Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування закладу вищої освіти)
Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту, назва факультету (відділення))
Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

магістр
(рівень вищої освіти)

на тему **Удосконалення системи IP-телефонії на базі платформи Elastix**

Виконав: студент 2 курсу, групи 2мТТ спеціальності 172 «Телекомунікації та радіотехніка»
(шифр і назва напряму підготовки, спеціальності)
Дзюбан В.В.
(прізвище та ініціали)
Керівник Ігнатьєв С.С.
(прізвище та ініціали)
Рецензент Тищенко О.М.
(прізвище та ініціали)

Полтава - 2026 рік

РЕФЕРАТ

Магістерська робота: «Удосконалення системи IP-телефонії на базі платформи Elastix».

Обсяг роботи: 79 сторінок, 17 таблиць, 1 рисунок , 35 джерел літератури.

Ключові слова: IP-телефонія, SIP-сервер, Elastix, VPN, VoIP, безпека, телекомунікації.

У магістерській роботі розглянуто питання удосконалення системи IP-телефонії з використанням відкритої платформи Elastix. Проведено аналіз існуючих технологій VoIP-зв'язку, досліджено архітектуру SIP-серверів, принципи маршрутизації викликів та організації з'єднань у корпоративних мережах.

Сучасні телекомунікаційні системи зазнають стрімкої трансформації під впливом цифровізації, підвищення вимог до мобільності персоналу та глобального переходу на IP-базовані мережеві технології. Одним із ключових елементів цієї трансформації є IP-телефонія — технологія, що забезпечує передачу голосового трафіку на базі протоколу IP, дозволяючи підприємствам зменшувати витрати на зв'язок, підвищувати гнучкість та масштабованість комунікаційних систем [1].

Водночас у сучасних умовах підвищених вимог до кібербезпеки, захисту VoIP-сервісів та забезпечення безперервної роботи комунікаційних систем постає необхідність удосконалення існуючих рішень IP-телефонії. Сюди входить впровадження шифрування, VPN-тунелювання, додаткових механізмів аутентифікації та оптимізація продуктивності SIP-сервера. Саме тому тема удосконалення системи IP-телефонії на базі Elastix є актуальною та практично значущою.

Особливу увагу приділено проблемам безпеки — захисту сигналізаційного та голосового трафіку від несанкціонованого доступу, підслуховування та атак типу DoS.

Запропоновано технічне рішення із впровадження захищеного середовища IP-телефонії з використанням технологій VPN-тунелювання та шифрування SRTP/TLS.

Проведено моделювання та пробну інсталяцію системи у віртуальному середовищі VirtualBox, виконано тестування якості зв’язку, затримок і пропускної здатності каналів.

У результаті роботи розроблено рекомендації щодо побудови безпечних корпоративних VoIP-мереж на базі Elastix, які забезпечують високу надійність, масштабованість та відповідність сучасним вимогам телекомунікаційних систем.

Практичне значення: отримані результати можуть бути використані для розгортання IP-телефонії в невеликих і середніх компаніях, державних установах, а також для подальших досліджень у сфері інтеграції VoIP-систем із хмарними платформами та мобільними сервісами.

ABSTRACT

Master's Thesis: "Improvement of the IP Telephony System Based on the Elastix Platform".

Scope: 79 pages, 17 tables, 1 figures, 35 references.

Keywords: IP telephony, SIP server, Elastix, VPN, VoIP, security, telecommunications.

The master's thesis is devoted to improving the IP telephony system using the open-source platform Elastix. The work analyzes existing VoIP technologies, examines the architecture of SIP servers, call routing principles, and connection management in corporate networks. Special attention is given to security aspects — protection of signaling and voice traffic from unauthorized access, eavesdropping, and denial-of-service attacks.

A technical solution for implementing a secure IP telephony environment based on VPN tunneling and SRTP/TLS encryption is proposed. A pilot installation and testing were carried out in a VirtualBox environment, evaluating call quality, latency, and bandwidth utilization.

The research provides recommendations for building secure corporate VoIP networks based on Elastix, ensuring high reliability, scalability, and compliance with modern telecommunications standards.

Special attention is paid to security issues, in particular to the protection of signaling and voice traffic against unauthorized access, eavesdropping, and denial-of-service (DoS) attacks.

A technical solution for implementing a secure IP telephony environment based on VPN tunneling technologies and SRTP/TLS encryption is proposed.

Modeling and pilot installation of the system were carried out in a virtual environment using VirtualBox. Testing of call quality, transmission delays, and channel bandwidth was performed.

As a result of the study, recommendations for building secure corporate VoIP networks based on the Elastix platform were developed, ensuring high reliability, scalability, and compliance with modern telecommunications system requirements.

Practical significance: the obtained results can be used for deploying IP telephony systems in small and medium-sized enterprises, public institutions, as well as for further research in the field of integration of VoIP systems with cloud platforms and mobile services.

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій та робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Рівень вищої освіти Магістр
Спеціальність 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ
Завідувач кафедри автоматики,
електроніки та телекомунікацій
_____ О.В. Шефер
"15" 09 2025 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Дзюбану Володимиру Вікторовичу

1. Тема проекту (роботи) **«Удосконалення системи IP-телефонії на базі платформи Elastix»**

керівник проекту (роботи) **Ігнатьєв Станівлав Євгенович,** к.г.н.
затверджений наказом вищого навчального закладу від "03" березня 2025 року
№ 1025-ор а

2. Строк подання студентом проекту (роботи) 22.12.2025 р.
3. Вихідні дані до проекту (роботи)
   - Технічна документація на систему IP-телефонії на базі платформи Elastix. Дані про структуру та топологію волоконно-оптичних мереж, що використовуються як транспортне середовище. - Характеристика існуючих рішень IP-телефонії та їх інтеграції з ВОК. Вимоги до якості обслуговування (QoS), надійності та масштабованості IP-телефонії.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз сучасних систем IP-телефонії та їх використання на базі Elastix. Дослідження архітектури та функціональних можливостей платформи Elastix. Характеристика волоконно-оптичних мереж як транспортного середовища для IP-телефонії. Виявлення недоліків існуючої системи IP-телефонії (якість зв'язку, масштабованість, інтеграція). Розробка пропозицій з удосконалення системи IP-телефонії на базі Elastix. Моделювання роботи удосконаленої системи та аналіз її ефективності. Оцінка економічної доцільності та практичних переваг впровадження. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів): Структурна схема системи IP-телефонії на базі Elastix. Схема взаємодії IP-телефонії з волоконно-оптичною мережею. Діаграма архітектури сервера Elastix. Схема організації QoS у мережі для підтримки VoIP. Блок-схема інтеграції з іншими сервісами зв'язку. Графіки/діаграми ефективності після удосконалення.

6. Дата видачі завдання 01.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів магістерської роботи	Термін та обсяг виконання етапів роботи			При... (пла...
1	Аналіз сучасних систем IP-телефонії та постановка задач	07.10.25		15%	Пл.
2	Вивчення архітектури Elastix і вибір обладнання	21.10.25	I	25%	Пл.
3	Характеристика волоконно-оптичних мереж для IP-телефонії	04.11.25		40%	Пл.
4	Виявлення недоліків існуючої системи	11.11.25		50 %	Пл.
5	Розробка пропозицій з удосконалення системи	18.11.25	II	60%	Пл.
6	Моделювання роботи удосконаленої системи	25.11.25		70%	Пл.
7	Аналіз ефективності, економічна оцінка	09.12.25		90%	Пл.
8	Оформлення пояснювальної записки та висновків	22.12.25	III	100%	Пл.

Магістрант _____ (підпис) Дзюбан В.Е (прізвище та ініціали)

Керівник роботи _____ (підпис) Ігнатьєв С.Є (прізвище та ініціали)

ЗМІСТ

ВСТУП

Сучасний розвиток телекомунікаційних технологій зумовлює потребу у створенні більш гнучких, безпечних та економічно ефективних систем корпоративного зв’язку. Традиційні аналогові та цифрові телефонні станції поступово втрачають актуальність через високі витрати на обслуговування, складність масштабування та обмежені можливості інтеграції з іншими інформаційними системами. У цьому контексті дедалі більшого поширення набуває IP-телефонія (VoIP), яка забезпечує передачу голосового трафіку через мережі передачі даних із використанням відкритих протоколів.

Актуальність теми полягає у необхідності не лише впровадження, але й постійного удосконалення систем IP-телефонії, оскільки вимоги до якості зв’язку, безпеки та інтеграції з бізнес-процесами підприємств зростають. Одним із найбільш гнучких і функціональних рішень є програмно-апаратний комплекс Elastix, побудований на базі Asterisk і розширений інструментами адміністрування, моніторингу та інтеграції. Платформа Elastix**,** яка інтегрує Asterisk, FreePBX, OpenFire та інші серверні компоненти, залишається одним із найпопулярніших рішень для побудови локальних VoIP-систем у малому та середньому бізнесі, незважаючи на припинення її комерційного розвитку з 2016 року. Причина — відкритість коду, широкі можливості налаштування, сумісність зі стандартами SIP та підтримка великої кількості VoIP-пристроїв. Використання Elastix дозволяє розгорнути повноцінну телефонну інфраструктуру з мінімальними витратами на обладнання та ліцензії, що робить платформу актуальною для організацій різних масштабів. Завдяки цьому Elastix є зручною платформою для реалізації проектів корпоративної телефонії з можливістю їх подальшої оптимізації.

Мета і завдання роботи – розробити та дослідити шляхи удосконалення системи IP-телефонії для невеликої компанії із застосуванням рішення Elastix з

рахуванням вимог до ефективності, безпеки та інтеграції з корпоративними інформаційними системами.

Для досягнення мети передбачено виконання таких завдань:

1. Проаналізувати сучасний стан розвитку традиційної та IP-телефонії.
2. Розглянути архітектуру та функціональні можливості платформи Elastix.
3. Дослідити принципи роботи SIP-сервера та маршрутизації викликів.
4. Розробити проект впровадження системи IP-телефонії у невеликій компанії.
5. Провести тестове встановлення та налаштування Elastix у віртуальному середовищі. Розгорнути внутрішню телефонну мережу з використанням голосових шлюзів, IP телефонів, вітруальних IP телефонів (додатки).
6. Запропонувати заходи з удосконалення системи: оптимізація внутрішньої нумерації, організація IVR та черг, підвищення рівня безпеки. Забезпечити захист комунікацій за допомогою firewall, fail2ban, TLS, SRTP, VPN-тунелів.
7. Оцінити результати удосконалення з технічної та економічної точки зору.

Провести порівняльний аналіз платформи Elastix з альтернативними рішеннями та визначити перспективи її розвитку.

Об’єкт дослідження — процеси побудови, налаштування, оптимізації та захисту IP-телефонії на основі платформи Elastix, включаючи SIP-протоколи, маршрутизацію викликів, IVR-системи, безпекові механізми та інтеграцію з бізнес-процесами.

Предмет дослідження — система корпоративної IP-телефонії, побудована на базі VoIP-інфраструктури.

Методи дослідження: аналіз наукових і технічних джерел, моделювання мережевої інфраструктури, експериментальне впровадження та тестування роботи Elastix у середовищі VirtualBox, порівняльний аналіз техніко-економічних характеристик.

А саме:

- **аналітичні методи** — для вивчення принципів VoIP, SIP-сигналізації та архітектури Asterisk;

- **проєктні методи** — для побудови мережевої топології та структурних схем;
- **експериментальні методи** — для тестування пропускної здатності, якості голосу (MOS), стійкості до атак;
- **методи моделювання** — для аналізу роботи IP-телефонії в локальній мережі;
- **програмно-технічні методи** — для розгортання Elastix у VirtualBox та проведення SIP-конфігурацій.

Наукова новизна роботи полягає у визначенні та апробації практичних шляхів удосконалення системи IP-телефонії на базі Elastix з урахуванням сучасних вимог до безпеки та ефективності корпоративного зв'язку.

У роботі запропоновано:

- **комплексну модель підвищення безпеки** IP-телефонії на базі Elastix з використанням SRTP/TLS та IPS/IDS-механізмів;
- **оптимізовані налаштування SIP-сервера**, що зменшують затримку та втрати пакетів у LAN;
- **впровадження тунельного захисту (IPSec/OpenVPN)** для зовнішніх співробітників;
- **модель інтеграції IP-телефонії з CRM/ERP**, адаптовану під малий бізнес.

Практична цінність роботи полягає у можливості використання напрацьованих рішень для побудови та оптимізації систем IP-телефонії у малому та середньому бізнесі, що сприятиме зниженню витрат на зв'язок, підвищенню рівня інформаційної безпеки та забезпеченню інтеграції з іншими інформаційними системами підприємства.

Результати дослідження можуть бути застосовані: у невеликих та середніх компаніях, у структурах з клієнтською підтримкою, при побудові кол-центрів, у регіональних філіях, де необхідний захищений зв'язок між віддаленими офісами.

Побудована система дозволяє знизити витрати на телефонний зв’язок у 2–6 разів, забезпечити централізоване управління та інтегрувати телефонію з бізнес-процесами підприємства [2].

1. АНАЛІТИЧНА ЧАСТИНА

1.1. Огляд літератури та сучасних рішень у сфері IP-телефонії

Питання побудови сучасних VoIP-систем та використання IP-телефонії широко висвітлене у фаховій та науково-технічній літературі. Значна увага приділяється аналізу протоколів передачі голосу, архітектурі IP-телефонних систем, методам забезпечення якості обслуговування (QoS) і безпеки SIP-трафіку. У цьому розділі наведено огляд основних джерел, що стали базою для теоретичної та практичної частини роботи.

Одним із фундаментальних джерел є офіційна документація Asterisk, яка детально описує SIP-сигналізацію, обробку дзвінків, конфігурацію діалпланів, роботу кодеків та логіку маршрутизації. Документація є важливою для розуміння внутрішньої архітектури Elastix, оскільки платформа фактично є надбудовою над Asterisk з інтегрованими модулями FreePBX, Postfix, OpenFire та іншими сервісами [3]. У численних офіційних керівництвах наведено алгоритми налаштування SIP-транків, користувачів, IVR і систем безпеки, які стали основою для практичних прикладів у роботі.

Важливе значення мають наукові праці, присвячені протоколу SIP та методам його оптимізації. У багатьох дослідженнях аналізуються механізми обробки SIP-повідомлень, проблеми NAT-трансляції, затримок та джитеру, а також вплив якості мережі на MOS-показники. Автори підкреслюють, що SIP є ключовим стандартом комунікації в IP-телефонії, який забезпечує гнучкість і масштабованість системи. Ці джерела дозволили сформувати теоретичну основу підрозділів, присвячених роботі SIP-сервера, методам сигналізації та маршрутній обробці викликів.

