезпечити надійний та якісний зв'язок для всіх користувачів[3].

1.2 Огляд платформ для побудови VoIP-мереж

При виборі VoIP-рішення для корпоративної мережі, компанії стикаються з вибором між відкритими та комерційними рішеннями. Кожен тип рішення має свої переваги і недоліки, і вибір залежить від специфічних потреб і ресурсів організації.

Таблиця 1.2

Порівняння відкритих та комерційних VoIP-рішень

Критерій	**Відкриті рішення**	**Комерційні рішення**
Витрати	Відсутність ліцензійних витрат. Низькі початкові витрати.	Висока вартість ліцензій та підписок на технічну підтримку.
Гнучкість і масштабованість	Висока гнучкість, можливість модифікацій і розширень.	Обмежені можливості для модифікацій та налаштувань.
Технічна підтримка	Підтримка через спільноту користувачів. Відсутність офіційної підтримки.	Офіційна технічна підтримка та гарантії від виробника.
Зручність у використанні	Вимагають високого рівня технічних знань для налаштування та підтримки.	Інтуїтивно зрозумілий інтерфейс, легкість встановлення та налаштування.
Інтеграція	Висока сумісність з іншими системами та програмним забезпеченням.	Інтегровані рішення з готовими компонентами для комунікацій.
Надійність і стабільність	Залежить від налаштувань і технічного обслуговування.	Висока надійність та стабільність, пройдені суворі тести.
Мобільність	Можливість налаштування мобільності залежно від потреб.	Підтримка мобільності в межах запропонованих функцій.
Залежність від постачальника	Незалежність від конкретного постачальника.	Залежність від постачальника та його політики.
Безпека	Потребують додаткових налаштувань для забезпечення безпеки.	Вбудовані функції безпеки, офіційні оновлення та підтримка.

Вибір платформи для впровадження VoIP (Voice over Internet Protocol) є важливим кроком, що вимагає ретельного аналізу та врахування різноманітних критеріїв. Кожна організація має свої специфічні потреби та обмеження, тому

необхідно врахувати кілька ключових факторів, щоб обрати найбільш підходящу платформу.

Одним з найважливіших критеріїв при виборі платформи для VoIP є вартість. Це включає не лише початкові витрати на придбання обладнання та програмного забезпечення, але й постійні витрати на підтримку, обслуговування, оновлення та ліцензії. Відкриті рішення, такі як Asterisk або FreeSWITCH, можуть бути привабливими через відсутність ліцензійних витрат, але вони можуть вимагати значних інвестицій у технічну підтримку та навчання персоналу. Комерційні рішення, такі як Cisco або Avaya, можуть мати високі початкові витрати, але забезпечують офіційну підтримку та регулярні оновлення, що може знизити загальні витрати на обслуговування в довгостроковій перспективі[2].

Гнучкість платформи є ключовим фактором, особливо для компаній, що мають динамічні потреби або планують швидкий ріст. Відкриті рішення зазвичай пропонують високу гнучкість, дозволяючи користувачам налаштовувати та розширювати систему відповідно до специфічних потреб організації. Вони можуть бути налаштовані для підтримки різних протоколів, інтеграції з іншими системами та додавання нових функцій. Комерційні рішення можуть бути менш гнучкими, але часто пропонують готові рішення з широким набором функцій, що можуть задовольнити потреби більшості організацій без додаткових налаштувань.

Надійність та стабільність платформи є критично важливими для забезпечення безперервної комунікації. Комерційні платформи, такі як Cisco або Avaya, зазвичай проходять суворі тести на надійність та стабільність і пропонують офіційну підтримку та регулярні оновлення. Відкриті платформи можуть бути менш надійними, якщо вони не налаштовані та не підтримуються належним чином. Однак, при правильній конфігурації та регулярному обслуговуванні вони можуть забезпечити високий рівень надійності.

Наявність технічної підтримки є важливим фактором при виборі платформи. Комерційні рішення зазвичай пропонують офіційну технічну підтримку від виробника, включаючи допомогу в налаштуванні, обслуговуванні та вирішенні проблем. Це може бути критично важливим для організацій, що не мають

власного технічного персоналу з достатніми знаннями. Відкриті рішення покладаються на підтримку спільноти користувачів, що може бути корисним, але не завжди забезпечує швидке та надійне вирішення проблем[4].

Здатність платформи інтегруватися з існуючими інформаційними системами організації, такими як CRM, ERP, електронна пошта та інші бізнес-додатки, є важливим критерієм. Відкриті рішення зазвичай мають високу сумісність і можуть бути налаштовані для інтеграції з різними системами через відкриті стандарти та API. Комерційні рішення також пропонують інтеграцію з багатьма популярними системами, але можуть мати обмеження в сумісності з менш поширеними або власними системами.

Безпека є одним з найважливіших аспектів при виборі VoIP-платформи. VoIP-системи можуть бути вразливими до різних кіберзагроз, таких як атаки на відмову в обслуговуванні (DoS), перехоплення дзвінків, шахрайство та інші. Комерційні рішення зазвичай пропонують вбудовані функції безпеки, такі як шифрування дзвінків, аутентифікація користувачів і захист від несанкціонованого доступу. Відкриті рішення також можуть забезпечувати високий рівень безпеки, але можуть вимагати додаткових налаштувань та конфігурацій для досягнення такого рівня захисту.

Простота використання платформи є важливим фактором, особливо для організацій, що не мають великого досвіду в налаштуванні та обслуговуванні VoIP-систем. Комерційні рішення зазвичай пропонують інтуїтивно зрозумілий інтерфейс і добре продуманий процес установки, що робить їх зручними для користувачів без глибоких технічних знань. Відкриті рішення можуть вимагати більше зусиль для налаштування та обслуговування, але також можуть бути адаптовані для зручності користувачів за допомогою налаштувань та додаткових інструментів[3].

Здатність платформи підтримувати мобільність користувачів є важливою для сучасних бізнесів, що потребують гнучкості в комунікаціях. VoIP-системи дозволяють користувачам здійснювати та приймати дзвінки з будь-якої точки світу, де є інтернет-з'єднання. Відкриті та комерційні рішення обидва можуть

забезпечувати високу мобільність, але комерційні рішення часто пропонують більш зручні та інтуїтивно зрозумілі мобільні додатки.

Вибір платформи для VoIP вимагає ретельного аналізу всіх цих критеріїв з урахуванням специфічних потреб і ресурсів організації. Правильний вибір платформи може забезпечити ефективні та надійні комунікації, що сприятимуть успіху бізнесу.

1.3 Особливості платформи Elastix

Elastix є однією з провідних платформ для впровадження VoIP (Voice over Internet Protocol) систем, заснованою на відкритому коді. Платформа поєднує в собі численні комунікаційні інструменти, такі як IP-телефонія, відеоконференції, електронна пошта, факс та інші сервіси, створюючи єдину інтегровану систему для ефективного управління корпоративними комунікаціями. Архітектура Elastix відрізняється високою гнучкістю, масштабованістю та модульністю, що робить її ідеальною для підприємств будь-якого розміру[4].

Основою архітектури Elastix є ядро, яке включає кілька ключових компонентів. Центральним елементом є Asterisk - потужний та гнучкий сервер для IP-телефонії, який відповідає за обробку голосових викликів. Asterisk забезпечує всі функції телефонної системи, включаючи маршрутизацію дзвінків, голосову пошту, автоматизовані голосові меню (IVR), конференц-зв'язок і багато інших. Його модульна архітектура дозволяє легко додавати нові функції та налаштовувати систему відповідно до потреб користувача. Elastix використовує FreePBX як графічний інтерфейс для управління Asterisk. FreePBX надає зручний веб-інтерфейс, який дозволяє адміністраторам легко налаштовувати та керувати системою без необхідності вивчати складні команди Asterisk. Через цей інтерфейс користувачі можуть додавати та налаштовувати внутрішні номери, маршрути дзвінків, створювати голосові меню та виконувати багато інших завдань.

Elastix також інтегрує інші важливі компоненти для забезпечення повного спектру комунікаційних послуг. Одним з таких компонентів є Postfix - потужний і

надійний сервер електронної пошти, який дозволяє налаштувати корпоративну пошту без необхідності використовувати окремий поштовий сервер. Це дозволяє об'єднати всі комунікації в одній системі, спрощуючи управління та підвищуючи ефективність роботи. Для управління факсами Elastix використовує Hylafax і Avantfax. Hylafax - це сервер факсів з відкритим кодом, який підтримує відправку та прийом факсів через інтернет, а Avantfax - це веб-інтерфейс для управління Hylafax. Ці компоненти дозволяють користувачам легко відправляти та отримувати факси, використовуючи електронну пошту або веб-інтерфейс, що робить процес роботи з факсами більш зручним і сучасним[4].

Безпека є важливим аспектом будь-якої комунікаційної системи, і Elastix не є винятком. Платформа включає кілька компонентів для забезпечення безпеки. Одним з таких компонентів є fail2ban - інструмент для захисту від атак, що базується на аналізі лог-файлів та блокуванні IP-адрес, які виявляються підозрілими. Це допомагає запобігати несанкціонованому доступу та захистити систему від потенційних загроз. Elastix також використовує IPTables для управління мережевими фільтрами та забезпечення додаткового рівня безпеки. IPTables дозволяє налаштовувати правила фільтрації трафіку, що допомагає контролювати доступ до системи та запобігати атакам.

