Міністерство освіти і науки України
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

Розводовський Назар Володимирович

«Алгоритми підвищення інформаційної безпеки IP-телефонії на основі протоколів розподілених ключів / Algorithms to increase information security of IP-telephony on the basis of distributed key protocols»

Студент групи КІм – 21
Розводовський Назар Володимирович
_____

Науковий керівник
к.т.н., доцент, І.Р. Паздрій
_____

Тернопіль – 2020

РЕЗЮМЕ

Кваліфікаційна робота на тему «Алгоритми підвищення інформаційної безпеки IP-телефонії на основі протоколів розподілених ключів.» зі спеціальності 123 Комп'ютерна інженерія освітнього ступеня магістр має обсяг 84 сторінки, та містить 57 рисунків, 3 таблиці, 2 додатки, та 50 джерел.

Метою випускної кваліфікаційної роботи є визначення меж ефективного стиснення мовленнєвої інформації при реалізації технології передачі і захисту в IP-телефонії.

Методи дослідження: методи та алгоритми машинного навчання.

Було досліджено телефонну мережу, що виконано за технологією SIP.

Проаналізовано методи для оптимізації перетворення голосового сигналу в цифровий та протоколи захисту IP-телефонії. Розглянуто сучасні телефонні системи та основні типології IP-телефонії.

Обрані найбільш оптимальні налаштування для встановлення та перевірки серверу Asterisk. Налаштовано логіку обробки дзвінків, створено голосове меню для умовного підприємства. Підключено базу даних MySQL для деталізованх звітів про виклики.

Можливими напрямками подальших досліджень є розробка ефективних засобів безпеки телефонії, з оновленням програмного забезпечення для зв’язку.

КЛЮЧОВІ СЛОВА: IP-ТЕЛЕФОНІЯ, ТЕЛЕФОННІ СИСТЕМИ, VOIP, ПРОТОКОЛИ ЗАХИСТУ, СТАНДАРТИ ЗАХИСТУ МСЕ-Т, КОДЕК.

RESUME

Qualification work on «Algorithms to increase information security of IP-telephony on the basis of distributed key protocols». Dedicated to the specialty 123 Computer Engineering degrees magister has a volume of 84 pages, and contains 57 figures, 3 tables, 2 appendixes and 50 references.

The aim of the release kvalifikatsinoyiyno work is to identify between efektivnoe stiffening of speech information in the implementation of technology transfer and protection in the IP-telephony.

Research methods: methods and algorithms of machine learning.

The telephone network was investigated, which was done with SIP technology.

Analyzed methods for optimizing the conversion of voice signals into digital and protocols for the protection of IP-telephony. Examined modern phone systems and the main typologies of IP-telephony.

Obrenovated the most optimal settings for installing and checking the server Asterisk. Settings logics of processing calls, created a voice menu for the enterprises. Included MySQL database for detailed records of incoming calls.

Possible areas of further research is to develop effective means of telephone security, with the updating of software for the connection.

KEY WORDS: IP-TELEPHONY, TELEPHONE SYSTEMS, VOIP, PROTECTION PROTOCOLS, STANDARDS OF MSCT PROTECTION, CODEC.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасне життя надає не лише нові технології, але й диктує нові підходи до класичних, усталених роками. Для багатьох сучасних прикладних аспектів людської взаємодії кінцевим пристроєм абонентського доступу є персональний комп'ютер, тому IP-телефонія може вважатися більш зручним інструментом для цього. Водночас ця технологія є більш гнучкою при реалізації ефективних алгоритмів захисту інформації, що дозволяє її використовувати і в сфері бізнесу і в інших додатках. Тому дослідження в галузі передачі та захисту інформації в IP-телефонії є актуальним.

Сучасному періоду розвитку телекомунікацій відповідають зростаючі об'єми трафіку в корпоративних мережах. IP-телефонією називають технологію передавання мовлення на базі протоколу IP. Причина розвитку та поширення IP-телефонії послугувала низька вартість порівняно з аналоговою телефонією, а також, універсальність, мобільність, що дозволяє перетворювати мовлення в потім даних в будь-якій точці мережевої інфраструктури.

Стандартизація протоколів, а також поширене використання персональних комп'ютерів в якості терміналів користувача послуг IP-телефонії привели до розробки великої кількості програм для IP-телефонії в тому числі програмного забезпечення з відкритим кодом, що дозволяє розширювати можливості і використовувати додаткові алгоритми в програмах.