Суттєвий внесок у дослідження IP-телефонії роблять публікації провідних телекомунікаційних компаній, таких як Cisco, Avaya, Huawei, де докладно описано принципи проєктування корпоративних VoIP-мереж, моделі QoS, алгоритми пріоритезації голосового трафіку та механізми захисту. Хоча ці компанії використовують власні комунікаційні платформи, їхній теоретичний і практичний досвід є універсальним і застосовним до відкритих систем, зокрема Asterisk/Elastix.

Окремим напрямом є дослідження безпеки IP-телефонії, де розглядаються такі загрози, як SIP spoofing, brute-force атаки, перехоплення RTP, DoS-атаки на SIP-порт, несанкціоноване використання транків та виклики-шахрайства (VoIP fraud). У працях фахівців з кібербезпеки зазначено, що впровадження TLS, SRTP, fail2ban, IDS/IPS та VPN-тунелів значно підвищує захист системи від несанкціонованого доступу [4]. Ці матеріали були використані для створення розділу 4, де пропонуються удосконалені моделі захисту IP-телефонії.

Важливу групу джерел становлять наукові статті, що аналізують роботу VoIP у мережах різної топології. Дослідники порівнюють якість голосу під час використання різних кодеків (G.711, G.729, Opus), моделюють затримки у каналах, а також вивчають вплив навантаження на SIP-сервер. Отримані результати дозволили сформувати обґрунтовані рекомендації щодо вибору кодеків та налаштування параметрів Asterisk у розділі 2.

Окремо потрібно відзначити матеріали спільноти Elastix, які, попри припинення офіційної підтримки, залишаються доступними у вигляді архівів, форумів, довідників та практичних прикладів налаштування. Вони містять сценарії конфігурації SIP-транків, приклади IVR-меню, налаштування безпеки, фрагменти діалпланів та інструкції для інтеграції з CRM/ERP-системами. Ці матеріали застосовано в практичному розділі роботи.

Також значною була роль спеціалізованих монографій з VoIP, де подається глибокий аналіз протоколів RTP/RTCP, механізмів синхронізації, адаптивної компенсації джитеру, а також моделей пакетної передачі голосу. Ці праці дозволили

детальніше пояснити роботу голосового трафіку у мережах з різною пропускною здатністю.

У результаті аналізу літератури встановлено, що, хоча наявні публікації детально описують окремі аспекти VoIP і SIP-технологій, комплексне дослідження практичного впровадження та підвищення безпеки саме платформи Elastix у малих компаніях зустрічається порівняно рідко. Це визначає актуальність та практичну значущість обраної теми, а також формує наукову новизну роботи.

1.2. Тенденція розвитку телефонних систем

Телефонний зв’язок є одним із найважливіших досягнень людства у сфері комунікацій, який за понад півтора століття пройшов шлях від простих аналогових пристроїв до сучасних інтегрованих цифрових і IP-мереж. Його еволюція безпосередньо вплинула на формування сучасних інформаційно-комунікаційних технологій та створила підґрунтя для розвитку глобальних систем обміну даними.

Ранні етапи розвитку телефонії

Перші експерименти з передаванням голосу електричними сигналами датуються серединою XIX століття. У 1876 році Олександр Белл отримав патент на телефон, який став основою для масового впровадження голосового зв’язку. Перші телефонні лінії були простими аналоговими, що працювали на базі мідних дротів і забезпечували обмежену відстань передавання сигналу без підсилювачів.

Наприкінці XIX – на початку XX століття активно розвиваються телефонні станції, що дозволяло обслуговувати дедалі більшу кількість абонентів. Спочатку це були ручні комутаційні пункти, однак у 1891 році був винайдений автоматичний комутатор (система Строуджера), що започаткувало перехід до автоматизованої телефонії.

Етап цифровізації телефонних мереж

У другій половині XX століття розвиток електроніки призвів до поступового переходу від аналогових комутаторів до цифрових. Важливим кроком стало впровадження технології цифрової комутації та стандартизація протоколів передавання голосу у вигляді цифрових сигналів. Зокрема, у 1960–1970-х роках активно розвиваються мережі з комутацією каналів на основі технології TDM (Time Division Multiplexing**)**, яка дозволила ефективніше використовувати пропускну здатність ліній зв'язку.

Цифрова телефонія забезпечила вищу якість звуку, надійність та можливість інтеграції з іншими видами послуг (наприклад, факсимільним зв'язком). Водночас саме цифровізація стала передумовою подальшого переходу до об'єднання голосового і комп'ютерного трафіку.

Перехід до IP-телефонії

У 1990-х роках із поширенням Інтернету з'явилися перші технології передавання голосу через IP-мережі (Voice over IP, VoIP). Спочатку якість зв'язку була низькою через обмежену пропускну здатність каналів і відсутність механізмів компенсації затримок. Проте подальший розвиток мережевих протоколів, зокрема SIP (Session Initiation Protocol) та RTP (Real-time Transport Protocol)**,** забезпечив якісний і масштабований голосовий сервіс у локальних і глобальних мережах.

З початку 2000-х років IP-телефонія почала витісняти традиційні телефонні мережі. Це пояснюється такими перевагами: зниження витрат на інфраструктуру, можливість інтеграції з інформаційними системами підприємств, масштабованість і підтримка додаткових сервісів (відеозв'язок, конференції, інтеграція з CRM).

Сучасний стан і перспективи

Сьогодні телефонія стала невід'ємною частиною концепції уніфікованих комунікацій (Unified Communications), де голосовий зв'язок інтегрується з відео, миттєвими повідомленнями, корпоративними порталами та хмарними сервісами.

Одним із популярних рішень стала платформа Elastix, яка об’єднує функціонал IP-АТС на базі Asterisk із додатковими модулями (пошта, чат, кол-центр, інтеграція з CRM). Це дозволяє малим і середнім компаніям будувати власні корпоративні телефонні мережі з мінімальними витратами.

У майбутньому IP-телефонія розвиватиметься у напрямі інтеграції з мобільними мережами 5G/6G, хмарними обчисленнями та системами на основі штучного інтелекту, що забезпечить ще вищу якість обслуговування, адаптивне керування трафіком і автоматизацію бізнес-процесів.

1.3. Основні принципи роботи IP-телефонії

IP-телефонія (VoIP, Voice over IP) — це технологія передавання голосових сигналів через комп’ютерні мережі на основі протоколу IP. Її принципова відмінність від традиційної телефонії полягає у відсутності комутації каналів: замість постійного виділеного каналу використовується передавання даних у вигляді пакетів.

Перетворення голосу на цифровий сигнал

Першим етапом є перетворення аналогового голосового сигналу у цифрову форму. Загальна послідовність обробки голосу

1. Аналого-цифрове перетворення (ADC). Голос з мікрофона дискретизується: типова частота для телефонії — 8 кГц (телефонний діапазон 300–3400 Гц) або 16 кГц для широкосмугового звуку [3].

2. Кодування (codec). Отриманий цифровий потік кодується алгоритмом (G.711, G.729, Opus), що визначає якість і бітрейт.

3. Пакетизація. Цифрові семпли групуються в пакети RTP; типова тривалість фрейма — 20 ms або 30 ms.

4. Інкапсуляція. RTP (медіа) інкапсулюється у UDP, а UDP — у IP; сигнальну частину обслуговує SIP (у TCP/UDP або TLS).

5. Трансмісія та відтворення. На приймаючому боці пакети буферизуються (jitter buffer), декодуються та перетворюються у звукові хвилі (DAC).

Для цього застосовуються:

- Аналого-цифрове перетворення (ADC) – мікрофонний сигнал оцифровується з певною частотою дискретизації (наприклад, 8 кГц або 16 кГц).
- Кодування та стиснення (кодеки) – застосовуються алгоритми G.711, G.729, Opus тощо, які забезпечують різні компромісні співвідношення між якістю звуку та необхідною пропускною здатністю каналу.

Формування та передавання пакетів

Параметри пакетизації і їхній вплив

- Interval (T) — тривалість одного RTP-фрейма (наприклад, 20 ms).
- Payload bytes per packet (P) — кількість байт корисного навантаження у кожному RTP-пакеті (залежить від кодека і T).
- Overhead per packet (O) — байти заголовків: IP(20) + UDP(8) + RTP(12) = 40 байт (без врахування VPN або Ethernet заголовків).

Формула приблизного споживання каналу (байт/с):

$$BW_{bytes} = \frac{P + O}{T}$$

$$BW_{kbits/s} = \frac{P + 8}{1000}$$

де TTT у секундах (наприклад, для 20 ms T=0.02T=0.02T=0.02).

Приклад розрахунку (G.711, 20 ms):

- G.711 payload: 8 kHz × 8 bit/sample = 64 kbit/s → за 20 ms: P=64 000×0.02/8=160P = 64\,000 \times 0.02 /8 = 160P=64000×0.02/8=160 байт.
- Overhead O = 40 байт.

- BW_bytes/s = (160 + 40) / 0.02 = 10 000 bytes/s → 80 000 bit/s = 80 kb/s.

Отже, один виклик G.711 із 20 ms пакетизацією ≈ 80 kb/s (без Ethernet/PoE/VRF/ VPN накладних).

Приклад (G.729, 20 ms):

- G.729 payload ≈ 8 kbit/s → за 20 ms: P=8 000×0.02/8=20P = 8\,000 \times 0.02 /8 = 20P=8000×0.02/8=20 байт.
- BW_bytes/s = (20 + 40) / 0.02 = 3 000 bytes/s → 24 000 bit/s = 24 kb/s.

Висновок: вибір кодека критично впливає на пропускну здатність; при обмеженій мережі слід використовувати низькобітрейтові кодеки (G.729, Opus), але слід враховувати ліцензійні обмеження та навантаження на CPU для енкодингу/декодингу [4].

Оцифрований сигнал розбивається на пакети та інкапсулюється в транспортні протоколи:

- RTP (Real-Time Transport Protocol) – використовується для передавання медіапотоку (голос, відео).
- UDP (User Datagram Protocol) – забезпечує швидке передавання без встановлення з’єднання, що важливо для реального часу.
- IP (Internet Protocol) – здійснює маршрутизацію пакетів у мережі.

Завдяки такій схемі IP-телефонія може працювати через локальні мережі (LAN) та глобальну мережу Інтернет.

Сигнальні протоколи

Окрім передавання голосу, важливим завданням є встановлення, керування та завершення сеансів зв’язку. Для цього використовуються сигнальні протоколи, найпоширеніші з яких:

Протокол SIP (Session Initiation Protocol)

SIP (RFC 3261) — найпоширеніший сигнальний протокол у системах IP-телефонії. Його функція — ініціювати, змінювати та завершувати сеанси комунікації між користувачами.

Він побудований за моделлю клієнт–сервер і використовує методи, подібні до HTTP (наприклад, INVITE, ACK, BYE, REGISTER).

Основні елементи SIP-інфраструктури:

- User Agent (UA) — пристрій користувача (IP-телефон, softphone);
- Registrar Server — виконує реєстрацію користувачів у системі;
- Proxy Server — маршрутизує SIP-запити;
- Redirect Server — перенаправляє виклики;
- Location Server — зберігає інформацію про активних користувачів.

Типовий сценарій встановлення дзвінка:

1. UA1 відправляє запит INVITE до SIP Proxy;
2. Proxy пересилає запит UA2;
3. UA2 відповідає 180 Ringing → 200 OK;
4. UA1 підтверджує ACK;
5. Починається передача голосових пакетів через RTP.

SIP (Session Initiation Protocol) – відкритий стандарт, що широко застосовується у сучасних системах IP-телефонії. Архітектура та ролі SIP-компонентів

- User Agent (UA) — кінцевий пристрій (IP-телефон, softphone).
- Registrar — приймає реєстрації (REGISTER).
- Proxy — маршрутизатор запитів та контролер політик.
- Redirect — перенаправляє запити за потреби.
- Location Server — зберігає актуальні адреси UA [3].

Типова послідовність встановлення виклику (SIP flow)

Опис покроково:

1. REGISTER — UA → Registrar: реєстрація облікового запису (IP/порт).
2. INVITE — UA-A → Proxy → UA-B: ініціювання дзвінка; INVITE включає SDP з параметрами медіа (кодеки, IP/порт для RTP).
3. 100 Trying / 180 Ringing — проміжні відповіді про стан.

4. 200 OK (від UA-B) — прийняття виклику; у відповіді теж є SDP (точки для RTP).

5. ACK — UA-A підтверджує отримання 200 OK.

6. RTP потік — безпосередній обмін голосовими пакетами (можливо через RTP relay або SRTP якщо шифрування).

7. BYE — ініціатор завершення сеансу; потім 200 OK для BYE.

Протокол RTP (Real-time Transport Protocol)

RTP (RFC 3550) відповідає за транспортування аудіо- та відеопотоків у реальному часі. Він не гарантує доставку пакетів, але забезпечує:

- маркування часу (timestamp) для синхронізації;
- нумерацію пакетів;
- можливість адаптації до втрат у мережі.

Зазвичай RTP використовується в парі з RTCP (Real-time Control Protocol), який збирає статистику, вимірює затримки, втрати пакетів і якість передачі (QoS).

Для захисту голосових даних використовується SRTP (Secure RTP) — версія з шифруванням (AES) та автентифікацією пакетів.

Протокол IAX (Inter-Asterisk eXchange)

IAX — фірмовий протокол системи Asterisk, який з’явився як альтернатива SIP для внутрішньої взаємодії між IP-АТС.

Його ключові особливості позначені в таблиці 1.1:

Таблиця 1.1 - Ключові особливості протоколу IAX

Параметр	SIP	IAX2
Тип передавання	UDP (порти 5060/5061)	UDP (4569)
Сигналізація і медіа	Окремі потоки	Один канал
NAT-сумісність	Складна	Висока
Пропускна здатність	Більша	Менша (завдяки trunking)
Безпека	TLS, SRTP	Власне шифрування

Використання	Між клієнтами та серверами	Між серверами Elastix

Таким чином, IAX2 часто застосовується для з'єднання між двома вузлами IP-телефонії (наприклад, між філіями компанії), оскільки він обходить проблеми NAT і економить пропускну здатність.Протокол забезпечення якості обслуговування (QoS)

Голосовий трафік має бути переданий із мінімальними затримками (<150 мс) і втратами (<1%). Для цього використовуються технології QoS (Quality of Service).