Однією з найбільших переваг Elastix є його здатність інтегруватися з іншими системами та додатками. Платформа підтримує інтеграцію з різноманітними CRM-системами, такими як vTiger та SugarCRM, що дозволяє об'єднати комунікаційні функції з управлінням відносинами з клієнтами. Це дає змогу покращити продуктивність і ефективність бізнес-процесів, оскільки всі дані та інструменти знаходяться в одній системі. Наприклад, коли клієнт телефонує, система автоматично відображає інформацію про нього з CRM, що дозволяє оператору швидко отримати доступ до історії взаємодії з клієнтом і надавати більш персоналізоване обслуговування. Це підвищує задоволеність клієнтів і покращує репутацію компанії[4].

Elastix також підтримує різні протоколи та стандарти, такі як SIP, IAX2, H.323 та інші, що забезпечує сумісність з широким спектром VoIP-пристроїв та

систем. Це дозволяє легко інтегрувати нові пристрої та додатки, розширюючи функціональність системи без значних зусиль[6].

Моніторинг і аналітика є важливими аспектами управління комунікаційною системою, і Elastix надає потужні інструменти для цього. Одним з таких інструментів є CDR (Call Detail Records) - журнал викликів, який дозволяє відстежувати всі дзвінки, що проходять через систему. Це дає змогу аналізувати використання ресурсів, визначати проблемні зони та оптимізувати роботу системи. Elastix також включає інструменти для моніторингу в реальному часі, такі як FOP2 (Flash Operator Panel), який надає адміністраторам можливість відстежувати стан всіх внутрішніх номерів та дзвінків у реальному часі. Це дозволяє швидко реагувати на проблеми та забезпечувати високий рівень обслуговування.

Останнім, але не менш важливим компонентом успіху Elastix є його активна спільнота користувачів та розробників. Відкритий код та активна участь спільноти дозволяють швидко вирішувати проблеми, ділитися досвідом та розробляти нові функції. Спільнота надає підтримку через форуми, документацію та різноманітні ресурси, що допомагає новим користувачам швидко освоїти платформу та використовувати її на повну потужність. Загалом, архітектура та основні компоненти Elastix забезпечують потужну, гнучку та масштабовану платформу для впровадження VoIP та інших комунікаційних сервісів. Вона об'єднує численні інструменти в єдину інтегровану систему, що спрощує управління та підвищує ефективність комунікацій для організацій будь-якого розміру.

Elastix є однією з найбільш популярних платформ для впровадження корпоративних VoIP-мереж завдяки численним перевагам, які вона пропонує.

Однією з основних переваг використання Elastix для корпоративних мереж є її економічна ефективність. Оскільки Elastix базується на відкритому коді, організації можуть значно знизити витрати на придбання програмного забезпечення та ліцензій. Відсутність необхідності сплачувати ліцензійні збори дозволяє компаніям зосередити свої фінансові ресурси на інших аспектах бізнесу, таких як модернізація обладнання або навчання персоналу[13].

Гнучкість та масштабованість Elastix робить її ідеальним рішенням для підприємств будь-якого розміру. Платформа дозволяє легко налаштовувати та адаптувати систему відповідно до специфічних потреб організації. Це особливо важливо для компаній, які планують розширення або мають динамічні потреби в комунікаціях. Завдяки модульній архітектурі, користувачі можуть додавати нові функції та компоненти без необхідності суттєво змінювати основну систему. Це забезпечує безперервність роботи та можливість поступового розширення функціональності[4].

Інтеграція різних комунікаційних інструментів є ще однією важливою перевагою Elastix. Платформа поєднує в собі IP-телефонію, відеоконференції, електронну пошту, факс та інші сервіси, створюючи єдину інтегровану систему для управління комунікаціями. Це значно спрощує управління комунікаціями всередині компанії, оскільки всі інструменти знаходяться в одній системі. Наприклад, користувачі можуть легко відправляти факси через електронну пошту або проводити відеоконференції без необхідності використовувати окремі програми.

Elastix також забезпечує високий рівень безпеки для корпоративних мереж. Платформа включає кілька інструментів для захисту від атак та несанкціонованого доступу. Наприклад, fail2ban аналізує лог-файли та блокує підозрілі IP-адреси, запобігаючи потенційним загрозам. IPTables дозволяє налаштовувати правила фільтрації трафіку, що допомагає контролювати доступ до системи та захистити її від атак. Завдяки цим інструментам компанії можуть бути впевнені в захищеності своїх комунікаційних систем[3].

Простота використання є ще однією перевагою Elastix. Завдяки зручному веб-інтерфейсу FreePBX, адміністратори можуть легко налаштовувати та керувати системою без необхідності мати глибокі технічні знання. Це дозволяє значно знизити витрати на навчання персоналу та забезпечити ефективне управління системою. Інтерфейс FreePBX дозволяє користувачам додавати нові внутрішні номери, налаштовувати маршрути дзвінків, створювати голосові меню та виконувати багато інших завдань за кілька кліків[7].

Платформа також забезпечує високу якість зв'язку та надійність. Завдяки використанню сучасних технологій та протоколів, таких як SIP, Elastix може забезпечити чітке звучання голосу без затримок і перешкод. Це особливо важливо для корпоративних мереж, де якість зв'язку має вирішальне значення для ефективної роботи. Платформа також включає інструменти для моніторингу та аналізу якості зв'язку, що дозволяє адміністраторам швидко виявляти та усувати проблеми.

Моніторинг і аналітика є ще одним важливим аспектом, що робить Elastix привабливим вибором для корпоративних мереж. Інструменти для моніторингу в реальному часі, такі як Flash Operator Panel (FOP2), дозволяють адміністраторам відстежувати стан всіх внутрішніх номерів та дзвінків у реальному часі. Це забезпечує швидке реагування на проблеми та підтримку високого рівня обслуговування. Журнали викликів (CDR) дозволяють детально аналізувати використання ресурсів, визначати проблемні зони та оптимізувати роботу системи.

Активна спільнота користувачів та розробників є ще однією значною перевагою Elastix. Відкритий код та активна участь спільноти дозволяють швидко вирішувати проблеми, ділитися досвідом та розробляти нові функції. Спільнота надає підтримку через форуми, документацію та різноманітні ресурси, що допомагає новим користувачам швидко освоїти платформу та використовувати її на повну потужність. Це також забезпечує постійний розвиток платформи, додавання нових можливостей та вдосконалення існуючих функцій[3].

Висновки

У першому розділі було проведено огляд технологій VoIP (Voice over Internet Protocol), починаючи з базових принципів роботи та закінчуючи аналізом основних протоколів та стандартів, таких як SIP, RTP та H.323. Було розглянуто переваги VoIP, такі як зниження витрат, гнучкість, масштабованість та широкий спектр функцій, а також недоліки, такі як залежність від якості інтернет-з'єднання, вразливість до збоїв електроживлення та кіберзагроз. Було проведено порівняльний аналіз різних платформ для побудови VoIP-мереж, включаючи відкриті та комерційні рішення, з акцентом на переваги та недоліки кожного типу. Також було досліджено платформу Elastix, яка є відкритим рішенням на базі Asterisk, що пропонує широкий спектр функціональних можливостей та гнучкість налаштування. Зокрема платформа підтримує численні комунікаційні інструменти, такі як IP-телефонія, відеоконференції, електронна пошта, факс та інші сервіси, що дозволяє побудувати на її основі єдину систему корпоративних комунікацій. Окрім того, Elastix має нативні інструменти для моніторингу працездатності компонентів системи, забезпечення захисту доступу до системи та попередження атак.

РОЗДІЛ 2

РОЗРОБКА КОРПОРАТИВНОЇ VOIP-МЕРЕЖІ НА ОСНОВІ ELASTIX

2.1 Аналіз вимог та планування мережі

Визначення потреб користувачів є критично важливим етапом у процесі впровадження будь-якої нової системи, особливо такої складної, як корпоративна VoIP-мережа. Цей процес включає ретельний аналіз та розуміння вимог, очікувань та поведінки кінцевих користувачів, щоб створити систему, яка максимально відповідає їхнім потребам та забезпечує високу ефективність роботи.

Першим кроком у визначенні потреб користувачів є проведення всебічного аналізу існуючої комунікаційної інфраструктури. Це включає оцінку поточних засобів зв'язку, таких як телефонні системи, електронна пошта, факси, відеоконференції та інші інструменти, що використовуються в організації. Аналіз існуючої системи допоможе виявити слабкі місця, визначити, які функції використовуються найчастіше, і які з них потребують покращення або заміни[3].

Наступним важливим етапом є проведення опитувань та інтерв'ю з кінцевими користувачами. Це може включати як керівництво компанії, так і рядових співробітників, оскільки потреби і вимоги можуть значно відрізнятися залежно від рівня відповідальності та функціональних обов'язків. Опитування дозволяють зібрати інформацію про те, які саме функції та сервіси є найбільш важливими для різних груп користувачів, з якими проблемами вони стикаються у своїй щоденній роботі та які покращення вони хотіли б бачити у новій системі.

Крім опитувань, важливо також провести спостереження за робочими процесами користувачів. Спостереження допомагають зрозуміти, як саме користувачі взаємодіють з поточною системою, які інструменти вони використовують найчастіше, які завдання виконують і як нова система може допомогти їм виконувати ці завдання ефективніше. Спостереження можуть виявити невидимі на перший погляд проблеми, які можуть бути вирішені за допомогою нових функцій та покращень[2].

Аналіз потреб користувачів також включає оцінку майбутніх потреб організації. Це означає врахування планів щодо розширення бізнесу, зростання кількості співробітників, відкриття нових офісів або філій, а також можливих змін у бізнес-процесах. Прогнозування майбутніх потреб дозволяє створити систему, яка буде гнучкою і масштабованою, щоб підтримувати розвиток організації без необхідності у значних модернізаціях або замінах у найближчому майбутньому.