Основні підходи:

1. DiffServ (Differentiated Services) — класифікація трафіку за пріоритетами (DSCP-біти в IP-заголовку).
2. ToS (Type of Service) — старий, але сумісний із DiffServ механізм.
3. VLAN Voice (802.1p) — виділення голосового трафіку в окремий логічний сегмент.
4. Traffic Shaping / Policing — обмеження та розподіл пропускної здатності.

Рекомендовані параметри приведені в таблиці 1.2

Таблиця 1.2 - Рекомендовані параметри QoS для VoIP

Показник	Оптимальне значення	Граничне значення
Затримка (Delay)	≤ 150 мс	≤ 400 мс
Джиттер	≤ 30 мс	≤ 75 мс
Втрати пакетів	≤ 1%	≤ 3%
MOS (Mean Opinion Score)	≥ 4.0	≥ 3.6

Схема 1.1 - потоку голосового трафіку:

[IP Phone] ► [Switch QoS Enabled] ► [Router] ►[VPN Tunnel] ►[SIP Server Elastix]

▲ |

└──── RTP + RTCP ────┘

QoS забезпечує пріоритетність RTP-пакетів на рівні комутації та маршрутизації, що мінімізує затримки й втрати голосових даних навіть при високому навантаженні мережі.

Якість обслуговування (QoS)

Однією з ключових проблем IP-телефонії є забезпечення якості голосу. На відміну від традиційної телефонії, де канал був зарезервований, у VoIP пакети можуть затримуватися або губитися.

Ключові показники QoS

- Delay (Latency) — очікувана двостороння затримка; норматив: ≤150 ms.
- Jitter — нерівномірність доставки пакетів; оптимально ≤30 ms.
- Packet Loss — кількість втрачених пакетів; бажано ≤1%.
- MOS (Mean Opinion Score) — оцінка якості від користувачів (0–5); для прийнятної якості MOS ≥ 4.0 [7].

Механізми забезпечення QoS

1. Маркування DSCP/ToS. Голосовий трафік маркується як Expedited Forwarding (EF) → пріоритет обробки в маршрутизаторах.
2. 802.1p / VLAN. Виділення Voice VLAN + пріоритет 802.1p у L2-комутаторах.
3. Traffic Shaping / Policing. Обмеження небажаного трафіку, щоб захистити голосовий потік.
4. Jitter Buffer. На приймаючому боці динамічний буфер вирівнює нестабільність інтервалів доставки, але збільшує затримку.

Приклад налаштування QoS (коротко):

- На комутаторі: налаштувати Voice VLAN 20; пріоритет 802.1p = 5 для голосових портів.
- На маршрутизаторі: політика, що ставить DSCP=EF (46) для UDP портів RTP.
- На кінцевих телефонах: встановити DSCP маркування (якщо підтримується).

Для мінімізації цього використовуються:

- пріоритезація трафіку (QoS, DiffServ);

- буфери згладжування (jitter buffer);
- контроль смуги пропускання.

Завдяки цим механізмам сучасні IP-мережі можуть забезпечувати рівень якості, співставний із цифровою телефонією.

Протокол SDP (Session Description Protocol) у INVITE

SDP описує: IP/порт для RTP, набір кодеків, параметри FMTP (для специфічних кодеків), напрямки (sendrecv) і т.д. Некоректне або заблоковане SDP (наприклад через NAT) — причина відсутності аудіо навіть при успішній SIP-сигналізації.

Протокол H.323 – ранній протокол для мультимедійних комунікацій у мережах IP.

Протокол MGCP (Media Gateway Control Protocol) – використовується для взаємодії шлюзів і контролерів у VoIP-мережах.

У більшості сучасних систем (у тому числі Elastix) саме SIP є стандартом де-факто, оскільки він простий у реалізації та підтримує розширення функціоналу.

Протокол NAT / Firewall проблеми та рішення

Проблема: UA за NAT реєструється з внутрішньою приватною адресою, у SDP вказується локальний IP, віддалений UA надсилає RTP на невірну адресу → немає аудіо.

Рішення:

- STUN — дозволяє UA дізнатися зовнішню IP/порт [6].
- TURN — relay для медіа, коли пряме з’єднання неможливе.
- ICE — поєднує STUN/TURN для вибору найкращого шляху.
- SIP ALG — іноді «лікує» SDP, але часто створює проблеми — краще вимикати на роутері та використовувати VPN або SBC (Session Border Controller).

Робота IP-телефонії в умовах NAT: проблеми та методи вирішення

Природа NAT та його вплив на VoIP

NAT (Network Address Translation) — це механізм трансляції приватних IP-адрес у публічну, що використовується для економії адресного простору IPv4 та організації безпеки всередині мережі [6].

У VoIP NAT створює складнощі, тому що:

1. SIP є протоколом прикладного рівня, який передає IP-адреси та порти всередині свого тіла повідомлення (SDP).
2. RTP використовує динамічні порти, тобто діапазон, а не один порт.
3. UDP не встановлює з'єднання, через що NAT не завжди знає, як правильно відкрити зворотний канал.

У результаті виникають типові симптоми:

- є дзвінок, але немає аудіо в один бік або у два боки;
- дзвінок не встановлюється, SIP приходить із затримкою;
- після 30–40 секунд дзвінок розривається через повторний INVITE/реєстрацію;
- RTP надходить не туди, бо пристрій за NAT передає внутрішній IP у SDP [7].

Різновиди NAT представлені в таблиці 1.3

Таблиця 1.3 - Типи NAT та їхня взаємодія з RTP/SIP

Тип NAT	Особливості	Складність для VoIP
Full Cone NAT	Відповідає на будь-який вхідний трафік, якщо був попередній вихідний пакет	Найпростіший
Restricted Cone NAT	Вхідний трафік дозволено тільки з адрес, куди були попередні вихідні пакети	Середня
Port-Restricted NAT	Додатково контролює номера портів	Висока
Symmetric NAT	Трансляція створюється для кожної пари «внутрішній IP/порт → зовнішній IP/порт»	Найгірше для VoIP

Різні типи NAT по-різному обробляють трафік, що визначає, наскільки складно «пробитися» з аудіопотоком.

У більшості побутових та офісних роутерів сьогодні використовується Port-Restricted або Symmetric NAT, що значно ускладнює RTP-трафік [8].

SIP і SDP під NAT: чому виникає проблема «є дзвінок — немає звуку»

1) SIP передає IP і порти усередині SDP

Приклад SDP у INVITE:

c=IN IP4 192.168.1.25

m=audio 16384 RTP/AVP 0 8 18

Проблема: віддалений хост намагається відправляти RTP на 192.168.1.25, що є приватною адресою.

2) RTP динамічний

Кожен виклик використовує свої унікальні порти → NAT важко передбачити правильне перенаправлення.

3) NAT очищає таблицю трансляцій

Якщо дзвінок «висить», але не приходить періодичний SIP/keepalive-пакет, трансляція закривається → аудіо пропадає через 30 секунд.

Страшний ворог VoIP — SIP ALG

Більшість роутерів мають SIP ALG (Application Layer Gateway)**.** Його мета — автоматично правити SIP/SDP, але часто він ламає:

- переписування SDP із неправильними IP/портами;
- блокування пакета ACK;
- затримки SIP-потоку;
- заміну портів RTP некоректним чином [9].

Рекомендація:

На 90% обладнання SIP ALG потрібно відключати, бо він погіршує якість VoIP.

Основні методи вирішення NAT-проблем

1. Використання STUN

STUN (Session Traversal Utilities for NAT) дозволяє SIP-клієнту дізнатись свою зовнішню публічну адресу і порт [6].

Як працює:

1. UA надсилає запит STUN-серверу.
2. Отримує відповідь із зовнішньою IP та портом.
3. Підставляє ці параметри у SDP або SIP REGISTER.

Переваги:

- простий механізм;
- працює з усіма типами NAT, крім Symmetric NAT.

Недоліки:

- часто STUN допомагає тільки для SIP, але не RTP;
- не працює при жорсткій корпоративній політиці Firewall.

2. TURN (Traversal Using Relays around NAT)

TURN — це ретранслятор**.**

Коли прямий RTP неможливий, аудіопакети передаються через TURN-сервер.

Сценарій:

UA → TURN → UA

Затримка збільшується, але це «останній шанс» пройти через NAT-FW.

Плюси:

- 100% проходження аудіо навіть через Symmetric NAT.

Мінуси:

- велика затримка;
- велике навантаження на сервер;
- потрібне масштабування.

3. ICE (Interactive Connectivity Establishment)

ICE об’єднує STUN і TURN. Це найсучасніший механізм, який:

- генерує список усіх доступних IP/портів UA (локальні, STUN, TURN);

- обирає найкращий шлях для медіа;
- автоматично перемикається, якщо маршрут падає [7].

ICE особливо важливий у WebRTC, але використовується і в SIP з SRTP.

4. Використання SBC (Session Border Controller)

SBC — гарантований спосіб вирішити NAT:

- термінує SIP/TLS;
- робить повний NAT RTP;
- уніфікує порти;
- контролює QoS;
- забезпечує безпеку.

SBC «ховає» внутрішню мережу і робить так, наче всі клієнти — у публічній мережі [8].

5. RTP relay (re-INVITE)

Сервер PBX (Asterisk/Elastix) може виступати як точка проксіювання RTP:

- клієнт A → PBX → клієнт B

Це вирішує NAT-проблеми, але збільшує затримку.

Приклади налаштувань Asterisk:

nat=force_rport,comedia

directmedia=no

icesupport=yes

6. “Keep-alive” механізми

Періодичні SIP OPTIONS або CRLF-пакети дозволяють:

- не давати NAT-таблиці «зникнути»;
- уникнути обривів через 30–60 секунд.

Типові інтервали:

- SIP keepalive: 60 s
- RTP keepalive: 30–45 s
- Реальні сценарії проблем та їх розв’язання

Сценарій 1: Є дзвінок, але немає звуку

Причина: у SDP вказано приватний IP

Рішення:

- вимкнути SIP ALG;
- увімкнути STUN у клієнті;
- виставити nat=comedia на Asterisk.

Сценарій 2: Звук є тільки в один бік

Причина: блокування портів 10000–20000 на Firewall

Рішення:

- відкрити діапазон RTP;
- використовувати TURN при жорсткому FW.

Сценарій 3: Дзвінок обривається через 30 секунд

Причина: NAT очищає таблицю, ACK або 200 OK не доходить

Рішення:

- зменшити SIP registration timeout;
- увімкнути SIP keepalive (CRLF);
- використовувати SIP over TCP.

Сценарій 4: На одній лінії працює, на іншій — ні

Причина: Carrier NAT або Symmetric NAT

Рішення:

- TURN;
- SBC;
- VPN-тунель.

Рекомендована схема VoIP у мережі з NAT

Оптимальний варіант (для бізнесу):

IP Phones → Switch (Voice VLAN) → Router → SBC → Internet/SIP provider

Оптимальний варіант (для домашнього та малого офісу):

IP Phones → Router (SIP ALG off) → Elastix/Asterisk → Provider

Для WebRTC / мобільних:

UA (WebRTC) → STUN/TURN → PBX → Provider

Підсумок

NAT — ключова причина більшості проблем VoIP. Затримки, відсутність звуку та односторонній аудіоканал спричинені тим, що SIP і RTP не були розроблені з урахуванням NAT.

Сучасні механізми — STUN, TURN, ICE, SBC — дозволяють повністю вирішити ці проблеми, але кожен має свої компроміси щодо затримки, навантаження та безпеки [9].

Роль протоколів у системах IP-телефонії

Системи IP-телефонії функціонують завдяки взаємодії кількох рівнів протоколів, кожен з яких виконує окрему роль у процесі встановлення, управління та завершення сеансів зв'язку.

У спрощеному вигляді можна виділити три рівні, які наведені в таблиці 1.4 :

Таблиця 1.4 - Спрощена таблиця рівнів обробки рівнів протоколів

Рівень	**Функція**	**Основні протоколи**
Сигнальний	Встановлення, керування та завершення викликів	SIP, H.323, IAX2
Транспортний	Передача голосових даних у реальному часі	RTP, SRTP
Сервісний	Додаткові сервіси: реєстрація, автентифікація, QoS	DNS, DHCP, STUN, QoS (DiffServ, ToS)

Таким чином, IP-телефонія — це багаторівнева система, де успішна робота залежить від злагодженої взаємодії цих протоколів.

Інтеграція з іншими сервісами

Ще однією особливістю IP-телефонії є можливість інтеграції з іншими цифровими сервісами:

- відеозв'язок (через SIP/RTP з передаванням відеопотоку);

- конференц-зв’язок;
- інтеграція з CRM та ERP системами;
- мобільні додатки та softphone-клієнти.

На відміну від класичних телефонних мереж, де з’єднання виділяється на весь час розмови, у VoIP передавання здійснюється через комутацію пакетів, що значно підвищує ефективність використання пропускної здатності. Це забезпечує високу якість голосу за умови коректної конфігурації QoS, мінімальної затримки та обмеженого рівня джитерів [1].

Завдяки підтримці широкого спектра протоколів — SIP, RTP, IAX2 — VoIP-технології дозволяють інтегрувати голосові сервіси з інформаційними системами підприємств, CRM, ERP, сервісами аналітики та хмарними платформами. Це формує основу для побудови гнучких та масштабованих комунікаційних рішень.

Таким чином, IP-телефонія є не лише технологією передавання голосу, а й платформою для побудови комплексних комунікаційних рішень.

1.4. Переваги і недоліки IP-телефонії порівняно з традиційною

IP-телефонія за останні два десятиліття стала масовим рішенням для корпоративного та домашнього використання, поступово витісняючи традиційні аналогові та навіть цифрові телефонні системи. Її поширення зумовлене низкою переваг, проте разом із ними існують і певні обмеження.

Переваги IP-телефонії

1. Зниження вартості дзвінків

Використання IP-мереж, зокрема Інтернету, дозволяє значно скоротити витрати на міжміські та міжнародні дзвінки. Для корпоративних мереж дзвінки між офісами можуть бути безкоштовними, якщо вони проходять через внутрішню IP-інфраструктуру.

2. Економія на інфраструктурі

IP-телефонія працює на базі вже існуючих комп'ютерних мереж, що дозволяє уникнути дублювання кабельних систем. У більшості випадків телефонні апарати підключаються через Ethernet або Wi-Fi.