Важливим аспектом визначення потреб користувачів є також розуміння специфічних вимог до функціональності та безпеки системи. Це включає визначення необхідності в таких функціях, як голосова пошта, автоматизовані голосові меню (IVR), конференц-зв'язок, інтеграція з CRM-системами та іншими бізнес-додатками, а також вимоги до якості зв'язку (QoS) і безпеки даних. Залежно від галузі та типу бізнесу, вимоги до безпеки можуть варіюватися від базових рівнів захисту до високих стандартів безпеки, що включають шифрування дзвінків, багатофакторну аутентифікацію та захист від несанкціонованого доступу.

Після збору всієї необхідної інформації, наступним кроком є її аналіз та систематизація. Це включає групування потреб та вимог за категоріями, такими як функціональність, зручність використання, безпека, масштабованість та інші. Важливо також пріоритетизувати ці вимоги, щоб визначити, які з них є критичними для успіху системи, а які можуть бути впроваджені на наступних етапах розвитку.

На основі отриманих даних створюється детальне технічне завдання (ТЗ), яке включає опис всіх вимог та специфікацій до нової системи. ТЗ слугує керівництвом для розробників та впроваджувальних команд, забезпечуючи, що всі критичні потреби користувачів будуть враховані та реалізовані у фінальному продукті. Це документ також може використовуватися для оцінки вартості проекту, визначення необхідних ресурсів та планування графіку робіт[6].

Визначення потреб користувачів є безперервним процесом, який не завершується після впровадження системи. Після запуску нової системи важливо продовжувати збирати зворотний зв'язок від користувачів, проводити регулярні

опитування та спостереження за їх роботою, щоб виявляти нові потреби та проблеми. Це дозволяє постійно вдосконалювати систему, додаючи нові функції та покращення, що забезпечують високий рівень задоволеності користувачів та ефективність роботи організації.

Оцінка існуючої інфраструктури є важливим процесом, що включає детальний аналіз поточних технологічних засобів та ресурсів компанії. Це дозволяє визначити готовність до впровадження нової VoIP-системи та виявити необхідні зміни для забезпечення її успішної інтеграції. Оцінка починається з аналізу існуючих засобів зв'язку та комунікацій, таких як телефонні системи, електронна пошта, факси, відеоконференції та інші інструменти, які використовуються в компанії. Важливо розуміти, які функції та сервіси є критичними для бізнесу, і які з них потребують покращення або збереження в новій системі[8].

Інвентаризація наявного обладнання та програмного забезпечення є наступним кроком. Це включає оцінку серверів, маршрутизаторів, комутаторів, IP-телефонів, комп'ютерів та програмного забезпечення, які використовуються для управління комунікаціями. Важливо перевірити, чи відповідає це обладнання вимогам нової VoIP-системи, чи підтримує необхідні протоколи та стандарти, такі як SIP, та чи достатньо його для обслуговування всіх користувачів без збоїв і затримок.

Аналіз мережевої інфраструктури є ключовим етапом оцінки. Мережа повинна мати достатню пропускну здатність і стабільність для підтримки високоякісних голосових та відео викликів без затримок і втрат пакетів. Оцінка швидкості інтернет-з'єднання, внутрішньої пропускної здатності локальної мережі, можливостей забезпечення якості обслуговування (QoS) і захисту від перевантажень є важливими аспектами цього аналізу. Це включає тестування швидкості та стабільності з'єднання, перевірку налаштувань маршрутизаторів і комутаторів, а також аналіз трафіку для виявлення можливих проблем.

Безпека є ще одним важливим аспектом оцінки існуючої інфраструктури. Необхідно перевірити, наскільки поточна система захищена від

несанкціонованого доступу, атак на відмову в обслуговуванні (DoS) та інших кіберзагроз. Це включає аналіз наявних засобів захисту, таких як міжмережеві екрани, системи виявлення та запобігання вторгнень (IDS/IPS), шифрування даних, а також процедури резервного копіювання і відновлення. Якщо поточна інфраструктура не забезпечує необхідний рівень безпеки, потрібно врахувати необхідні зміни для посилення захисту[3].

Оцінка також включає аналіз організаційних та людських ресурсів. Важливо оцінити наявність кваліфікованого персоналу для управління та обслуговування нової системи, а також потребу в додатковому навчанні співробітників. Якщо компанія не має достатньо технічних спеціалістів, можливо, доведеться залучити зовнішніх експертів або провести навчальні курси для існуючих співробітників.

Після завершення оцінки всі зібрані дані систематизуються та аналізуються. Це включає створення детального звіту, який описує поточний стан інфраструктури, виявлені проблеми та обмеження, а також рекомендації щодо необхідних змін і модернізацій. Звіт включає опис поточного стану інфраструктури, виявлені проблеми та обмеження, а також рекомендації щодо необхідних змін і модернізацій[3].

Оцінка існуючої інфраструктури дозволяє визначити слабкі місця та обмеження поточної технологічної бази, що допомагає підготувати інфраструктуру до впровадження нової VoIP-системи. Це забезпечує безперебійне функціонування нової системи, яка відповідає потребам та вимогам організації.

Таблиця 2.1

Планування топології мережі для корпоративної VoIP-системи

Етапи планування	**Опис**
Аналіз існуючої інфраструктури	Проведення детального аналізу поточних засобів зв'язку, телефонних систем, електронної пошти, факсів, відеоконференцій, а також оцінка поточної мережевої топології, включаючи маршрутизатори, комутатори, сервери, IP-телефони та інше обладнання.
Визначення оптимальної структури мережі	Вибір зіркоподібної топології для кожного офісу, де всі кінцеві пристрої підключені до центрального комутатора. Використання VPN для міжофісних з'єднань, забезпечуючи безпечне і надійне з'єднання між різними офісами компанії.
Вибір обладнання та програмного забезпечення	Вибір центральних комутаторів з підтримкою QoS, виділених маршрутизаторів з підтримкою VPN, IP-телефонів з підтримкою SIP, і сервера для управління VoIP-зв'язком на базі Elastix.
Налаштування якості обслуговування (QoS)	Пріоритезація голосових пакетів даних на всіх комутаторах і маршрутизаторах для забезпечення стабільності і якості голосового трафіку. Налаштування мінімальних гарантованих пропускних здатностей для голосового трафіку.
Забезпечення безпеки	Шифрування VoIP-з'єднань через VPN для захисту від перехоплення і несанкціонованого доступу. Налаштування міжмережевих екранів на маршрутизаторах і комутаторах для захисту від потенційних загроз. Використання сучасних методів шифрування для сервера управління VoIP-зв'язком.
Тестування та оптимізація	Проведення детального тестування якості зв'язку, пропускної здатності мережі, затримок і стабільності з'єднань. Внесення необхідних коректив для оптимізації роботи системи.
Моніторинг і підтримка	Використання спеціалізованих інструментів для відстеження стану мережі в реальному часі, моніторингу трафіку, якості зв'язку і виявлення можливих проблем для забезпечення безперебійного функціонування системи.

2.2 Встановлення та налаштування Elastix

Починається все з вибору відповідного серверного обладнання, яке відповідає вимогам VoIP-системи. Важливо врахувати обчислювальну потужність, обсяг оперативної пам'яті, дисковий простір і пропускну здатність мережі. Сервери повинні бути досить потужними, щоб обробляти велику кількість одночасних викликів і забезпечувати високу якість зв'язку. Рекомендується використовувати сервери з багатоядерними процесорами, великою кількістю оперативної пам'яті (16 ГБ і більше) та швидкими жорсткими дисками або твердотільними накопичувачами[16].

Наступним кроком є встановлення операційної системи на сервер. Для VoIP-систем зазвичай використовуються операційні системи на базі Linux, такі як CentOS, Debian або Ubuntu. Вибір конкретної операційної системи залежить від вимог і рекомендацій використовуваного програмного забезпечення. Після встановлення операційної системи необхідно налаштувати базові параметри, включаючи мережеві налаштування, час і дату, користувачів та права доступу, а також встановити всі необхідні оновлення та патчі безпеки.

Після налаштування операційної системи потрібно встановити програмне забезпечення для VoIP-системи. Однією з популярних платформ є Elastix, яка об'єднує в собі можливості для управління голосовими викликами, відеоконференціями, електронною поштою і факсами. Встановлення Elastix включає завантаження та розпакування програмного забезпечення, встановлення залежностей і необхідних бібліотек, запуск інсталяційного скрипта і налаштування базових параметрів системи. Після успішної установки необхідно провести початкове налаштування системи, включаючи створення користувачів, налаштування внутрішніх номерів, маршрутизації викликів та інших основних параметрів.

Безпека системи є ще одним важливим аспектом підготовки серверного обладнання. Необхідно налаштувати міжмережевий екран (firewall) для захисту серверів від несанкціонованого доступу та атак. Це включає визначення і відкриття необхідних портів для VoIP-трафіку, а також блокування всіх

непотрібних портів і служб. Крім того, рекомендується використовувати системи виявлення та запобігання вторгнень (IDS/IPS) для додаткового захисту мережі. Важливо також налаштувати механізми шифрування даних, такі як TLS (Transport Layer Security), для захисту голосових викликів і забезпечення конфіденційності інформації[14].

Резервне копіювання є невід'ємною частиною підготовки серверного обладнання. Потрібно налаштувати регулярне резервне копіювання всіх критичних даних, включаючи конфігураційні файли, бази даних, журнали викликів та іншу важливу інформацію. Це дозволить швидко відновити систему в разі збою або втрати даних. Рекомендується зберігати резервні копії на окремому фізичному або хмарному сховищі для забезпечення додаткового захисту.

Після завершення всіх налаштувань потрібно провести детальне тестування серверного обладнання. Це включає тестування продуктивності серверів, перевірку якості зв'язку, пропускної здатності мережі та стабільності роботи системи під навантаженням. Важливо переконатися, що сервери можуть обробляти максимальну кількість одночасних викликів без втрати якості і збоїв. За результатами тестування можна внести необхідні корективи для оптимізації роботи системи.

Процес встановлення операційної системи та платформи Elastix є багатоступеневим і включає кілька важливих етапів, які забезпечують належну роботу системи та підготовку до впровадження VoIP-інфраструктури.

Таблиця 2.2

Процес встановлення операційної системи та платформи Elastix

Етапи	**Опис**
Підготовка до встановлення	Вибір відповідного дистрибутиву Linux (CentOS, Debian, Ubuntu). Завантаження останньої стабільної версії та створення завантажувального носія (USB-накопичувач або DVD).
Встановлення операційної системи	Підключення завантажувального носія до сервера, завантаження системи, вибір опції встановлення. Проходження через кроки встановлювача: вибір мови, налаштування розкладки клавіатури, вибір диска для встановлення та налаштування параметрів мережі.
Базове налаштування операційної системи	Створення користувачів та налаштування прав доступу, налаштування часу та дати. Встановлення останніх оновлень та патчів безпеки за допомогою пакетного менеджера (yum для CentOS або apt для Debian/Ubuntu).
Встановлення Elastix	Завантаження останньої версії Elastix з офіційного сайту. Розпакування архіву, запуск інсталяційного скрипта, встановлення залежностей та необхідних компонентів, включаючи веб-сервер, базу даних, Asterisk та інші модулі.
Початкове налаштування Elastix	Налаштування веб-інтерфейсу для управління системою. Створення облікових даних адміністратора, налаштування внутрішніх номерів, маршрутизації викликів, створення користувачів та груп, налаштування голосової пошти та інших функцій.
Забезпечення безпеки	Налаштування міжмережевого екрану (firewall) для захисту від несанкціонованого доступу та атак. Відкриття необхідних портів для VoIP-трафіку, блокування непотрібних портів і служб. Налаштування систем виявлення та запобігання вторгнень (IDS/IPS). Налаштування шифрування даних з використанням TLS для захисту голосових викликів.
Налаштування резервного копіювання	Налаштування регулярного резервного копіювання всіх критичних даних, включаючи конфігураційні файли, бази даних, журнали викликів та іншу важливу інформацію. Зберігання резервних копій на окремому фізичному або хмарному сховищі для додаткового захисту.
Тестування системи	Перевірка продуктивності серверів, якості зв'язку, пропускної здатності мережі та стабільності роботи системи під навантаженням. Переконання у здатності системи обробляти максимальну кількість одночасних викликів без втрати якості та збоїв. Внесення коректив для оптимізації роботи системи за результатами тестування.

Базові налаштування та конфігурація VoIP-системи на базі платформи Elastix включають кілька важливих кроків, які потрібно виконати послідовно, щоб забезпечити стабільну та ефективну роботу системи.

Таблиця 2.3

Базові налаштування та конфігурація VoIP-системи на базі Elastix

Етапи налаштування	**Опис**
Налаштування мережевих параметрів	Встановлення статичної IP-адреси, маски підмережі, шлюзу та DNS-серверів. Перезавантаження мережевого інтерфейсу для застосування змін.
Створення облікових записів користувачів	Веб-інтерфейс Elastix: створення облікових записів, додавання внутрішніх номерів, налаштування прав доступу та голосової пошти для кожного користувача.
Налаштування маршрутизації викликів	Визначення правил маршрутизації для внутрішніх і зовнішніх викликів, налаштування транків та маршрутів для вихідних дзвінків, налаштування вхідних маршрутів для направлення дзвінків до відповідних відділів або співробітників.
Налаштування автоматизованих голосових меню (IVR)	Створення IVR-меню, налаштування привітання та варіантів вибору для користувачів, спрямування дзвінків до відповідних відділів або осіб на основі вибору користувача.
Забезпечення безпеки	Налаштування міжмережевого екрану (firewall) для захисту від несанкціонованого доступу та атак, відкриття необхідних портів для VoIP-трафіку, закриття всіх непотрібних портів та служб, налаштування систем виявлення та запобігання вторгнень (IDS/IPS), налаштування шифрування даних за допомогою TLS для захисту голосових викликів.
Налаштування якості обслуговування (QoS)	Перевірка підтримки QoS маршрутизаторами та комутаторами, налаштування пріоритетів для голосового трафіку через веб-інтерфейс мережевого обладнання, встановлення пріоритету для SIP-трафіку (порт 5060) та RTP-трафіку (порти 10000-20000).
Налаштування резервного копіювання	Налаштування регулярного резервного копіювання всіх критичних даних, створення скрипта резервного копіювання для архівування конфігураційних файлів, баз даних, журналів викликів, налаштування cron-джоба для регулярного виконання скрипта, зберігання резервних копій на окремому фізичному або хмарному сховищі для додаткового захисту.
Тестування системи	Перевірка якості зв'язку, здійснення тестових дзвінків між внутрішніми номерами, перевірка маршрутизації викликів для зовнішніх дзвінків, перевірка роботи IVR-меню шляхом здійснення тестових дзвінків і перевірки опцій, перевірка роботи резервного копіювання шляхом відновлення даних з резервної копії на тестовому сервері.

2.3 Інтеграція та налаштування VoIP-обладнання

Підключення та налаштування IP-телефонів є важливим етапом у впровадженні VoIP-системи, оскільки саме ці пристрої забезпечують основну функцію голосового зв'язку. Процес включає кілька кроків, які допоможуть забезпечити належне функціонування телефонів у мережі компанії та їх інтеграцію з системою Elastix. Належна настройка IP-телефонів забезпечить високу якість зв'язку, стабільність та зручність користування.

Першим етапом є підготовка мережевої інфраструктури для підключення IP-телефонів. Для цього необхідно переконатися, що мережа має достатню пропускну здатність та якість обслуговування (QoS) для підтримки голосового трафіку. Це включає налаштування комутаторів та маршрутизаторів для пріоритизації VoIP-трафіку над іншими видами трафіку. Комутатори повинні підтримувати Power over Ethernet (PoE), якщо IP-телефони отримують живлення через мережу. Це дозволить забезпечити живлення телефонів без додаткових блоків живлення, спрощуючи встановлення та знижуючи кількість необхідних кабелів.

Наступним кроком є фізичне підключення IP-телефонів до мережі. Це включає підключення телефонів до комутаторів або маршрутизаторів за допомогою Ethernet-кабелів. Якщо комутатори підтримують PoE, телефони автоматично отримають живлення через кабелі. Після підключення телефонів до мережі вони мають автоматично отримати IP-адреси від DHCP-сервера. Для цього необхідно переконатися, що DHCP-сервер налаштований правильно та має достатню кількість доступних IP-адрес[17].

Після фізичного підключення та отримання IP-адреси необхідно налаштувати самі IP-телефони. Для цього слід увійти в веб-інтерфейс кожного телефону, використовуючи його IP-адресу. Це можна зробити, відкривши веб-браузер і ввівши IP-адресу телефону в адресний рядок. Зазвичай, веб-інтерфейс вимагає введення облікових даних адміністратора. Якщо ці дані не були змінені, вони можуть бути за замовчуванням, що вказано в документації до телефону.

Після входу в веб-інтерфейс IP-телефону слід налаштувати основні параметри для підключення до VoIP-системи Elastix. Це включає введення внутрішнього номера, пароля та адреси SIP-сервера. Внутрішній номер та пароль зазвичай створюються в системі Elastix під час налаштування користувачів та розширень. Адреса SIP-сервера – це IP-адреса або доменне ім'я сервера Elastix, який обробляє дзвінки. Крім того, слід налаштувати інші параметри, такі як кодеки для стиснення голосу, які використовуватимуться телефоном. Рекомендується використовувати кодеки з високою якістю звуку, такі як G.711 або G.722.

Після налаштування основних параметрів необхідно зберегти зміни та перезавантажити IP-телефон. Після перезавантаження телефон повинен підключитися до SIP-сервера та бути готовим до використання. Для перевірки правильності налаштувань можна здійснити тестовий дзвінок на інший внутрішній номер або зовнішній номер. Якщо дзвінок успішний, значить телефон налаштований правильно[7].

Окрім базових налаштувань, можуть знадобитися додаткові налаштування для забезпечення оптимальної роботи IP-телефонів у мережі. Це включає налаштування функцій безпеки, таких як шифрування SIP-трафіку за допомогою TLS або SRTP. Це забезпечить захист голосових даних від несанкціонованого доступу та прослуховування. Також може бути корисно налаштувати функції якості обслуговування (QoS) на самому IP-телефоні, якщо це підтримується, для додаткової пріоритизації голосового трафіку.

Інший важливий аспект налаштування IP-телефонів – це оновлення програмного забезпечення (прошивки) телефонів. Виробники регулярно випускають оновлення, які покращують функціональність та безпеку пристроїв. Перед початком налаштування рекомендується перевірити наявність оновлень та встановити їх на телефони. Це забезпечить максимальну сумісність із сучасними VoIP-сервісами та захист від відомих вразливостей.

Налаштування шлюзів та адаптерів є важливим кроком у впровадженні корпоративної VoIP-системи, адже ці пристрої інтегрують традиційні телефонні

лінії з IP-мережею, дозволяючи здійснювати та приймати дзвінки через інтернет. Процес складається з декількох ключових етапів, які забезпечують коректну роботу та інтеграцію з системою Elastix.

Спочатку потрібно підготувати мережеву інфраструктуру для підключення шлюзів та адаптерів. Важливо переконатися, що мережа має достатню пропускну здатність для обробки голосового трафіку і підтримує пріоритизацію VoIP-трафіку. Також слід перевірити наявність вільних портів на маршрутизаторах і комутаторах, які будуть використовуватися для підключення пристроїв.