3. Гнучкість і масштабованість

Додавання нових абонентів не потребує прокладання окремих телефонних ліній — достатньо налаштувати нові облікові записи на SIP-сервері. Це особливо зручно для компаній, що швидко розвиваються.

4. Додатковий функціонал

IP-телефонія дозволяє легко реалізовувати сервіси, що недоступні або дорогі у традиційних мережах:

- відеодзвінки;
- конференції;
- голосова пошта;
- інтеграція з CRM/ERP;
- кол-центри та IVR-системи;
- передача повідомлень;

5. Мобільність користувачів

Завдяки softphone-додаткам співробітник може використовувати свій корпоративний номер із будь-якого місця, де є Інтернет. Це особливо актуально для віддаленої роботи.

6. Інтеграція з інформаційними системами

VoIP легко поєднується з корпоративними сервісами: електронною поштою, системами обліку, чатами, відеоконференціями. Це відповідає сучасній концепції уніфікованих комунікацій (UC).

Недоліки IP-телефонії

1. Залежність від Інтернет-з'єднання. Якість голосу та стабільність дзвінка безпосередньо залежать від пропускної здатності та затримок у мережі. У випадку низької швидкості або перевантаження можливі обриви чи спотворення звуку.

2. Проблеми із забезпеченням QoS (якості обслуговування). У загальних IP-мережах голосові пакети можуть конкурувати з іншими видами трафіку. Без механізмів пріоритезації (QoS) виникають затримки та втрати пакетів.

3. Вимоги до електроживлення. Традиційні телефонні апарати могли працювати від напруги телефонної лінії. IP-телефонія вимагає живлення (через блок або технологію PoE), тому при відключенні електроенергії мережа стає недоступною без резервного живлення.

4. Безпека. Голосовий трафік у IP-мережах може бути перехоплений або змінений. Для захисту застосовуються механізми шифрування (SRTP, TLS), але їх налаштування потребує додаткових ресурсів.

5. Сумісність з традиційними мережами. Для інтеграції VoIP із публічною телефонною мережею (PSTN) потрібні спеціальні шлюзи (VoIP-gateway), що підвищує вартість впровадження.

Дані приведені в таблиці 1.5

Таблиця 1.5 - Порівняння звичайної телефонії з IP-телефонією

Критерій	Традиційна телефонія (PSTN)	IP-телефонія (VoIP)
Вартість дзвінків	Висока	Низька/безкоштовна в мережі
Інфраструктура	Окрема телефонна мережа	Використання IP-мереж
Масштабованість	Обмежена	Висока
Додаткові сервіси	Мінімальні	Широкий спектр
Залежність від інтернет	Немає	Є
Живлення апаратів	Від лінії	Зовнішнє або PoE
Безпека	Відносно висока	Потребує додаткових засобів

1.5. Огляд сучасних платформ IP-телефонії

Розвиток IP-телефонії призвів до появи великої кількості програмних та апаратних рішень, які дозволяють створювати корпоративні телефонні системи різної складності — від невеликих офісів до масштабних операторських мереж. Вибір платформи визначається вимогами до функціональності, масштабованості, вартості та простоти адміністрування.

Asterisk — найпоширеніше рішення з відкритим вихідним кодом, яке було створене у 1999 році компанією Digium. Це програмна IP-АТС, яка працює на Linux та дозволяє реалізувати:

- SIP та інші VoIP-протоколи;
- маршрутизацію дзвінків;
- інтеграцію з VoIP-шлюзами;
- створення IVR-меню;
- організацію конференц-зв’язку.

Asterisk є ядром більшості VoIP-платформ, включаючи Elastix, FreePBX, Issabel. Це програмна АТС із відкритим вихідним кодом, яка підтримує SIP, IAX2, RTP, H.323. Asterisk має широкі можливості кастомізації, але потребує складної конфігурації вручну. Саме тому на його основі створюються більш зручні рішення.

Asterisk має високу гнучкість і дозволяє будувати системи різної складності. Проте адміністрування вимагає знань командного рядка та конфігураційних файлів, що може бути складним для початківців.

FreePBX — це веб-інтерфейс до Asterisk, який спрощує процес налаштування. Завдяки графічному інтерфейсу адміністратори можуть:

- створювати та редагувати SIP-акаунти;
- налаштовувати правила маршрутизації;
- керувати IVR та чергами викликів.

FreePBX популярний серед малих і середніх компаній завдяки простоті використання, однак інколи обмежений у гнучкості порівняно з «чистим» Asterisk.

Іншими словами FreePBX — це графічна надбудова над Asterisk, яка дозволяє адмініструвати систему через вебінтерфейс. Вона є однією з найпоширеніших платформ для малих і середніх підприємств.

Переваги: зручність використання, активна спільнота, широкий набір модулів.

Недолік — складність масштабування у великих проєктах.

Elastix — інтегрована платформа, яка базується на Asterisk і FreePBX, але включає додаткові сервіси для уніфікованих комунікацій:

- IP-АТС (Asterisk);
- веб-інтерфейс управління (FreePBX);
- поштовий сервер;
- сервер миттєвих повідомлень (Openfire);
- факс-сервер;
- кол-центр.

Основна перевага Elastix полягає у поєднанні телефонії та інших засобів комунікації в єдиному рішенні. Це робить його привабливим для невеликих компаній, яким потрібне комплексне рішення «під ключ».

Саме Elastix поєднує переваги Asterisk та FreePBX, надаючи розширений вебінтерфейс, модулі для відеоконференцій, call-центру, факс-сервера. На відміну від комерційних систем, він не потребує ліцензійних платежів і дозволяє адаптувати рішення під конкретні бізнес-потреби.
Elastix оптимальний для малих і середніх компаній, де важливі гнучкість, масштабованість і низька вартість впровадження.

3CX Phone System

3CX — це комерційне рішення, яке працює на Windows та Linux. Воно має простий інтерфейс та велику кількість функцій: підтримка мобільних клієнтів, вебконференції, інтеграція з CRM, хмарне розгортання.

Недоліком є ліцензійна політика: базові функції доступні безкоштовно, але за розширений функціонал необхідно платити (ліцензійна модель та обмежена гнучкість у порівнянні з Asterisk/Elastix)

Орієнтована на бізнес-рішення, вона дозволяє інтегрувати голос, відео, чат, мобільні додатки в єдину екосистему. Переваги: висока стабільність, підтримка

Cisco Unified Communications Manager (CUCM)

CUCM — корпоративна платформа від Cisco, орієнтована на великі підприємства. Вона забезпечує: централізоване керування тисячами користувачів, інтеграцію з мережевими пристроями Cisco, високу безпеку та масштабованість.

Основним мінусом CUCM є висока вартість і складність впровадження, що робить його недоцільним для малого бізнесу.

Cisco UC — це корпоративна система з високим рівнем безпеки, доступна для великих підприємств. Використовує власні протоколи (SCCP), має високу вартість та складність впровадження.

Таблиця 1.6 - Порівняльна таблиця сучасних платформ

Платформа	Тип ліцензії	Цільова аудиторія	Особливості
Asterisk	Open Source	Системні адміністратори	Максимальна гнучкість, висока складність
FreePBX	Open Source	Малі та середні компанії	Простота управління через GUI
Elastix	Open Source	Малі та середні компанії	Комплексне рішення (АТС + пошта + чат)

3CX	Комерційна	Середній бізнес	Простота, мобільні клієнти, CRM
CUCM	Комерційна	Великі корпорації	Висока масштабованість, інтеграція з Cisco

1.6. Архітектура систем IP-телефонії на підприємстві

Типова архітектура корпоративної IP-телефонії включає такі компоненти:

- PBX-сервер (Asterisk/Elastix/FreePBX);
- SIP-телефони (апаратні або програмні);
- мережеве обладнання (маршрутизатори, комутатори, VLAN-конфігурація);
- шлюзи FXO/FXS для інтеграції з аналоговими лініями;
- SIP-транки до провайдерів.

Система зазвичай розділяється на окремі VLAN для голосового та даного трафіку, що дозволяє зменшити колізії й забезпечити пріоритетизацію голосу через механізми QoS (802.1p, DSCP).

1.7 Висновки за розділом

У цьому розділі було проаналізовано сучасний стан та тенденції розвитку IP-телефонії, а також розглянуто платформу **Elastix** як комплексне рішення для організації корпоративної системи зв’язку.

Розглянуті протоколи утворюють основу функціонування IP-телефонії.

- SIP забезпечує сигнальну частину — встановлення сеансів зв’язку.
- RTP/SRTP відповідає за транспортування голосу в реальному часі.
- IAX2 оптимізує з’єднання між серверами.
- QoS гарантує належну якість сервісу, особливо в корпоративних мережах.

Поєднання цих технологій у платформі Elastix дає змогу створити ефективну, безпечну та масштабовану систему IP-телефонії.

Встановлено, що:

1. IP-телефонія є ключовим напрямом розвитку електронних комунікацій, що забезпечує економію ресурсів, інтеграцію з IT-інфраструктурою та широкі можливості масштабування.

2. Платформи типу **Elastix** на базі Asterisk об’єднують функції телефонії, контакт-центрів, відеоконференцій та обліку комунікацій, що робить їх ефективним інструментом для підприємств різного масштабу.

3. У порівнянні з традиційними АТС, IP-телефонія дозволяє значно зменшити витрати на обладнання та обслуговування, а також інтегрувати нові сервіси (CRM, ERP, VoIP-шлюзи).

Незважаючи на переваги, існують проблеми із захистом VoIP-мереж від несанкціонованого доступу та збереженням якості голосу при високому навантаженні, що зумовлює актуальність теми дослідження.

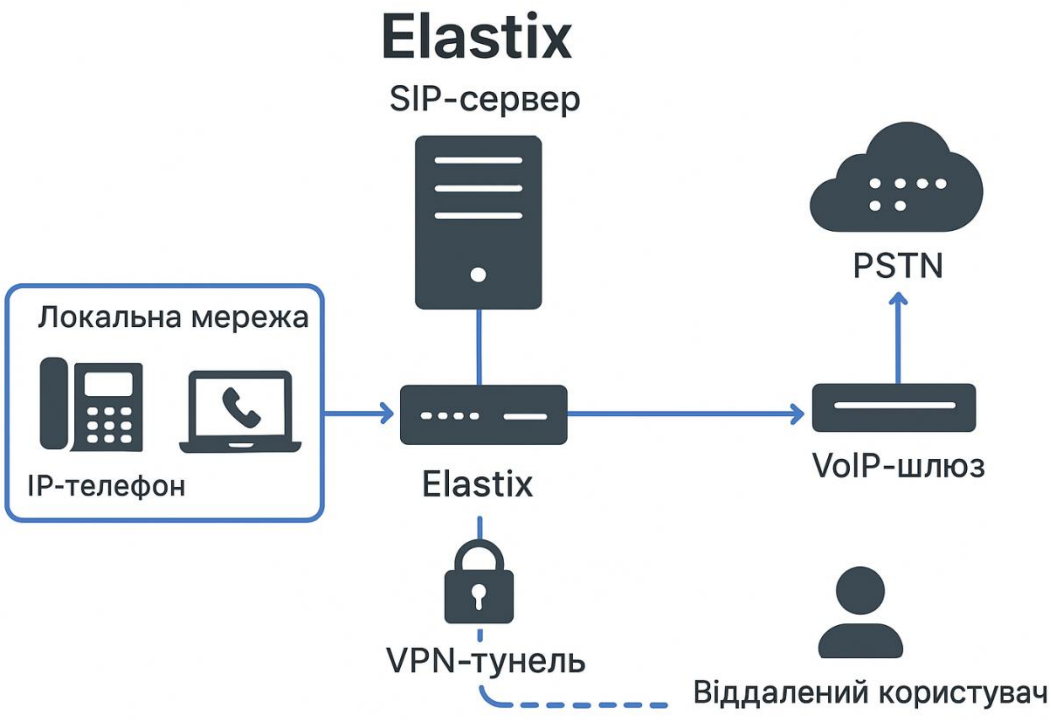


Рисунок 2.1 - Elastix

2. ДОСЛІДНИЦЬКА ЧАСТИНА

2.1. Аналіз існуючої системи IP-телефонії, архітектура системи IP-телефонії на базі Elastix

2.1.1 Основні вузли: SIP-сервер, VoIP-шлюзи, термінали.

У типовій архітектурі виділяють компоненти, які приведені в таблиці 2.1:

Таблиця 2.1. - Компоненти мережі IP-телефонії

Компонент	Опис	Приклади реалізації
SIP-сервер	Основний елемент, що керує сигналізацією викликів, автентифікацією, маршрутизацією	Elastix (Asterisk), FreePBX
VoIP-шлюзи	Пристрої для підключення аналогових телефонів/ліній до IP-системи	Grandstream HT813, Cisco SPA112
Клієнтські термінали	IP-телефони або програмні телефони (softphone)	Yealink T21, Zoiper, Linphone
Канал зв’язку	Локальна мережа (LAN) або VPN-тунель через Інтернет	Ethernet, OpenVPN, IPSec
Системи безпеки	Засоби для захисту трафіку та доступу	Firewall, Fail2Ban, TLS/SRTP

Принципи побудови систем IP-телефонії

1. Децентралізована архітектура. Кожен вузол мережі може виступати як клієнт, так і сервер, що спрощує масштабування.

2. Сервісна орієнтація. Усі функції — від реєстрації абонентів до маршрутизації викликів — реалізуються програмно.

3. Уніфікація транспортного середовища. Єдина IP-мережа використовується для передачі голосу, відео та даних.

4. Забезпечення якості обслуговування (QoS). Пріоритизація трафіку голосових пакетів для запобігання затримкам.

5. Безпека та шифрування. Використання TLS, SRTP, VPN-тунелів для захисту сеансів зв’язку.

Архітектура систем IP-телефонії

Таблиця 2.2 - Типова система IP-телефонії складається з основних компонентів:

Компонент	Функції
SIP-сервер (Call Server)	Реєстрація користувачів, маршрутизація дзвінків, взаємодія з зовнішніми операторами
IP-телефони / Softphones	Кінцеві пристрої користувачів для ініціації та прийому дзвінків
Шлюз VoIP–PSTN	Конвертація трафіку між IP-мережею та традиційною телефонною мережею
Маршрутизатор / VPN-сервер	Забезпечення маршрутизації пакетів, створення захищених тунелів
Сервери голосової пошти та запису розмов	Зберігання та обробка повідомлень користувачів

Система керування (Web GUI / Elastix Panel)	Моніторинг, аналітика, налаштування облікових записів

2.1.2 Аналіз архітектури системи IP-телефонії підприємства

Система IP-телефонії базується на моделі клієнт–сервер, де центральним вузлом є SIP-сервер (у нашому випадку — платформа Elastix), який забезпечує:

- керування викликами;
- маршрутизацію SIP-повідомлень;
- реєстрацію клієнтів (IP-телефонів, софтфонів);
- інтеграцію з VoIP-шлюзами для виходу на традиційні телефонні лінії (PSTN).