Наступним кроком є фізичне підключення шлюзів та адаптерів до мережі. Це здійснюється за допомогою Ethernet-кабелів, що з'єднують пристрої з комутаторами або маршрутизаторами. Після підключення шлюзи та адаптери повинні автоматично отримати IP-адреси від DHCP-сервера. У разі необхідності статичних IP-адрес їх можна налаштувати вручну через веб-інтерфейс або консоль управління пристроєм.

Далі потрібно налаштувати основні параметри шлюзів та адаптерів. Для цього слід увійти в веб-інтерфейс кожного пристрою, використовуючи його IP-адресу. У веб-інтерфейсі вводяться облікові дані адміністратора, якщо вони не були змінені, зазвичай вони знаходяться у документації до пристрою. Після входу потрібно налаштувати SIP-акаунти, кодеки та правила маршрутизації викликів. Це включає введення внутрішніх номерів, паролів та адреси SIP-сервера, а також вибір кодеків для стиснення голосу, таких як G.711 або G.722, та налаштування правил для обробки вхідних і вихідних дзвінків.

Щоб забезпечити безпеку системи, налаштовують міжмережевий екран (firewall) на шлюзах та адаптерах. Це включає відкриття тільки необхідних портів для VoIP-трафіку та закриття всіх інших, щоб захистити систему від несанкціонованого доступу та атак. Важливо також налаштувати шифрування SIP-трафіку за допомогою TLS або SRTP для забезпечення конфіденційності голосових даних[4].

Після налаштування основних параметрів і безпеки необхідно зберегти зміни та перезавантажити пристрої. Після перезавантаження шлюзи та адаптери

повинні підключитися до SIP-сервера та бути готовими до обробки дзвінків. Для перевірки правильності налаштувань можна здійснити кілька тестових дзвінків, як внутрішніх, так і зовнішніх, щоб переконатися, що пристрої працюють належним чином.

Крім базових налаштувань, можуть бути потрібні додаткові налаштування для оптимізації роботи шлюзів та адаптерів у мережі. Це включає налаштування функцій QoS на пристроях для пріоритизації голосового трафіку та оновлення прошивки до останньої версії для забезпечення максимальної сумісності та безпеки. Регулярне оновлення програмного забезпечення допомагає уникнути вразливостей і забезпечує покращену функціональність пристроїв[14].

Тестування та усунення проблем є невід'ємними етапами впровадження VoIP-системи, адже саме вони забезпечують її стабільну і надійну роботу. Першим кроком у цьому процесі є перевірка фізичних підключень. Слід ретельно оглянути всі кабелі, живлення та мережеві з'єднання для IP-телефонів, шлюзів, адаптерів та іншого обладнання, щоб переконатися у правильності їх підключення та функціональності. У разі використання PoE (Power over Ethernet), перевіряється, чи отримують пристрої необхідне живлення через мережу.

Перевірка мережевої інфраструктури є наступним важливим етапом. Це включає тестування пропускної здатності мережі, затримок, втрат пакетів та інших параметрів, які можуть впливати на якість зв'язку. Інструменти типу iPerf або PingPlotter допомагають провести детальний аналіз мережевих з'єднань. Важливо переконатися, що мережа має достатню пропускну здатність для обробки голосового трафіку і що затримки та втрати пакетів не перевищують допустимих меж.

Далі слід перейти до тестування якості зв'язку. Здійснюються тестові дзвінки між внутрішніми номерами, а також на зовнішні номери. Під час тестових дзвінків слід оцінити якість звуку, затримки, ехо та інші параметри. Для цього використовуються внутрішні інструменти моніторингу системи Elastix або спеціалізоване програмне забезпечення для аналізу VoIP-трафіку. Якщо

виявляються проблеми з якістю звуку, необхідно переглянути налаштування кодеків, QoS та інших параметрів[14].

Особливу увагу слід приділити тестуванню функціональних можливостей системи, таких як автоматизовані голосові меню (IVR), голосова пошта, переадресація дзвінків, конференц-зв'язок та інші. Важливо переконатися, що всі налаштування та сценарії використання працюють коректно і відповідають вимогам. Наприклад, для перевірки IVR необхідно здійснити тестові дзвінки і вибрати різні опції, щоб переконатися, що всі дзвінки спрямовуються до правильних відділів або співробітників.

Налаштування безпеки є критично важливим аспектом. Це включає перевірку міжмережевих екранів (firewalls), систем виявлення та запобігання вторгнень (IDS/IPS), а також налаштування шифрування SIP-трафіку за допомогою TLS або SRTP. Використовуючи інструменти для перевірки безпеки мережі, такі як Nmap або Nessus, можна виявити вразливості та потенційні загрози. Забезпечення належного рівня безпеки допоможе захистити систему від несанкціонованого доступу та атак.

У разі виявлення проблем, необхідно провести їх усунення. Це може включати перевірку та коригування налаштувань мережі, заміну несправного обладнання, оновлення програмного забезпечення або прошивки пристроїв, а також налаштування додаткових параметрів для покращення якості зв'язку та безпеки. Важливо мати системний підхід до усунення проблем, документуючи кожен крок та зміни для забезпечення стабільної роботи системи в майбутньому[3].

Журнали подій та звіти про помилки є цінними інструментами для діагностики та усунення проблем. Система Elastix і більшість VoIP-пристроїв мають вбудовані можливості для запису журналів, які допомагають виявляти причини проблем і визначати шляхи їх вирішення. Аналіз цих журналів дозволяє отримати інформацію про можливі помилки та неправильно налаштовані параметри.

Після усунення всіх виявлених проблем необхідно провести повторне тестування системи. Це включає перевірку фізичних підключень, мережевої інфраструктури, якості зв'язку, функцій системи та налаштувань безпеки. Повторне тестування допомагає переконатися, що всі проблеми вирішені і система працює стабільно. Регулярне тестування та моніторинг системи дозволяють вчасно виявляти та усувати проблеми, забезпечуючи високу якість зв'язку та задоволеність користувачів[2].

Важливим аспектом є навчання користувачів та технічного персоналу. Користувачі повинні знати, як користуватися системою та її функціями, а також як повідомляти про проблеми. Технічний персонал має володіти необхідними знаннями та навичками для ефективного усунення проблем та підтримки стабільної роботи системи. Проведення регулярних навчальних сесій та тренінгів, а також створення документації та інструкцій з використання системи, допомагають забезпечити належний рівень підготовки персоналу.

Висновки

У другому розділі було детально розглянуто процес розробки корпоративної VoIP-мережі на основі платформи Elastix. Було досліджено вимоги, необхідні для визначення оптимальної структури та впровадження корпоративної мережі, що задовольнить існуючі потреби та окрім того забезпечить належний рівень безпеки. Зокрема аналіз існуючої інфраструктури для виявлення слабких місць та спостереження за робочими процесами користувачів.

Було описано процес встановлення та налаштування платформи Elastix, включаючи налаштування мережевих параметрів, створення облікових записів користувачів, маршрутизацію викликів, налаштування голосової пошти та інших важливих функцій. Особливу увагу було приділено інтеграції VoIP-обладнання, такого як IP-телефони, шлюзи та адаптери, з платформою Elastix, включаючи налаштування SIP-акаунтів, кодеки та правила маршрутизації.

У цьому розділі розглянуто глобальний процес аналізу, розробки та практичного впровадження корпоративної VoIP-мережі на базі Elastix, враховуючи потреби та особливості конкретної організації.

РОЗДІЛ 3

ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ТА БЕЗПЕКИ В VOIP-МЕРЕЖІ

3.1 Забезпечення якості зв'язку (QoS)

Механізми QoS (Quality of Service) у VoIP-мережах є критично важливими для забезпечення високої якості голосового зв'язку, оскільки вони допомагають управляти та пріоритизувати трафік, мінімізуючи затримки, втрати пакетів і варіації затримок (джиттер). У VoIP-мережах голосовий трафік має бути оброблений швидко і з мінімальними затримками, щоб забезпечити чітке і безперебійне звучання. Ось кілька основних механізмів QoS, що використовуються у VoIP-мережах[14].

Одним із найважливіших механізмів є класифікація та маркування трафіку. Це процес, за допомогою якого мережеві пристрої ідентифікують та маркують пакети даних відповідно до їх пріоритету. Для VoIP-мереж це означає, що голосовий трафік отримає вищий пріоритет порівняно з іншими типами трафіку, такими як веб-серфінг або передача файлів. Одним із методів маркування є використання поля DSCP (Differentiated Services Code Point) у заголовку IP-пакета. Це поле дозволяє призначати різні рівні пріоритету для різних типів трафіку.

Далі йде механізм чергування, який забезпечує пріоритезацію обробки пакетів на мережевих пристроях. Існують різні методи чергування, такі як PQ (Priority Queuing), WFQ (Weighted Fair Queuing) і CBWFQ (Class-Based Weighted Fair Queuing). PQ використовує кілька черг з різними рівнями пріоритету і обробляє пакети з найвищим пріоритетом першими. WFQ розподіляє пропускну здатність між всіма чергами на основі вагових коефіцієнтів, що дозволяє надавати більше ресурсів для пріоритетного трафіку. CBWFQ дозволяє створювати класи трафіку і призначати їм різні вагові коефіцієнти, що забезпечує гнучке управління трафіком.

Управління чергами також включає механізми уникнення заторів, такі як WRED (Weighted Random Early Detection). WRED дозволяє уникати заторів, виявляючи переповнені черги і випадковим чином відкидаючи деякі пакети ще до

того, як черга буде повністю заповнена. Це допомагає запобігти повному переповненню черг і зменшити затримки та втрати пакетів[17].

Механізм управління пропускною здатністю (policing and shaping) є ще одним важливим компонентом QoS. Управління пропускною здатністю дозволяє контролювати максимальну швидкість передачі трафіку на певних інтерфейсах або у певних класах трафіку. Policing здійснює негайне відкидання або маркування пакетів, які перевищують встановлені ліміти швидкості. Shaping, на відміну від policing, не відкидає пакети, а затримує їх, щоб передати їх у відповідності з встановленими лімітами. Це дозволяє вирівнювати трафік і зменшити ризик заторів.

Транспортування трафіку з високим пріоритетом також вимагає механізмів забезпечення якості обслуговування на кінцевих пристроях, таких як IP-телефони і шлюзи. Це може включати налаштування буферизації для зменшення джиттера та налаштування алгоритмів стиснення голосу (кодеків) для оптимального використання пропускної здатності мережі.

Механізм RSVP (Resource Reservation Protocol) також може використовуватися для забезпечення QoS у VoIP-мережах. RSVP дозволяє додаткам резервувати необхідні ресурси в мережі для певних сеансів передачі даних. Це забезпечує виділення достатньої пропускної здатності для голосового трафіку і гарантує необхідний рівень якості обслуговування для кожного дзвінка[3].

Процес налаштування QoS починається з класифікації та маркування трафіку. Цей етап включає визначення різних типів трафіку, таких як голосовий, відео, дані, і призначення кожному типу відповідного пріоритету. Для цього використовуються поля DSCP (Differentiated Services Code Point) або CoS (Class of Service) у заголовках IP-пакетів. Маркування пакетів дозволяє мережевому обладнанню розрізняти трафік і застосовувати відповідні політики QoS до кожного типу трафіку.

Далі слід налаштувати чергування на маршрутизаторах і комутаторах. Чергування визначає, як пакети обробляються, коли вони надходять на мережеві

пристрої. Популярні методи чергування включають PQ (Priority Queuing), WFQ (Weighted Fair Queuing) та CBWFQ (Class-Based Weighted Fair Queuing). PQ дозволяє обробляти пакети з найвищим пріоритетом першими, забезпечуючи мінімальні затримки для голосового трафіку. WFQ розподіляє пропускну здатність між всіма чергами на основі вагових коефіцієнтів, дозволяючи надавати більше ресурсів для пріоритетного трафіку. CBWFQ дозволяє створювати класи трафіку і призначати їм різні вагові коефіцієнти, що забезпечує гнучке управління трафіком.

Ще одним важливим аспектом налаштування QoS є управління пропускною здатністю, або поліціювання та шейпінг. Поліціювання контролює максимальну швидкість передачі трафіку на певних інтерфейсах або у певних класах трафіку, відкидаючи або маркуючи пакети, які перевищують встановлені ліміти. Шейпінг, на відміну від поліціювання, затримує пакети, щоб передати їх у відповідності з встановленими лімітами, вирівнюючи трафік і зменшуючи ризик заторів[3].

Налаштування QoS на кінцевих пристроях, таких як IP-телефони і шлюзи, також є важливим елементом. Це включає налаштування буферизації для зменшення джиттера та вибір оптимальних кодеків для стиснення голосу, що дозволяє максимально ефективно використовувати пропускну здатність мережі. Підтримка QoS на кінцевих пристроях забезпечує послідовну і високу якість зв'язку на всіх етапах передачі голосового трафіку[4].

Моніторинг та управління якістю зв'язку є важливими компонентами забезпечення стабільної роботи VoIP-мереж. Ці процеси допомагають виявляти та усувати проблеми, підтримувати високу якість зв'язку та забезпечувати задоволення користувачів. Моніторинг дозволяє відстежувати стан мережі в режимі реального часу, аналізувати різні параметри, такі як затримки, втрати пакетів, джиттер, а також завантаженість мережевих пристроїв. Управління якістю зв'язку включає налаштування та коригування мережевих параметрів для оптимізації роботи мережі.

Моніторинг починається з використання інструментів для збору та аналізу даних про трафік у мережі. Одним з таких інструментів є NetFlow, який надає детальну інформацію про потоки трафіку, дозволяючи ідентифікувати джерела та

отримувачі даних, типи трафіку та обсяги переданих даних. Інший інструмент, sFlow, забезпечує вибірковий збір даних про пакети, що дозволяє отримати загальну картину завантаженості мережі та виявити потенційні проблеми[8].

Для моніторингу якості зв'язку використовуються спеціалізовані інструменти, такі як VoIPmonitor, SolarWinds VoIP & Network Quality Manager або PRTG Network Monitor. Ці інструменти надають інформацію про якість голосових викликів, включаючи показники затримки, джиттера, втрат пакетів і оцінки MOS (Mean Opinion Score). Вони також дозволяють аналізувати дані в режимі реального часу та створювати звіти для подальшого аналізу.

Управління якістю зв'язку включає налаштування мережевих пристроїв, таких як маршрутизатори, комутатори та шлюзи, для забезпечення оптимальної роботи VoIP-трафіку. Це може включати налаштування QoS (Quality of Service) для пріоритезації голосового трафіку над іншими видами трафіку. Використання політик QoS дозволяє забезпечити мінімальні затримки та втрати пакетів для голосових викликів, що є критично важливим для підтримки високої якості зв'язку.

Одним з ключових аспектів управління якістю зв'язку є налаштування чергування на мережевих пристроях. Чергування визначає, як пакети обробляються, коли вони надходять на маршрутизатори та комутатори. Існують різні методи чергування, такі як PQ (Priority Queuing), WFQ (Weighted Fair Queuing) та CBWFQ (Class-Based Weighted Fair Queuing). Вибір відповідного методу чергування залежить від вимог мережі та типів трафіку[3].

Регулярне тестування мережі є невід'ємною частиною процесу моніторингу та управління якістю зв'язку. Це включає проведення тестових дзвінків для оцінки якості зв'язку, перевірку налаштувань QoS, аналіз показників затримки, джиттера та втрат пакетів. Тестування дозволяє виявити проблеми на ранніх стадіях і вжити заходів для їх усунення.

Важливим аспектом є автоматизація процесів моніторингу та управління якістю зв'язку. Використання автоматизованих систем дозволяє зменшити час реакції на проблеми, підвищити ефективність управління та забезпечити

постійний контроль за станом мережі. Автоматизовані системи можуть самостійно виявляти аномалії, генерувати сповіщення та пропонувати рекомендації щодо оптимізації роботи мережі.

Документування та аналіз результатів моніторингу є важливими для покращення якості зв'язку. Ведення журналів подій, створення звітів та аналіз даних дозволяють виявляти тренди, прогнозувати можливі проблеми та планувати необхідні зміни в інфраструктурі. Це допомагає підтримувати високу якість зв'язку в довгостроковій перспективі[7].

3.2 Безпека в VoIP-мережах

VoIP-технології, як і будь-які інші мережеві технології, піддаються різним видам атак, що можуть призвести до порушення конфіденційності, цілісності та доступності даних. Ось декілька основних загроз і вразливостей, характерних для VoIP-мереж.

Першою важливою загрозою є перехоплення голосового трафіку, відоме як прослуховування (eavesdropping). Це відбувається, коли зловмисник перехоплює голосові пакети, які передаються через мережу, і відновлює з них голосові розмови. Така атака може бути здійснена через недостатній захист трафіку, наприклад, відсутність шифрування. Перехоплення голосових розмов може призвести до витоку конфіденційної інформації, що є особливо критичним для бізнесу[13].

Іншою значною загрозою є атаки на відмову в обслуговуванні (DoS). Ці атаки спрямовані на перевантаження VoIP-сервера або мережевої інфраструктури великим обсягом трафіку, що призводить до неможливості обслуговування законних користувачів. Атаки DoS можуть викликати значні збої в роботі VoIP-мережі, роблячи її недоступною для здійснення та прийому дзвінків.

Підміна (spoofing) є ще однією серйозною загрозою для VoIP-мереж. Зловмисники можуть підробити ідентифікатори виклику (caller ID), роблячи так, щоб виклик здавався здійсненим з іншого джерела. Це може бути використано для

обману користувачів, здійснення шахрайських дзвінків або отримання несанкціонованого доступу до системи.

Сигнальні атаки, такі як SIP-флудинг, також представляють серйозну загрозу. Вони полягають у надсиланні великої кількості SIP-повідомлень до VoIP-сервера з метою його перевантаження та виведення з ладу. Такі атаки можуть призвести до збоїв у роботі сервера, втрати дзвінків і деградації якості обслуговування[14].

Вразливості в програмному забезпеченні VoIP-систем можуть бути використані зловмисниками для здійснення атак. Недоліки у коді, такі як буферні переповнення або ін’єкції SQL, можуть дозволити зловмисникам виконати довільний код на VoIP-сервері або отримати доступ до конфіденційних даних. Відсутність регулярних оновлень і патчів для VoIP-систем робить їх вразливими до експлуатації відомих уразливостей.

Фішинг є ще однією загрозою, яка може бути спрямована на користувачів VoIP-систем. Зловмисники можуть використовувати VoIP для здійснення фішингових дзвінків, намагаючись обманом отримати конфіденційну інформацію, таку як паролі або фінансові дані. Це особливо небезпечно, оскільки користувачі можуть бути менш настороженими при отриманні дзвінків, ніж при отриманні електронних листів.

Недостатній захист облікових записів та автентифікації також є важливою вразливістю. Використання слабких або передбачуваних паролів, відсутність двофакторної автентифікації та недостатній контроль доступу можуть дозволити зловмисникам отримати несанкціонований доступ до VoIP-систем. Це може призвести до викрадення облікових даних, здійснення шахрайських дзвінків або отримання доступу до конфіденційної інформації[12].