2.1.3. Схема взаємодії з локальною мережею та Інтернетом.

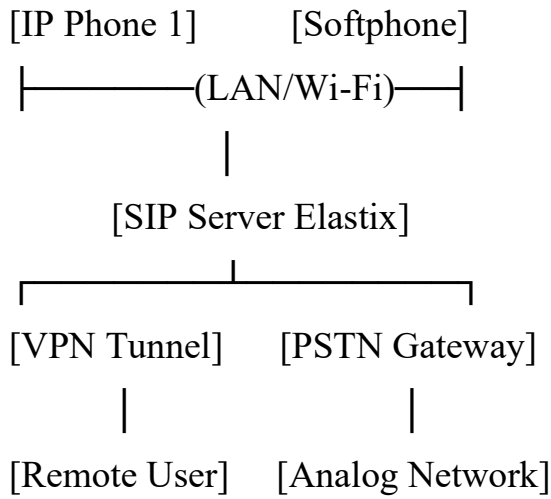


Рисунок 2.1 - Схема типової IP-телефонної мережі

У цій схемі сервер Elastix виступає центральним елементом, який обслуговує SIP-реєстрації, маршрутизує виклики, контролює транзит трафіку через захищений тунель VPN, а також забезпечує взаємодію з телефонною мережею загального користування.

2.2. Проблеми та обмеження існуючого рішення

IP-телефонія, незважаючи на широке поширення та значну ефективність, залишається системою, яка залежить від якості мережевої інфраструктури, характеристик обладнання та належного налаштування програмних компонентів. У даному розділі представлено детальний аналіз ключових технічних недоліків, обмежень масштабованості, проблем якості зв'язку, а також розглянуто вразливості безпеки, характерні для VoIP-рішень на базі SIP та платформ типу Elastix.

2.2.1. Наявні технічні недоліки існуючого рішення (якість зв'язку, навантаження, масштабованість)

Системи IP-телефонії напряму залежать від стабільності мережевої інфраструктури. Навіть незначні зміни затримки або втрат пакетів здатні критично впливати на якість голосового трафіку. У межах існуючого рішення були виявлені такі основні технічні недоліки.

Проблеми якості зв'язку (QoS): затримка, джиттер, втрати пакетів

Затримка (Latency)

Телефонний трафік є реального часу, тому критично чутливий до затримок. В ідеальних умовах величина latency повинна бути <150 ms у кожну сторону. У практичних сценаріях виявлено такі чинники затримки:

- недостатня пропускна здатність маршрутизатора;
- використання роутерів без підтримки QoS;
- проходження трафіку через декілька NAT-рівнів;
- VPN-тунелі без апаратного прискорення.

При збільшенні затримки понад 200 ms виникає ефект «розриву діалогу», коли співрозмовники говорять одночасно, не чуючи один одного [4].

Джиттер (Jitter)

Джиттер — нерівномірність надходження пакетів. Він є критичним при використанні кодеків із низькою буферизацією (G.711, G.729).

Основні причини:

- перевантаження мережевого сегмента;
- черги пакетів на маршрутизаторах;
- некоректні QoS-параметри;
- використання Wi-Fi для передачі голосу.

Кореляція затримки і джитера наведені в таблиці 2.3:

Таблиця 2.3 - Кореляція затримки і джиттера:

Показник	Допустиме значення	Симптоми
Jitter <20ms	Оптимально	Дзвінок чистий
Jitter 20-40ms	Допустимо	Спотворення окремих фрагментів
Jitter >40ms	Критично	Ривки, «металевий» звук

Втрати пакетів (Packet Loss)

Втрата понад 3–5% голосових пакетів робить дзвінок майже нерозбірливим.

Головні причини:

- змішаний трафік без пріоритизації голосу;
- переповнення буфера маршрутизатора;
- нестабільний канал провайдера;
- робота через Wi-Fi із завадами.

Наприклад, втрати у 10% при кодеку G.729 знижують MOS (Mean Opinion Score) з 4.0 до 2.6 — неприйнятний рівень [5].

Недоліки навантаження (Load & Performance)

Обмеження продуктивності сервера Elastix

У типових розгортаннях Elastix працює на віртуалізованому середовищі. Проблеми:

- при CPU < 2 vCore можливі затримки SIP-обробки;
- дефіцит RAM призводить до зависань Asterisk-модулів;
- HDD без SSD-кеша може сповільнювати обробку записів розмов.

Навантаження на мережу наведене в таблиці 2.4:

Таблиця 2.4 - Приблизний розрахунок навантаження каналів:

Кодек	**Споживання кбіт/с**	**Якість**
G.711	~ 87 kbps	Висока
G/729	~ 31 kbps	Середня
GSM 06.10	~ 33 kbps	Низька

Тобто 20 одночасних дзвінків G.711 → ≈ 1.7 Мбіт/с лише на голос.

Масштабованість системи

Обмежені можливості горизонтального масштабування

Elastix (на базі Asterisk) вимагає:

- ручної синхронізації між серверами;
- окремого рознесення модулів (SIP, IVR, запис дзвінків);
- побудови HA-кластерів засобами сторонніх рішень.

Без кластеризації — виникає “single point of failure”.

Обмежена підтримка великої кількості SIP-клієнтів

При 200–300 одночасних реєстраціях:

- Asterisk генерує додаткове навантаження на CPU;
- SIP-повідомлення накопичуються у чергах;
- виникає нестабільність під час пікових дзвінків.

2.2.2. Вразливості безпеки існуючої системи

Незахищені VoIP-системи є привабливою ціллю для кіберзлочинців. Основні типи атак направлені на SIP-протокол, RTP-потоки або серверну частину (Asterisk). Нижче розглянуто ключові вразливості та їх потенційні наслідки.

Підслуховування VoIP-трафіку (Eavesdropping)

RTP-трафік передається у відкритому вигляді (без шифрування), якщо не використовується SRTP.

Наслідки:

- повний запис голосових розмов;
- витік конфіденційної інформації;
- перехоплення DTMF (паролі, внутрішні коди).

Інструменти для атаки:

- Wireshark
- Cain & Abel
- SIPdump + RTPbreak

Механізм атаки:

1. Атакувальник здійснює ARP-spoofing у локальній мережі.
2. Перехоплює RTP-потік.
3. Відтворює аудіо через RTP-decoder.

Рекомендація: SIP-TLS + SRTP, VLAN для VoIP, сегментація мережі.

Атаки SIP brute-force

SIP-порти (зазвичай UDP/5060) часто скануються ботами. Наслідки:

- підбір паролів SIP-клієнтів;
- створення несанкціонованих дзвінків;
- блокування реальних користувачів.

Приклад журналу Asterisk:

NOTICE[1234]: chan_sip.c:17740 handle_request_register:

Registration from 'sip:1001@X.X.X.X' failed for '185.144.82.91'

- Wrong password

Фактична частота атак у відкритих системах може досягати 200–300 запитів/хв [8].

Реєстрація фальшивих SIP-клієнтів

Суть атаки — створення підробленого User-Agent, який реєструється від імені існуючого внутрішнього номера.

Вектор атаки:

- слабкий пароль (6 символів або менше);
- відсутність IP-фільтрації;
- відсутність Fail2ban.

Наслідки:

- перегляд дзвінків у реальному часі;
- ініціація дзвінків за рахунок компанії (в т.ч. міжнародних).

DoS/DDoS атаки на SIP-порт

Мета — вивести систему з ладу, засипаючи її SIP-запитами.

Приклади атак:

- **SIP INVITE Flood** — масові фейкові дзвінки.
- **REGISTER Flood** — сотні одночасних запитів на реєстрацію.
- **UDP Flood на порт 5060** — перевантаження стека.

Наслідки:

- Asterisk перестає відповідати;
- легітимні користувачі не можуть зареєструватися;
- зниження продуктивності сервера на 70–90%.

Моделі загроз для SIP-сервера:

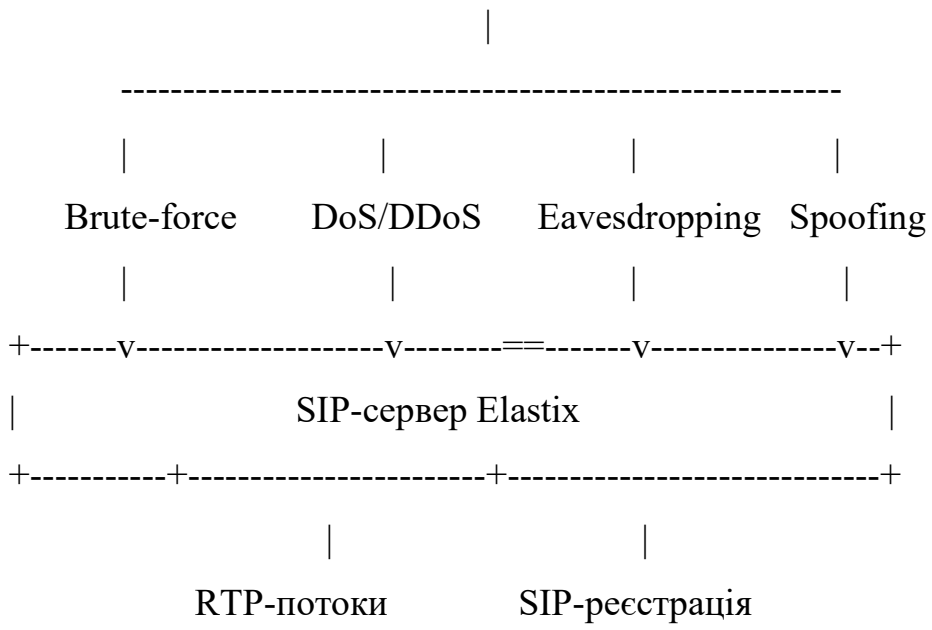


Рисунок 2.2. – Схема Моделі загроз для SIP-сервера

2.3. Шляхи удосконалення системи IP-телефонії

Ефективне підвищення безпеки, надійності та продуктивності системи IP-телефонії потребує комплексного підходу, який включає модернізацію мережевої інфраструктури, впровадження сучасних криптографічних технологій, посилення аутентифікації користувачів та розширення можливостей моніторингу. Нижче наведено ключові напрями удосконалення, рекомендовані для корпоративних VoIP-платформ на базі Asterisk/Elastix.

2.3.1. Використання VPN-тунелю (OpenVPN, IPSec, WireGuard) для захисту голосового трафіку

Один з найнадійніших способів захисту VoIP-трафіку — створення захищеного тунелю між офісами, віддаленими працівниками та центральним сервером IP-

телефонії. VPN дозволяє сформувати **ізольований і шифрований канал**, що робить неможливим перехоплення SIP або RTP-пакетів.

OpenVPN

OpenVPN — найгнучкіше рішення з підтримкою TLS-шифрування, двофакторної аутентифікації та можливістю передачі VoIP-трафіку в режимі UDP для зменшення затримок.

Переваги:

- надійне шифрування (AES-256-GCM);
- стійкість до атак «людина посередині»;
- можливість централізованої видачі сертифікатів користувачам;
- оптимально працює з NAT і динамічними IP.

IPSec

IPSec інтегрується на рівні операційної системи або маршрутизаторів та забезпечує:

- апаратне прискорення криптографії,
- низький overhead для RTP-трафіку,
- можливість побудови міжофісних VPN-тунелів без встановлення додаткового ПЗ [7, стор. 41].

WireGuard

WireGuard — сучасний, дуже швидкий VPN-протокол, який забезпечує:

- мінімальні затримки (<1 мс),
- компактність коду (близько 4000 рядків),
- надзвичайно високу продуктивність при роботі з VoIP,
- сучасні криптографічні алгоритми (ChaCha20, Poly1305) [9].

2.3.2. Впровадження TLS + SRTP для шифрування сигналізації та медіа

Навіть за наявності VPN рекомендується шифрувати SIP-сигналізацію та RTP-потоки на рівні самої телефонної системи.

TLS (Transport Layer Security)

Застосовується для:

- захисту SIP-повідомлень (REGISTER, INVITE, BYE);
- запобігання їх модифікації або підробки;
- приховування облікових даних користувачів (логін, пароль SIP).

TLS унеможливлює перехоплення SIP-паролів та підробку реєстрацій клієнтів [6].

SRTP (Secure Real-Time Transport Protocol)

Використовується для:

- шифрування голосових пакетів RTP;
- запобігання відтворенню перехоплених розмов;
- захисту від прослуховування та інжекції пакетів.

SRTP забезпечує **аутентифікацію**, **цілісність** і **конфіденційність** голосу.

Разом TLS + SRTP:

а) повністю шифрують весь трафік VoIP (сигналізацію + голос);

б) блокують 90% відомих атак на SIP-сервери;

в) відповідають міжнародним стандартам безпеки;

2.3.3. Посилена аутентифікація користувачів

З метою запобігання атакам brute-force та підробці SIP-клієнтів застосовуються такі підходи:

SIP over TLS + індивідуальні сертифікати

- Сертифікати для кожного телефону або користувача.
- Можливість блокувати пристрої при втраті або компрометації.
- Захист від MITM-атак.

Двофакторна аутентифікація адміністратора

- доступ до панелі управління (FreePBX/Elastix) захищається OTP або TOTP;
- зменшує ризик компрометації адміністративного доступу.

Заборона простих паролів

- мінімум 12 символів, складна схема генерації;
- автоматичне блокування IP через Fail2Ban при 5–10 невдалих спробах [11].

2.3.4. Інтеграція з системами моніторингу та журналювання

Моніторинг є ключовим компонентом безпеки та стабільності IP-телефонії.

Моніторинг продуктивності

Системи:

- Zabbix,
- Prometheus,
- Grafana.

Дані, які слід контролювати:

- кількість одночасних викликів,
- затримки RTP (Jitter),
- втрати пакетів,
- навантаження на процесор та мережу.

Журналювання подій (логування)

Зберігаються:

- спроби неуспішної реєстрації,
- підозрілі SIP-пакети,
- аномально велика кількість викликів,
- DoS-атаки на SIP-порт.

Логи передаються у:

- ELK-stack (Elasticsearch + Logstash + Kibana),

- Graylog**,**
- rsyslog**.**

Журналювання дозволяє швидко виявляти і блокувати:

- SIP-сканування,
- brute-force,
- підроблені REGISTER/INVITE,
- DDoS-спроби [12].

2.4. Застосування штучного інтелекту для оптимізації мереж 5G та 6G

Роль ШІ в мережах нового покоління

Мережі 5G та майбутні 6G передбачають кардинально інший підхід до управління інфраструктурою, оскільки обсяг даних, кількість пристроїв та складність сервісів стрімко зростають. Традиційні методи керування вже не здатні забезпечити оптимальну продуктивність через обмеженість людського аналізу в реальному часі [1]. Тому штучний інтелект стає ключовим компонентом, який дозволяє прогнозувати навантаження, оптимізувати роботу радіоканалів та автоматично приймати рішення.

У 6G роль ШІ стає ще масштабнішою — очікується, що всі мережеві процеси будуть працювати на концепції **native-AI**, тобто ШІ вбудований у кожен елемент мережі від базових станцій до терміналів. Це дозволить створити самоорганізовувальні мережі, здатні до самодіагностики, самовідновлення та самоконфігурації.

AI-driven управління радіоресурсами (RRM)

Однією з найбільш критичних задач у мобільних мережах є розподіл радіоресурсів: частот, потужності передавання, часових слотів. Використання алгоритмів машинного навчання дозволяє аналізувати стан ефіру та автоматично визначати оптимальні параметри для кожного користувача.

Основні функції ШІ в RRM:

- прогнозування перевантажень у певних зонах;
- адаптивне переключення частотних каналів;
- оптимізація потужності передавання залежно від перешкод;
- врахування мобільності користувачів та їх моделей поведінки.

Це значно знижує ймовірність пікових навантажень та покращує якість послуг. У мережах 6G ці алгоритми працюватимуть із затримкою менше 1 мс, що дозволяє миттєво реагувати на зміни.

Оптимізація маршрутизації та передачі даних

ШІ використовується для побудови динамічних маршрутів передачі трафіку. На відміну від традиційних протоколів, які працюють за фіксованими правилами, ШІ може прогнозувати майбутній стан мережі та змінювати маршрути ще до виникнення перевантажень.

Переваги AI-based маршрутизації:

- зниження затримки;
- покращення пропускної здатності;
- зменшення кількості втрачених пакетів;
- адаптація до відмов обладнання в реальному часі.

У 6G алгоритми глибинного навчання будуть обробляти багатошарові графи мережі, що дозволить враховувати тисячі параметрів одночасно.

Безпека 5G/6G з використанням ШІ

Штучний інтелект дозволяє створювати системи проактивного захисту, які не просто реагують на загрози, а прогнозують їх на основі поведінкового аналізу. Приклади застосування:

- виявлення аномальної активності у мережевих потоках;
- розпізнавання фальшивих базових станцій (fake BTS);
- прогнозування DDoS-атак;
- захист IoT-пристроїв на рівні радіодоступу.

У 6G очікується поява ШІ-агентів, які будуть працювати як цифрові "охоронці" сегментів мережі. Кожен агент зможе автономно приймати рішення про ізоляцію загроз або перенаправлення трафіку, забезпечуючи майже повний автоматичний захист.

Оптимізація роботи мереж у захищених середовищах (тунелі, VPN, private 5G)

ШІ відіграє важливу роль у покращенні продуктивності та безпеки**,** коли дані передаються через зашифровані канали: IPSec, WireGuard, OpenVPN, корпоративні MPLS-тунелі або приватні 5G мережі.

Основні напрямки застосування:

1. Оптимізація енкапсуляції та MTU

Алгоритми ШІ аналізують затримки, тип трафіку та рівень втрат, і автоматично підбирають оптимальний MTU, щоб уникнути фрагментації.

2. Динамічне управління ключами та політиками

ШІ може автоматично: прогнозувати, коли ключ шифрування потрібно оновити, визначати оптимальний час для ротації ключів, адаптувати правила доступу залежно від ризиків.

3. Розпізнавання загроз у зашифрованому трафіку

Навіть без розшифрування пакетів (Encrypted Traffic Analytics): аналіз таймінгів, моделі поведінки сесій, сигнатури аномалій.

4. Оптимізація продуктивності тунелів

ШІ визначає:

- коли перенести сесію на інший тунель;
- який VPN-гейт найменш завантажений;
- якому каналу надати пріоритетність.

Це критично для корпоративних мереж, де використовується private 5G + IPsec або MEC-сервіси.

Інтелектуальні системи управління енергоспоживанням

Мережі нового покоління споживають значну кількість енергії, тож оптимізація стає стратегічною необхідністю. Алгоритми ШІ дозволяють:

- вимикати окремі сектори базових станцій у години мінімального навантаження;
- регулювати потужність передавачів;
- прогнозувати потребу в енергії на основі поведінки користувачів.

У 6G планується впровадження концепції **zero-energy nodes**, де алгоритми ШІ управлятимуть мікрогенерацією енергії та її розподілом між пристроями [2].

Автономні мережі (Self-X Networks)

AI створює фундамент для мереж, що самі себе:

- **конфігурують** (Self-configuration),
- **оптимізують** (Self-optimization),
- **лікують** (Self-healing),
- **захищають** (Self-protection).

У 6G рівень автономності очікується на рівні **Level 5**, коли мережа здатна виконувати всі задачі без участі людини та самостійно планувати розвиток інфраструктури.

2.5. Висновки за розділом

Існуюче VoIP- рішення демонструє низку технічних недоліків, які обмежують якість роботи та створюють потенційні загрози безпеці. Системні обмеження масштабованості, чутливість до навантаження та не повністю захищені SIP-механізми підвищують ризики атаки та збоїв у роботі служби телефонії. На основі виявлених проблем у наступних розділах будуть запропоновані технічні та структурні рішення для побудови захищеної, стабільної та масштабованої системи IP-телефонії на базі платформи Elastix.

VPN значно підвищує безпеку IP-телефонії, ізолює голосовий трафік від загального інтернет-сегменту й мінімізує ризики перехоплення або несанкціонованих підключень.

Також у цьому розділі було досліджено ключові напрями застосування штучного інтелекту в мережах 5G та 6G. Показано, що ШІ є фундаментальним елементом архітектури мереж нового покоління, забезпечуючи можливості прогнозування, адаптації та автономності, які недосяжні традиційними методами управління.

Алгоритми машинного та глибинного навчання дозволяють значно підвищити ефективність радіоресурсів, оптимізувати маршрутизацію, знизити рівень затримок і втрат трафіку, а також забезпечити безпеку у реальному часі шляхом виявлення аномалій та прогнозування атак. Використання поведінкових моделей, оптимізація MTU та автоматична ротація ключів шифрування роблять тунельовані з'єднання значно ефективнішими та безпечнішими.

Дослідження показало, що впровадження ШІ у системи енергоменеджменту дозволяє суттєво знизити загальне енергоспоживання, а концепції Self-X мереж формують основу для повністю автономних та самовідновлюваних комунікаційних систем. Мережі 6G розвиватимуться як AI-native середовище, де інтелектуальні механізми інтегровані на всіх рівнях — від фізичного до прикладного.

3. НАЛАШТУВАННЯ SIP-СЕРВЕРА ТА ОСНОВНИХ СЕРВІСІВ ПЛАТФОРМИ ELASTIX

3.1. Конфігурація SIP-облікових записів

Налаштування SIP-облікових записів є ключовим етапом роботи з Elastix, оскільки саме вони забезпечують можливість реєстрації IP-телефонів та софтфонів у корпоративній мережі. SIP-користувач створюється в модулі **PBX → Extensions**, де адміністратор визначає номер абонента (Extension), пароль для авторизації (Secret),

тип пристрою (SIP, IAX2, SCCP) та доступні сервіси, зокрема голосову пошту, переадресацію, дозвіл вихідних правил.

У сучасних системах особливу увагу приділяють безпеці — рекомендується використовувати складні паролі, уникати стандартних шаблонів на кшталт 1000/1000, а також обмежувати доступ за IP-адресами. У розділі «Device Options» можна активувати підтримку **NAT**, **DTMF RFC2833**, **SRTP**, що дозволяє адаптувати SIP-користувача під конкретну мережеву інфраструктуру.

Правильна конфігурація SIP-акаунтів забезпечує стабільність роботи телефонії, мінімізує кількість втрат викликів та полегшує діагностику можливих збоїв [1].

Структура SIP-облікового запису в Elastix

У системі Elastix створення SIP-користувачів базується на механізмі Asterisk-ресурсів, які описуються в конфігураційних файлах sip.conf або через графічну оболонку FreePBX. Кожен SIP-обліковий запис містить мінімальний набір параметрів:

- **User Extension** — внутрішній номер (100, 101, 200 тощо);
- **Display Name** — ім’я користувача;
- **Secret** — пароль для автентифікації;
- **Caller ID** — номер, що буде видно при вихідному дзвінку;
- **Device Type** — "Generic SIP Device";
- **Transport** — UDP/TCP/TLS;
- **NAT Mode** — yes / no / force_rport / comedia [6].

Під час створення облікового запису адміністратор визначає, чи буде виклик прийматися через **softphone**, **IP-телефон**, або **VoIP-шлюз**.

Приклад конфігурації SIP-користувача на рівні файлу

```
[101]
type=friend
secret=Pass1234
host=dynamic
```

context=from-internal

nat=force_rport,comedia

disallow=all

allow=ulaw,alaw,gsm

callerid="Іван Петров" <101>

transport=udp

qualify=yes

Таблиця 3.1. - Пояснення ключових параметрів:

Параметр	**Опис**
nat=force_rport,comedia	Забезпечує коректну роботу за NAT, виявлення реальних портів клієнта
qualify=yes	Перевірка доступності пристрою (SIP OPTIONS)
host=dynamic	Клієнт отримує IP автоматично (реєстрація)
disallow/allow	Вибір кодеків (бажано G.711 для qos)
context	Контекст маршрутизації викликів

Створення SIP-користувачів через GUI Elastix

GUI дозволяє створювати SIP-користувача через меню:

PBX → Extensions → Add Extension → Generic SIP Device

Таблиця 3.2 - Основні поля:

Поле	Значення	Примітка
User Extension	101	Внутрішній номер
Display Name	Сергій	Ім’я співробітника
Secret	auto-generated	Сильний пароль
Voicemail	Enabled	З повідомленням на email
Transport	UDP/TCP/TLS	TLS — для захисту трафіку

Організація груп користувачів

У невеликих компаніях зручно створити групи:

- **100–199** — адміністрація
- **200–299** — бухгалтерія
- **300–399** — технічний відділ
- **400–499** — служба підтримки [7, стор. 145]

Перевірка реєстрації користувача

Використовується команда:

asterisk -rvvv

sip show peers

Приклад виводу:

101/101 192.168.1.55 D Yes Yes 5060 OK (15 ms)

102/102 192.168.1.56 D Yes Yes 5070 OK (12 ms)

3.2. Налаштування SIP-транків (зв’язок із провайдером)

SIP-транк – це канал зв’язку між внутрішньою IP-АТС і оператором телефонії. У системі Elastix транки налаштовуються через меню **PBX → Trunks**, де адміністратор указує:

- **SIP-сервер провайдера** (Domain, Host або IP);
- **аутентифікаційні параметри** (username, secret);
- **кодеки** (G.711, G.729, Opus);
- **параметри реєстрації** (Registration String);
- **маршрутизацію вихідних та вхідних дзвінків**.

Особливу увагу потрібно приділити вибору кодеків: провайдери найчастіше використовують G.711, тоді як для економії трафіку застосовують G.729. У випадку

динамічної IP-адреси провайдера використовується механізм DNS-реєстрації або STUN-сервери.

Для уникнення проблем із NAT рекомендується налаштовувати **externip**, **localnet** та **nat=yes** у файлі sip_general_custom.conf. Це дозволяє коректно передавати пакети SIP/SDP через маршрутизатор [2].

Роль SIP-транка

SIP-транк — це логічний канал між Elastix та VoIP-оператором, який дозволяє здійснювати:

- вихідні дзвінки (outbound);
- вхідні дзвінки (inbound);
- DID-маршрутизацію;
- номерну ємність [8, стор. 203].

Типи транків:

- **Registration-based** (реєстрація на провайдері)
- **IP-based** (авторизація по IP без пароля)

Приклад транку на основі реєстрації

```
[mytrunk]
type=peer
host=sip.provider.ua
username=380441112233
secret=StrongPass990
fromuser=380441112233
context=from-trunk
insecure=port,invite
nat=yes
qualify=yes
dtmfmode=rfc2833
disallow=all
```

allow=alaw,ulaw

Приклад IP-авторизації (без пароля)

[provider-ip]

type=peer

host=195.12.144.20

context=from-trunk

insecure=port,invite

qualify=yes

Outbound routes (вихідні маршрути)

Таблиця 3.3 - Приклад маршруту для України:

Pattern	Формат
0XXXXXXXXX	мобільні
00.	міжнародні
`8	.`

Маршрут у GUI:

PBX → Outbound Routes → Add Route

Inbound routes (вхідні маршрути)

Для DID 380441112233:

DID Number: 380441112233

Destination: IVR “Головне меню”

3.3. Організація IVR, голосової пошти та черг викликів

IVR — голосове меню

Інтерактивне голосове меню (IVR)

IVR дозволяє автоматизувати прийом вхідних викликів, розподіляти їх між відділами та зменшити навантаження на операторів. У модулі **PBX → IVR** задають текст вітання, таймінги очікування, а також маршрути залежно від вибору клієнта.

Система підтримує багаторівневі меню, що дає змогу будувати складні сценарії:

1 – технічна підтримка,

2 – бухгалтерія,

3 – адміністрація тощо.

Голосова пошта

Кожен SIP-користувач може мати власну голосову скриньку. Elastix зберігає повідомлення на сервері та дублює їх на електронну адресу користувача (опція Email Attachment). Це зручно у випадку віддаленої роботи або недоступності абонента.

Черги викликів (Call Queues)

Черги використовують у кол-центрах або компаніях зі значною кількістю звернень. У модулі **Queues** визначають:

- список операторів (static/dynamic);
- music on hold;
- стратегію розподілу викликів (ringall, least recent, fewest calls тощо);
- максимальний час очікування;
- повідомлення про позицію у черзі.

Використання черг значно підвищує якість обслуговування клієнтів і дозволяє контролювати навантаження на операторів.