Незахищені налаштування VoIP-обладнання також можуть створювати вразливості. За замовчуванням багато пристроїв можуть мати ввімкнені небезпечні протоколи або служби, які не використовуються, але можуть бути експлуатовані зловмисниками. Відсутність належного налаштування

міжмережевих екранів (firewalls) і систем виявлення та запобігання вторгнень (IDS/IPS) також може зробити VoIP-мережу вразливою до атак.

Важливо також враховувати соціальні інженерні атаки, спрямовані на користувачів VoIP-систем. Зловмисники можуть використовувати методи соціальної інженерії для обману користувачів і отримання від них конфіденційної інформації або переконання їх виконати дії, які можуть скомпрометувати безпеку системи.

Існує кілька ключових методів, які використовуються для захисту VoIP-трафіку та шифрування голосових даних.

Одним із основних методів захисту є використання шифрування трафіку. Шифрування допомагає захистити голосові дані від перехоплення та прослуховування зловмисниками. Один з найбільш поширених протоколів для шифрування VoIP-трафіку є Secure Real-time Transport Protocol (SRTP). SRTP забезпечує шифрування голосових пакетів, а також забезпечує автентифікацію і цілісність даних, що передаються, шляхом додавання до кожного пакета криптографічного підпису. Це значно ускладнює перехоплення і модифікацію голосового трафіку[16].

Ще одним важливим методом є використання Transport Layer Security (TLS) для захисту сигналізації VoIP. Протокол TLS забезпечує шифрування сигнальних повідомлень SIP (Session Initiation Protocol), які використовуються для встановлення, управління та завершення дзвінків. Шифрування сигнальних повідомлень запобігає перехопленню та підробці повідомлень, забезпечуючи захист від атак типу "людина посередині" (MITM) і підміни.

Аутентифікація користувачів є ще одним важливим аспектом захисту VoIP-мереж. Використання сильних паролів і двофакторної аутентифікації (2FA) допомагає запобігти несанкціонованому доступу до VoIP-систем. Двофакторна аутентифікація вимагає від користувача надання двох різних типів доказів своєї особи, таких як пароль та одноразовий код, який надсилається на мобільний пристрій користувача. Це значно підвищує рівень безпеки, знижуючи ризик компрометації облікових записів[17].

Налаштування міжмережевих екранів (firewalls) є необхідним для захисту VoIP-мережі від несанкціонованого доступу та атак. Firewalls дозволяють контролювати і фільтрувати вхідний та вихідний трафік, блокуючи небезпечні з'єднання та дозволяючи тільки легітимний трафік. Налаштування правил фільтрації для SIP і RTP (Real-time Transport Protocol) трафіку допомагає захистити VoIP-систему від зловмисних атак і забезпечити безперебійну роботу.

Використання систем виявлення та запобігання вторгнень (IDS/IPS) також є важливим компонентом захисту VoIP-мереж. IDS/IPS системи аналізують трафік у реальному часі, виявляючи підозрілу активність і атаки, такі як DoS (Denial of Service) або brute force атаки. Ці системи можуть автоматично вживати заходів для блокування атак і захисту VoIP-інфраструктури.

Регулярне оновлення програмного забезпечення та прошивок VoIP-пристроїв є критично важливим для захисту від відомих вразливостей. Виробники регулярно випускають оновлення, що включають патчі для виправлення виявлених вразливостей і покращення безпеки. Забезпечення своєчасного оновлення програмного забезпечення допомагає захистити VoIP-систему від експлуатації відомих вразливостей[14].

Сегментація мережі є ефективним методом захисту VoIP-інфраструктури. Сегментація передбачає розподіл мережі на окремі сегменти з різними рівнями доступу і безпеки. Наприклад, можна створити окремі VLAN для голосового трафіку, даних і управління. Це допомагає ізолювати голосовий трафік від інших видів трафіку і знижує ризик компрометації мережі.

Використання VPN (Virtual Private Network) для захисту віддалених з'єднань є ще одним важливим методом. VPN забезпечує шифрування трафіку між віддаленими користувачами та VoIP-системою, захищаючи дані від перехоплення в незахищених мережах, таких як публічні Wi-Fi. VPN також забезпечує автентифікацію користувачів, забезпечуючи додатковий рівень безпеки.

Нарешті, навчання користувачів є критичним аспектом захисту VoIP-мереж. Користувачі повинні бути обізнані про основні правила безпеки, такі як створення сильних паролів, розпізнавання фішингових атак та важливість регулярного

оновлення програмного забезпечення. Навчання допомагає знизити ризик соціальних інженерних атак і підвищує загальну безпеку VoIP-системи[3].

3.3 Резервування та відновлення системи

Стратегії резервного копіювання є важливою складовою управління IT-інфраструктурою, оскільки вони забезпечують захист даних від втрати внаслідок збоїв системи, атак, природних катастроф або людських помилок. У VoIP-системах, таких як платформа Elastix, резервне копіювання особливо критичне, адже втрати конфігураційних файлів, даних викликів або облікових записів можуть серйозно порушити роботу всієї системи. Розглянемо основні стратегії резервного копіювання, які можна використовувати для захисту даних на платформі Elastix.

Однією з найпоширеніших стратегій резервного копіювання є повне резервне копіювання (full backup). Це тип резервного копіювання, при якому копіюються всі дані та файли системи на певний носій або в хмарне сховище. Перевагою цього методу є те, що відновлення з повного резервного копіювання зазвичай найшвидше і найпростіше, оскільки всі дані зібрані в одному місці. Однак, цей метод є досить ресурсоємним, оскільки потребує багато часу і місця для зберігання[14].

Інкрементне резервне копіювання (incremental backup) є ще однією ефективною стратегією. Після створення початкового повного резервного копіювання, інкрементне резервне копіювання зберігає лише ті файли, які були змінені або додані з моменту останнього резервного копіювання (будь то повне або інкрементне). Це значно економить час і місце для зберігання, оскільки кожне інкрементне резервне копіювання містить лише зміни. Однак, відновлення даних може бути складнішим і тривалішим процесом, оскільки потрібно буде відновити початкове повне резервне копіювання, а потім застосувати всі інкрементні резервні копії.

Диференційне резервне копіювання (differential backup) схоже на інкрементне, але з однією ключовою різницею. Після початкового повного

резервного копіювання диференційне зберігає всі зміни, що сталися з моменту останнього повного резервного копіювання. Це означає, що диференційне резервне копіювання буде більшим за інкрементне, але відновлення даних буде простішим і швидшим, оскільки потрібно буде відновити лише початкове повне резервне копіювання і останню диференційну копію[2].

Важливою стратегією є регулярне резервне копіювання конфігураційних файлів. У системах на кшталт Elastix це може включати файли конфігурації Asterisk, налаштування користувачів, дані про виклики та інші важливі параметри. Ці файли зазвичай змінюються рідше, ніж інші дані, тому регулярне резервне копіювання (наприклад, щотижня) може бути достатнім для забезпечення їх захисту.

Окрім регулярного резервного копіювання, важливо передбачити стратегію архівування даних. Архівування включає довгострокове зберігання старих даних, які більше не потрібні для щоденної роботи, але можуть бути необхідні для звітності або аудиту. Архівні дані можуть зберігатися на менш дорогих носіях або в хмарних архівах для економії місця і ресурсів.

Забезпечення географічного розподілу резервних копій є ще однією важливою стратегією. Це передбачає зберігання резервних копій у різних фізичних місцях для захисту від локальних катастроф, таких як пожежі або повені. Географічно розподілені резервні копії можуть бути зберігані в різних дата-центрах або в хмарних сховищах різних провайдерів.

Регулярне тестування резервних копій є критично важливим для забезпечення їх надійності. Це включає проведення регулярних тестових відновлень даних, щоб переконатися, що резервні копії є повними і їх можна відновити без проблем. Регулярне тестування допомагає виявити будь-які потенційні проблеми до того, як вони стануть критичними[1].

Автоматизація процесів резервного копіювання допомагає забезпечити їх регулярність і зменшує ймовірність людської помилки. Використання спеціалізованого програмного забезпечення для автоматизації резервного

копіювання дозволяє налаштувати графіки резервного копіювання, моніторити стан резервних копій і отримувати сповіщення про можливі проблеми.

Таблиця 3.1

Процедури відновлення після збоїв

Етапи	**Опис**
Виявлення та оцінка проблеми	Виявлення причини збою шляхом аналізу лог-файлів, системних повідомлень і використання діагностичних інструментів. Визначення типу проблеми (апаратна, програмна або мережева).
Відновлення системи з резервних копій	Відновлення базових компонентів системи, таких як операційна система і бази даних. Якщо проблема апаратна, заміна несправних компонентів і відновлення системи з резервних копій.
Відновлення конфігураційних файлів	Відновлення файлів конфігурації Asterisk, налаштувань користувачів, даних про виклики та інших важливих параметрів з резервних копій.
Відновлення даних про виклики	Відновлення записів викликів, голосових повідомлень, записів розмов та інших важливих даних з резервних копій.
Перевірка цілісності та функціональності	Комплексне тестування системи для перевірки якості зв'язку, здійснення тестових дзвінків, перевірка роботи всіх функцій, таких як голосова пошта, переадресація дзвінків, конференц-зв'язок тощо.
Забезпечення безпеки	Переконання у правильності налаштувань безпеки, таких як шифрування трафіку, налаштування міжмережевих екранів (firewalls), аутентифікація користувачів, після відновлення системи.
Документування процесу відновлення	Записування всіх кроків, виконаних під час відновлення, включаючи виявлені проблеми, застосовані рішення та результати тестування, для покращення процесу в майбутньому.
Навчання персоналу	Регулярне навчання і тренінги для технічного персоналу, щоб вони були добре підготовлені до виконання процедур відновлення і знали всі деталі процесу.