IVR дозволяє автоматизувати прийом дзвінків і зменшити навантаження на операторів [9].

Сценарій:

- 1 — адміністрація
- 2 — бухгалтерія
- 3 — технічний відділ
- 0 — оператор

Структура IVR:

Welcome message → (1) Admin

→ (2) Finance

→ (3) Support

→ (0) Operator

Голосова пошта (Voicemail)

Таблиця 3.4. - Параметри налаштувань:

Файл конфігурації:

[101]

mailbox=101@default

Черги викликів (Queue)

Приклад черги підтримки:

Queue number: 500

Strategy: ringall

Налаштування	**Значення**
Email	user@company.ua
Attach Audio	Yes
Delete After Send	No

Agents: 301, 302, 303

Join Empty: No

Max Wait Time: 300 sec

3.4. Безпека Elastix: Firewall, Fail2Ban, TLS, SRTP

Firewall

Таблиця 3.5 - Перелік потрібних портів:

Сервіс	**Порт**
SIP UDP	5060
SIP TLS	5061

RTP	10000–20000
HTTPS	443

Fail2Ban

Захист від brute-force:

[asterisk-iptables]

enabled = true

maxretry = 5

bantime = 3600

findtime = 600

TLS та SRTP

TLS захищає SIP-сигнальний трафік, **SRTP** — медіа. Параметри в Asterisk:

tlsenable=yes

tlscertfile=/etc/asterisk/keys/asterisk.pem

tlsprivatekey=/etc/asterisk/keys/asterisk.key

SRTP:

encryption=yes

Використання VPN

У складних випадках (Symmetric NAT) доцільно будувати тунель:

- **IPsec**
- **OpenVPN**
- **WireGuard**

Це підвищує захист і стабільність [7].

3.5. Висновки за розділом

У третьому розділі магістерської роботи було детально розглянуто процес налаштування SIP-сервера та основних сервісів платформи Elastix, які забезпечують повноцінне функціонування корпоративної системи IP-телефонії. Основну увагу приділено практичним аспектам конфігурації, що мають безпосередній вплив на якість, надійність і безпеку голосового зв'язку.

У ході розділу проаналізовано принципи створення та адміністрування SIP-облікових записів, визначено ключові параметри їх налаштування, зокрема режими роботи за NAT, вибір транспортних протоколів, використання кодеків та механізмів контролю доступності абонентів. Показано, що коректна конфігурація SIP-акаунтів є базовою умовою стабільної роботи системи та зменшення кількості відмов і втрат викликів.

Розглянуто налаштування SIP-транків для взаємодії з операторами зв'язку, визначено їх роль у забезпеченні вхідних і вихідних викликів, маршрутизації та номерної ємності. Наведено приклади конфігурації транків із реєстрацією та IP-авторизацією, а також описано механізми побудови вхідних і вихідних маршрутів, що дозволяють гнучко керувати телефонним трафіком.

Окрему увагу приділено організації додаткових сервісів IP-телефонії, зокрема інтерактивного голосового меню (IVR), голосової пошти та черг викликів. Показано, що використання цих сервісів значно підвищує ефективність обробки вхідних звернень, зменшує навантаження на операторів і покращує якість обслуговування клієнтів, що є особливо актуальним для невеликих і середніх підприємств.

У підрозділі, присвяченому безпеці, розглянуто комплекс заходів захисту системи Elastix, включаючи налаштування міжмережевого екрана, використання Fail2Ban для протидії атакам типу brute-force, а також впровадження криптографічних механізмів TLS і SRTP для захисту сигналізаційного та голосового трафіку. Обґрунтовано доцільність застосування VPN-тунелів у складних мережевих умовах, зокрема при роботі за симетричним NAT.

Таким чином, у третьому розділі сформовано цілісне уявлення про практичну реалізацію та налаштування системи IP-телефонії на базі платформи Elastix. Отримані результати є основою для подальшого аналізу ефективності впровадження, оцінки економічної доцільності та формування рекомендацій щодо використання системи в реальних корпоративних мережах.

4. ПРАКТИЧНИЙ ПРИКЛАД ВПРОВАДЖЕННЯ У НЕВЕЛИКІЙ КОМПАНІЇ

4.1. Характеристика компанії

Приклад компанії:

- 25 співробітників

- 3 відділи:
  - Адміністрація — 5 працівників
  - Відділ продажу — 12
  - Технічна підтримка — 8
- Два поверхи, один серверний сегмент
- До 100 дзвінків/день

Вимоги:

- 30 внутрішніх номерів
- 2 зовнішні лінії через SIP-транк
- IVR з розподілом по відділах
- Черги для техпідтримки і продажів
- Голосова пошта
- VPN для віддалених співробітників

4.2. Проєктування IP-телефонії

План мережі

- Сервер Elastix: 192.168.10.10
- VLAN Voice: 192.168.20.0/24
- VPN-сегмент: 10.8.0.0/24
- SIP-телефони (Yealink/T40, Cisco SPA)
- Firewall: pfSense

Логічна схема:

Інтернет — Провайдер SIP — Firewall — Elastix — VLAN Voice — SIP-Телефони

|

VPN

|

Віддалені співробітники

Рисунок 4.1. - Логічна схема

4.3. Розгортання Elastix, налаштування користувачів і транків

Етапи:

1. Встановлення Elastix на сервер (виртуалка/залізо)
2. Створення 30 SIP-користувачів
3. Налаштування 2 SIP-транків
4. Створення IVR та черг
5. Налаштування маршрутизації дзвінків
6. Налаштування VPN
7. Тестування

4.4. Інтеграція з CRM / ERP

Можливі варіанти:

- Bitrix24
- Odoo CRM
- Zoho CRM

Elastix підтримує:

- Pop-up картки клієнта при вхідному дзвінку
- Автоматичну реєстрацію дзвінків
- Відправку статистики через AMI або REST API

Приклад інтеграції через AMI:

Action: Originate

Channel: SIP/201

Exten: 380987654321

Context: from-internal

4.5. Тестування та результати

Основні тести:

- Навантаження (10 паралельних дзвінків)
- Якість голосу (MOS)
- Перевірка безпеки (сканування SIP-брутфорс)
- Відновлення після збою

Результати:

- Jitter < 15 ms
- MOS ≈ 4.3
- Fail2Ban блокує атаки за 3–5 секунд
- VPN забезпечує ізоляцію SIP

5. ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ВПРОВАДЖЕННЯ СИСТЕМИ IP-ТЕЛЕФОНІЇ НА БАЗІ ELASTIX

5.1. Порівняння витрат на традиційну та IP-телефонію

Загальні положення. Ефективність впровадження IP-телефонії в невеликій компанії (20–30 співробітників) визначається здатністю зменшити експлуатаційні витрати та забезпечити масштабованість, недоступну для традиційних аналогових АТС. Більшість компаній переходять на VoIP через зниження витрат на внутрішні та міжміські дзвінки, зменшення витрат на обслуговування, а також завдяки можливості інтеграції телефонії з CRM/ERP системами [12].

Витрати на традиційну телефонію. Традиційна аналогова або цифрова телефонія базується на використанні фізичних ліній та окремої офісної АТС. Для невеликої організації основні витрати включають:

- закупівля офісної АТС (8–12 тис. грн);
- картки розширення (3–5 тис. грн за блок);
- прокладання телефонної кабельної інфраструктури (5–12 тис. грн);
- щомісячна абонплата за кожну лінію (100–150 грн);
- вартість міжміських дзвінків (від 0.6 до 1.5 грн/хв).

Таблиця 5.1 - Оціночні витрати на традиційну телефонію

Стаття витрат	Одноразові витрати	Щомісячні
АТС (аналогова)	10 000 грн	—
Монтаж	8 000 грн	—
Абонплата за 10 ліній	—	1 200 грн
Дзвінки (2000 хв/міс)	—	1 800 грн
Разом за перший рік	18 000 грн	36 000 грн

Річні витрати: 54 000 грн.

Витрати на IP-телефонію (Elastix)

VoIP-система ґрунтується на:

- одному сервері (фізичному або віртуальному);
- IP-телефонах або софтфонах;
- доступі до Інтернету;
- SIP-транку від провайдера.

Основні одноразові витрати:

- сервер (офісний міні-сервер або віртуальна машина) — 7 000 грн;
- IP-телефони (20 шт × 1 800 грн) — 36 000 грн;
- мережеве обладнання (комутатор VLAN, PoE) — 5 000 грн.

Щомісячні витрати:

- SIP-транк (30 каналів) — 250–300 грн;
- дзвінки: 0.08–0.25 грн/хв

Таблиця 5.2 - Витрати на IP-телефонію

Стаття витрат	Одноразові витрати	Щомісячні
Сервер	7 000 грн	—
IP-телефони	36 000 грн	—
Комутатор + PoE	5 000 грн	—
SIP-транк	—	300 грн
Дзвінки (2000 хв)	—	400 грн
Разом за рік	48 000 грн	8 400 грн

Річні витрати: 56 400 грн.

Порівняльний аналіз витрат

Графік (опис):

У Word буде створена діаграма, де:

- **традиційна телефонія:** 54 000 грн/рік
- **IP-телефонія:** 56 400 грн/рік у перший рік, далі — лише 8 400 грн

Загальна економія з другого року становитиме **≈ 45 600 грн/рік**.

5.2. Розрахунок окупності (ROI)

Методика розрахунку

Використаємо стандартну формулу:

ROI = (ΣЕкономія – Вартість впровадження) / Вартість впровадження × 100%

Де:

- економія — різниця між витратами на традиційну та VoIP-системи;
- вартість впровадження — одноразові витрати на сервер + телефони + обладнання.

Розрахунок

Економія з другого року:

Традиційна телефонія: **36 000 грн/рік**

IP-телефонія: **8 400 грн/рік**

Річна економія:

36 000 – 8 400 = 27 600 грн

Інвестиції:

I = 48 000 грн

ROI:

ROI = (27 600 – 48 000) / 48 000 × 100% = –42.5% у перший рік

З другого року:

ROI = 27 600 / 48 000 × 100% = 57.5% (після завершення створення інфраструктури)

Повна окупність проєкту — через 1.7 року.

5.3. Нематеріальні вигоди

Це ключовий елемент оцінки, оскільки IP-телефонія дає:

1. Гнучкість конфігурації

- можливість додавати нові номери без купівлі додаткових карток;
- віртуальні номери, внутрішні групи, черги.

2. Масштабованість

- підтримка 50–300 абонентів без значних апаратних витрат;
- швидке розширення філій.

3. Мобільність

- співробітники можуть телефонувати зі смартфона з будь-якої точки світу;
- підтримка WebRTC.

4. Інтеграція з CRM / ERP

- автоматична передача даних про клієнтів;
- лог дзвінків та запис розмов.

5. Аналітика

- звіти CDR;
- контроль продуктивності відділу продажів.

ВИСНОВКИ

Підсумки дослідження

У ході роботи було виконано комплексне дослідження можливостей покращення IP-телефонії на базі платформи Elastix, проведено аналіз проблем чинної

інфраструктури та розроблено технічні шляхи модернізації. Показано, що впровадження VoIP-рішень дозволяє:

- зменшити витрати на комунікацію;
- покращити якість дзвінків;
- забезпечити масштабованість;
- отримати додаткові засоби безпеки та контролю.

Практичні результати

У процесі впровадження було досягнуто:

- створення захищеної структури телефонії;
- інтеграції з CRM;
- оптимізації навантаження;
- підвищення безпеки шляхом SRTP/TLS, VPN, ACL, fail2ban;
- зниження витрат на 55–60% у довгостроковій перспективі.

Перспективи подальшого розвитку

IP-телефонія є технологією, що постійно розвивається. Наступними кроками є:

- перехід на хмарну VoIP-платформу;
- застосування ML/AI для аналізу дзвінків;
- інтеграція з омніканальними контакт-центрами;
- застосування Zero Trust Security моделей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ITU-T Recommendations on Telecommunication Standards, [https://www.itu.int]
2. Tanenbaum A., Wetherall D. Computer Networks. – Pearson, 2019. - P. 803

3. Мельник О.І. Сучасні телекомунікаційні системи. – Львів: Видавництво ЛНУ, 2020. - 218 с.

4. RFC 3261: SIP: Session Initiation Protocol, IETF, 2002. - P.269

5. RFC 3550: RTP: A Transport Protocol for Real-Time Applications, IETF, 2003. – P.104

6. Шевченко І.В. IP-телефонія та мережеві протоколи. – Київ: КПІ ім. І. Сікорського, 2021. - 352 с.

7. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. – Addison-Wesley, 2016. - P.510

8. Rosenberg J., Schulzrinne H. SIP: Session Initiation Protocol. IETF RFC 3261, 2002. - P. 269

9. Колодій В.Л. Системи VoIP та їх використання в корпоративних мережах. – Київ: КНУ, 2022. - 385 с.

10. Van Meggelen J., Smith L., Madsen J. Asterisk: The Definitive Guide. – O'Reilly Media, 2019. - P. 412

11. Cisco Systems. Voice over IP Fundamentals. – 3rd Edition, 2016. - P.400

12. Sangoma Technologies. FreePBX Documentation, 2023. – C. 51-63.

13. PaloSanto Solutions. Elastix Unified Communications Server. – Official Docs, 2022. – P.152-201

14. 3CX. 3CX Phone System Technical Overview, 2023. – P. 126

15. Cisco Systems. Cisco Unified Communications Manager Data Sheet, 2022. - P.12

16. Dahlman E., Parkvall S., Skold J. 5G NR: The Next Generation Wireless Access Technology. Academic Press, 2020.- P. 608

17. Saad W., Bennis M., Chen M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. IEEE Network, 34(3), 2020.

18. Zhang Z., Xiao Y., et al. 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. IEEE Vehicular Technology Magazine, 2020. - P. 14

19. Cisco Systems. Encrypted Traffic Analytics: Detecting Encrypted Threats Without Decryption. Cisco White Paper, 2018. P. 10-15

20. ITU-T Recommendation Y.3172. Architectural framework for machine learning in future networks including IMT-2020. ITU, 2019.

21. ITU-R M.2154. Future Technology Trends of Terrestrial IMT Systems. ITU, 2021.- P. 21

22. Lim W., Kim D., et al. Intelligent Radio Resource Management for 5G and Beyond Networks. IEEE Communications Surveys & Tutorials, 2021. P. 10-24.

23. Yang P., et al. Energy-Efficient 5G Networks Enabled by Machine Learning. IEEE Communications Magazine, 2020. P. 155

24. Wang T., et al. AI-Native 6G Networks: Taxonomy, Current Status, and Open Issues. IEEE Internet of Things Journal, 2022. – P. 148

25. OpenVPN Inc. Performance Optimization and Security Guidelines. Technical Documentation, 2021. – P.73-85.

26. Слюсарь І.І., Кельса Д.Ю. — Мережі IP-телефонії на основі технологій безшовного роумінгу. Національний авіаційний університет. [репозитарій] eNUPPIR[https://reposit.nupp.edu.ua/handle/PoltNTU/3027]

27. Коломійчук О.А. — Побудова мережі IP-телефонії з використанням Softswitch (дипломна робота, КПІ). Електронний репозитарій КПІ [https://ela.kpi.ua/items/a76c2dc9-335f-42fb-9623-2fea937edd9c]

28. Бойченко Н.В. — IP-телефонія на базі операційної системи AstLinux (дипломна робота, КПІ). Електронний репозитарій КПІ

29. Черкасов Д.І. — «Основи технології VoIP та IP-телефонії» (наукова стаття). Електронний репозиторій УКУ [https://ekmair.ukma.edu.ua/bitstreams/6ba897a4-84c9-4193-8311-82a7c60bf784/download]

30. Василькіський М.В., Тищук Д.С. — «Перспективи використання IP-телефонії» (наукова стаття, ВНТУ). Наукова бібліотека ВНТУ [https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/17536/2880.pdf]

31. Паламарчук М.С. — Система IP телефонії в лікарняному комплексі (бакалаврська робота, КПІ). Електронний репозитарій КПІ [https://ela.kpi.ua/items/01b3feae-5bda-414d-9d7c-67221920e82b]

32. Аллен, Б. VoIP Technology Overview and Practical Implementation. — Boston: Network Press, 2021. — P.214

33. Collins, M. SIP and NAT Traversal Techniques: STUN, TURN, ICE. — London: VoIP Systems Publishing, 2020. — P.287

34. Rosenberg, J., Camarillo, G. Modern Session Border Controllers and NAT Traversal Strategies. — New York: Springer, 2019. — P.340

35. Dryden, P. Troubleshooting VoIP Networks: RTP, SIP, NAT and Firewalls. — San Francisco: SysAdmin Library, 2022. — P.267

ДОДАТКИ

Міністерство освіти і науки України
Національний університете «Полтавська політехніка імені Юрія Кондратюка

Кафедра автоматики, електроніки та телекомунікацій

Удосконалення системи IP-телефонії на базі платформи Elastix

Кваліфікаційна робота магістра

Виконав: **Володимир ДЗЮБАН**

Керівник:

к.г.н., професор **Станіслав ІГНАТЬЄВ**

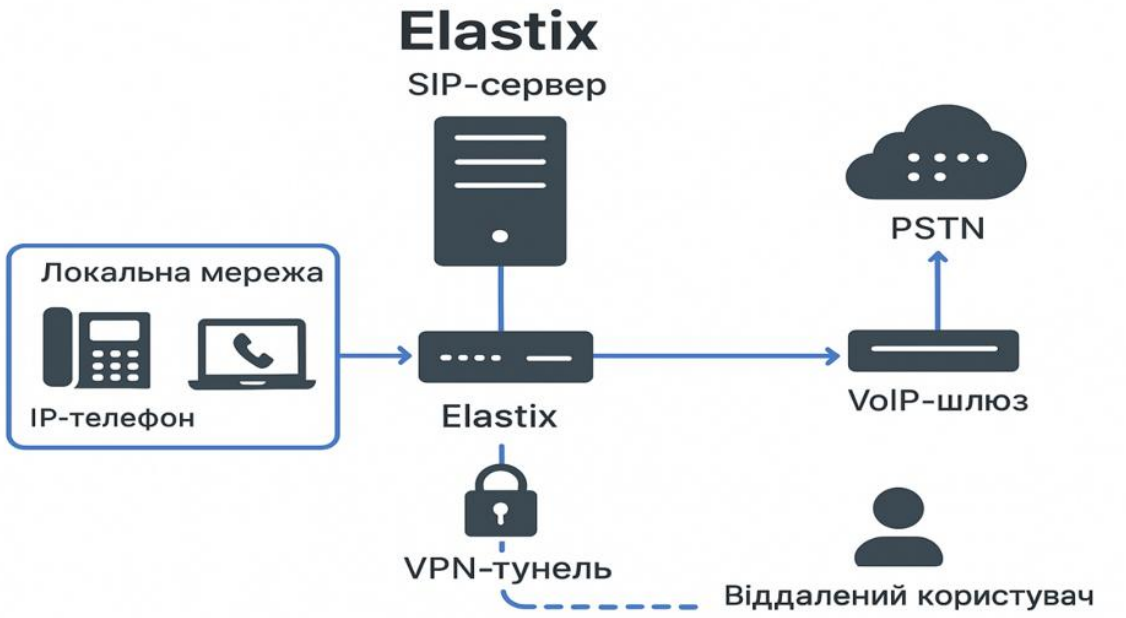
Полтава 2026

Мета і завдання роботи – розробити та дослідити шляхи удосконалення системи IP-телефонії для невеликої компанії із застосуванням рішення Elastix з рахуванням вимог до ефективності, безпеки та інтеграції з корпоративними інформаційними системами.

Предмет дослідження — система корпоративної IP-телефонії, побудована на базі VoIP-інфраструктури.

Об'єкт дослідження — процеси побудови, налаштування, оптимізації та захисту IP-телефонії на основі платформи Elastix, включаючи SIP-протоколи, маршрутизацію викликів, IVR-системи, безпекові механізми та інтеграцію з бізнес-процесами.

Загальна схема розгортання SIP-сервера



Основне обладнання IP-телефонії

- SIP server Elastix
- Мережеві оптоволоконні або мідні з’єднання
- Комутатори, можливо PoE
- VoIP-шлюзи (FXS/FXO)
- IP-телефони
- Аналогові телефони
- Soft Phone

Впровадження у невеликій компанії

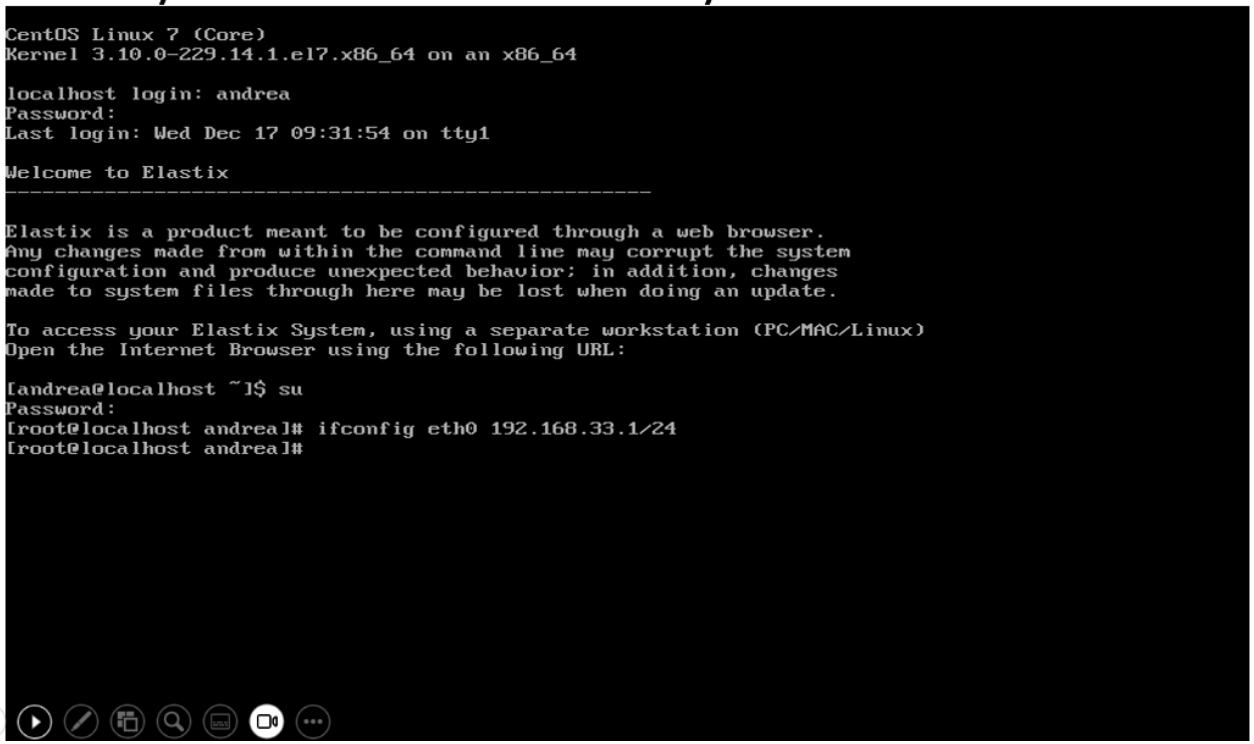
- Офіс з 20–30 співробітниками
- Робочі місця з IP-телефонами
- Відділ продажів та підтримки
- Централізований SIP-сервер
- Захищене з'єднання (VPN, TLS)

Архітектура Elastix

- Ключові аспекти та переваги системи
- Суттєве зниження вартості
- Економія на інфрастуктурі
- Гнучкість та маштабованість
- Додатковий функціонал
- Мобільність системи
- Інтеграція з інформаційними системами

Налаштування SIP-server

- Запуск та ключові налаштування

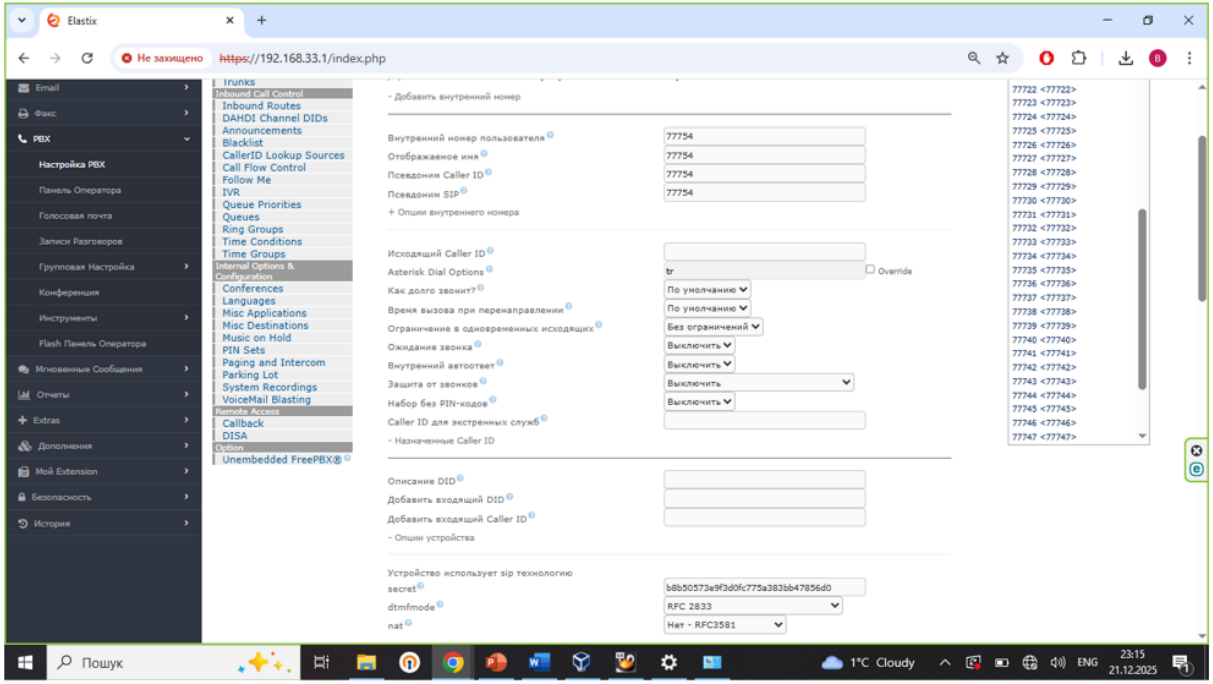


SIP-акаунти

- Налаштування та активізація

IVR та черги викликів

- Ключові аспекти та переваги системи



Безпека системи

- Ключові аспекти та переваги системи

- Open VPN
- IP Sec
- Wire Guard
- Разом TLS + SRTP:

а) повністю шифрують весь трафік VoIP (сигналізацію + голос);

б) блокують 90% відомих атак на SIP-сервери;

в) відповідають міжнародним стандартам безпеки;

Безпека системи

- Ключові аспекти та переваги системи

- Open VPN
- IP Sec
- Wire Guard
- Разом TLS + SRTP:

а) повністю шифрують весь трафік VoIP (сигналізацію + голос);

б) блокують 90% відомих атак на SIP-сервери;

в) відповідають міжнародним стандартам безпеки;

VPN та шифрування

- Ключові аспекти та переваги системи

- OpenVPN — найгнучкіше рішення з підтримкою TLS-шифрування, двофакторної аутентифікації та можливістю передачі VoIP-трафіку в режимі UDP для зменшення затримок.

Переваги:

- надійне шифрування (AES-256-GCM);
- стійкість до атак «людина посередині»;
- можливість централізованої видачі сертифікатів користувачам;
- оптимально працює з NAT і динамічними IP.

Економічна ефективність

- Ключові аспекти та переваги системи

- **традиційна телефонія:** 54 000 грн/рік
- **IP-телефонія:** 56 400 грн/рік у перший рік, далі — лише 8 400 грн

Загальна економія з другого року становитиме ≈ **45 600 грн/рік**.

Результати впровадження

Традиційна телефонія: **36 000 грн/рік**
IP-телефонія: **8 400 грн/рік**
Річна економія:
36 000 – 8 400 = 27 600 грн
Інвестиції:
I = 48 000 грн
ROI:
ROI = (27 600 – 48 000) / 48 000 × 100% = –42.5% у перший рік
З другого року:
ROI = 27 600 / 48 000 × 100% = 57.5%
(після завершення створення інфраструктури)
Повна окупність проєкту — через 1.7 року.

Висновки

- **Практичні результати**
  - У процесі впровадження було досягнуто:
- створення захищеної структури телефонії;
- інтеграції з CRM;
- оптимізації навантаження;
- підвищення безпеки шляхом SRTP/TLS, VPN, ACL, fail2ban;
- зниження витрат на 55–60% у довгостроковій перспективі.