Тестування системи на надійність є важливою складовою для забезпечення стабільної та безперебійної роботи VoIP-мережі. Цей процес охоплює кілька основних напрямків, кожен з яких допомагає виявити потенційні проблеми, оптимізувати продуктивність і забезпечити високий рівень якості зв'язку в різних умовах.

Перший напрямок – це навантажувальне тестування. Це тип тестування, який оцінює здатність системи справлятися з високими навантаженнями. Наприклад, симулюється велика кількість одночасних дзвінків, щоб побачити, як система реагує на пікові навантаження. Спеціалізовані інструменти, такі як SIPp

або Tsung, дозволяють створювати імітації сотень або тисяч дзвінків, аналізуючи, як система витримує навантаження. Це допомагає виявити можливі точки відмови та оптимізувати роботу системи[2].

Другий напрямок – тестування на відмовостійкість. Воно включає перевірку здатності системи продовжувати функціонувати навіть у разі відмови окремих компонентів. Наприклад, можна вимкнути один із серверів або мережевих пристроїв і перевірити, чи система здатна автоматично переключитися на резервні компоненти без втрати зв'язку. Це тестування виявляє слабкі місця в архітектурі системи і допомагає впровадити додаткові заходи для підвищення її надійності.

Третій напрямок – це тестування безпеки. Воно включає перевірку стійкості системи до різних типів атак, таких як атаки на відмову в обслуговуванні (DoS), підміна (spoofing) і перехоплення даних (eavesdropping). Використовуючи інструменти для тестування на проникнення, такі як Metasploit або Wireshark, можна симулювати атаки і перевірити, наскільки система захищена від них. Це дозволяє виявити вразливості та поліпшити заходи безпеки.

Четвертий напрямок – тестування якості зв'язку. Це включає аналіз якості голосового трафіку, перевірку затримок (latency), джиттера (jitter) і втрат пакетів (packet loss). Інструменти моніторингу, такі як VoIPmonitor або SolarWinds VoIP & Network Quality Manager, дозволяють проводити детальний аналіз якості зв'язку в різних умовах навантаження. Це допомагає виявити проблеми з мережею або конфігурацією системи, що можуть впливати на якість зв'язку[1].

П'ятий напрямок – тестування резервного копіювання та відновлення. Це включає перевірку процедур створення резервних копій конфігураційних файлів, баз даних та інших важливих даних, а також тестування відновлення системи після збоїв. Важливо переконатися, що резервні копії створюються регулярно і можуть бути використані для швидкого відновлення системи у разі збою. Це гарантує, що всі резервні копії є повними і можуть бути відновлені без проблем.

Шостий напрямок – тестування сумісності. Це перевірка роботи системи з різним обладнанням та програмним забезпеченням, яке може бути інтегроване в VoIP-мережу. Наприклад, перевіряється сумісність IP-телефонів, шлюзів,

адаптерів та інших пристроїв з платформою Elastix, щоб переконатися, що вони працюють належним чином. Це допомагає виявити та усунути проблеми сумісності, що можуть вплинути на загальну надійність системи.

Сьомий напрямок – тестування оновлень і патчів. Це перевірка роботи системи після встановлення оновлень програмного забезпечення, що може включати виправлення безпеки, нові функції або поліпшення продуктивності. Перед впровадженням оновлень у виробниче середовище необхідно тестувати їх у контрольованих умовах, щоб переконатися у відсутності негативного впливу на роботу системи. Це допомагає мінімізувати ризики, пов'язані з оновленнями, і забезпечує стабільну роботу системи[7].

Тестування системи на надійність включає навантажувальне тестування, тестування на відмовостійкість, тестування безпеки, перевірку якості зв'язку, тестування резервного копіювання та відновлення, тестування сумісності та тестування оновлень і патчів. Виконання цих заходів дозволяє забезпечити високу надійність VoIP-системи, її стійкість до різних загроз і стабільну роботу в різних умовах.

Висновки

Третій розділ присвячено важливим аспектам забезпечення якості та безпеки VoIP-мережі. Було розглянуто механізми QoS (Quality of Service), які дозволяють управляти пропускною здатністю, контролюючи максимальну швидкість передачі даних на певних інтерфейсах та пріоритизувати голосовий трафік, мінімізуючи затримки та втрати пакетів, що забезпечує високу якість голосового зв'язку. Також важливою складовою QoS є моніторинг працездатності стану мережі в режимі реального часу. Було проаналізовано різні загрози безпеці VoIP-мереж, такі як перехоплення трафіку, атаки на відмову в обслуговуванні, підміна та інші, а також методи захисту, включаючи шифрування SRTP та TLS, двохфакторну аутентифікацію, використання міжмережевих екранів та систем виявлення вторгнень. Детально описано стратегії резервного копіювання, такі як повне, інкрементне та диференційне резервне копіювання, а також процедури

відновлення системи після збоїв, що включають відновлення операційної системи, конфігураційних файлів та даних про виклики. Цей розділ підкреслює важливість комплексного підходу до забезпечення якості та безпеки VoIP-мереж, адже він є критичним для успішного функціонування та захисту від потенційних загроз.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

У дослідженні було проведено всебічний аналіз технологій VoIP та платформи Elastix, розроблено корпоративну VoIP-мережу на основі Elastix, а також розглянуто питання забезпечення якості та безпеки в VoIP-мережах. Кожен з розділів дослідження сприяв досягненню поставлених завдань та отриманню повної картини про сучасні можливості VoIP-технологій та їх впровадження в корпоративному середовищі.

Розглянуто технології VoIP, що включає принципи їх роботи, переваги та недоліки. Проаналізовано основні платформи для побудови VoIP-мереж, включаючи їх функціональні можливості та відмінності. Особливу увагу приділено платформі Elastix, яка поєднує в собі потужні інструменти для побудови та управління VoIP-мережами, інтегруючи Asterisk, бази даних, веб-інтерфейс та інші необхідні компоненти.

Були проаналізовані вимоги до мережі та проведено її планування, що включало визначення необхідного обладнання, мережевої топології та параметрів налаштування. Детально розглянуто процес встановлення та налаштування платформи Elastix, включаючи налаштування облікових записів, транків, маршрутизації викликів та інших параметрів. Завершальним етапом стало інтегрування та налаштування VoIP-обладнання, такого як IP-телефони, шлюзи та адаптери, для забезпечення повноцінного функціонування мережі.

Розглянуто методи забезпечення якості зв'язку (QoS), які дозволяють мінімізувати затримки, втрати пакетів та інші проблеми, що можуть впливати на якість голосового трафіку. Аналізувалися аспекти безпеки в VoIP-мережах, включаючи захист від несанкціонованого доступу, шифрування трафіку та інші заходи безпеки. Особливу увагу приділено резервуванню та відновленню системи, що включало стратегії резервного копіювання та процедури відновлення після збоїв, які забезпечують надійність і безперервність роботи VoIP-мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азаров О.Д., Захарченко С.М., Кадук О.В. Комп’ютерні мережі: навчальний посібник. Вінниця: Вінницький Національний Технічний Університет, 2013. 371 с. ISBN 978-966-641-543-4.
2. Азарова, А. О. Комп’ютерні мережі та телекомунікації: навчальний посібник / Азарова А. О., Лисак Н. В. – Вінниця : ВНТУ, 2012. – 293 с.
3. Буров Є.В. Комп’ютерні мережі. Львів: Магнолія, 2016. 262 с.
4. Гольдштейн Б. С., Пінчук А. В., Суховицький А. Л. IP-телефонія: Радіо і зв'язок, 2008.
5. Ракеш Арора. Передача голосових даних через IP: протоколи та стандарти (Voice over IP : Protocols and Standards), 1999
6. Джонатан Девідсон, Джеймс Пітерс, Манож Бхатія, Сатіш Калідінді, Судіпто М. Основи передачі голосових даних по мережах IP (IP Voice over IP Fundamentals); Вільямс, 2007
7. Жуковицький І.В., Педенко І.О. Аналіз безпеки бездротових мереж Wi-Fi в автоматизованих системах залізничного транспорту // Наука та прогрес транспорту. 2020. № 4 (88). С. 7-21.
8. Комп'ютерні мережі. Підручник / Ю.О. Кулаков, Г.М. Луцький. Київ: Вид-во "Юніор", 2015.
9. 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.
10. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу». - Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України - Київ 1999 – 53 с.
11. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі. Київ: Юніор, 2003. 400 с.

12. Николайчук Я.М., Возна Н.Я., Пітух І.Р. Проектування спеціалізованих комп’ютерних систем: Навчальний посібник. Тернопіль: ТзОВ "Терно граф", 2010.
13. Особливості побудови локальних мереж – URL: http://studopedia.org/13-100846.html
14. Передачі голосових даних в реальному часі через інтернет протокол / Режим доступу до ресурсу: http://inmad.vntu.edu.ua/portal/static/E3E35C35-800E-48F9-A804- 4DD5DB290AF0.pdf
15. Посібник користувача Elastix (Elastix User Manual) / Режим доступу до ресурсу: http://voip.com.vn/freeshare/datasheet/elastix_user_manual.pdf.
16. Романовський Ю.Р., Олексюк В.В., Балик А.В. Адміністрування комп’ютерних мереж і систем: Навч. пос. Тернопіль: Навчальна книга Богдан, 2014. 196 с.
17. Яковина В.С. Основи безпеки комп’ютерних мереж: Навчальний посібник / За ред. Д.В. Федасюка. Львів: НВФ "Українські технології", 2015. 396 с.