Мета і задачі дослідження. Мета даної роботи – визначення меж ефективного стиснення мовленнєвої інформації при реалізації технології передачі і захисту в IP-телефонії.

Для досягнення цієї мети в роботі необхідно вирішити наступні завдання:

– проаналізувати роботу кодеків в IP-телефонії по алгоритмам стиснення мовленнєвої інформації;

– аналізувати побудова мереж Інтернет-зв'язку;

– виявляти типи загроз в IP-телефонії і визначати методи боротьби з ними;

Об’єктом дослідження є процес передачі мовного сигналу з використанням технології IP-телефонії в умовах забезпечення заданого ступеня конфіденційності.

Предметом дослідження є телефонна мережа, виконана за технологією VoIP на базі протоколу SIP.

Наукова новизна одержаних результатів. В результаті виконання даної випускної кваліфікаційної роботи було розглянуто основні принципи IP-телефонії та протоколи захисту IP-телефонії,

Практичне значення одержаних результатів. Дослідження IP-телефонії показали, що параметри передачі мовного сигналу(кодеки) суттєво впливають на вибір методів її захисту.

Апробація результатів роботи. Публікації та апробація випускної кваліфікаційної роботи. Отримані результати апробовані в межах III науково-практичної конференції молодих вчених і студентів «Інтелектуальні комп’ютерні системи та мережі» Західноукраїнського національного університету та опубліковано дві тези доповіді по темі роботи [1,2].

1 ЗАГАЛЬНІ ПРИНЦИПИ ПОБУДОВИ МЕРЕЖІ ІНТЕРНЕТ ТА IP-ПРОТОКОЛІВ

1.1 VoIP та IP-протоколи

VoIP – система зв'язку, що передає голосовий сигнал через інтернет або будь-яку іншу IP-мережу. Сигнал по каналу зв'язку передається в цифровому вигляді і, як правило, перед передачею перетворюється (стискується) для видалення надмірності. Раніше оператори насторожено ставилися до використання IP-телефонії, вважаючи рівень безпеки таких мереж низьким. Вже сьогодні можна сказати, що IP-телефонія стала певним стандартом телефонного зв'язку. Це пов'язано із зручністю, відносної надійністю і відносно невисокою вартістю IP-телефонії в порівнянні з аналоговим зв'язком. Можна стверджувати, що IP-телефонія підвищує ефективність ведення бізнесу і дозволяє виконувати раніше недоступні операції, такі як інтеграція з різними бізнес-додатками. Якщо говорити про недоліки і слабкі місця IP-телефонії, то в першу чергу слід відзначити ті ж недоліки, що і у інших сервісів, що використовують протокол IP. Це сприйнятливість до вірусних атак, DoS-атак, несанкціонованого віддаленого доступу і так далі. Хоча при побудові інфраструктури IP-телефонії ця послуга зазвичай відділяється від сегментів мережі, що не містять голосових даних, це не є гарантією безпеки. Сьогодні велика кількість компаній інтегрують IP-телефонію з іншими додатками, такими як електронна пошта. З одного боку, це створює додаткові переваги, а з іншого – нові уразливості. Серед основних загроз IP-телефонної мережі:

– реєстрація чужого терміналу, що дозволяє здійснювати дзвінки за чужий рахунок;

– заміна абонента;

– внесення змін до голосової або сигнальний трафік;

– зниження якості голосового трафіку;

– перенаправлення голосового або сигнального трафіку;

– перехоплення голосового або сигнального трафіку;

– підробка голосових повідомлень;

– завершення сеансу зв'язку;

– відмова в обслуговуванні;

– віддалений несанкціонований доступ до компонентів інфраструктури IP-телефонії;

– несанкціоноване оновлення ПЗ на IP-телефонії (наприклад, з метою впровадження троянської або шпигунської програми);

– взлом білінгової системи (для операторської телефонії).

IP-телефонія – це найпростіший спосіб реалізувати ряд послуг, включаючи передачу даних і відео по IP. Таким чином, IP-телефонія – це майбутнє мережі загального користування і, відповідно, її необхідно підтримувати і розвивати.

Існує величезна кількість інформації про Інтернет-технологіях і використовуваному в них IP-протоколі, як в Інтернеті, так і в друкованих ЗМІ. Нижче наведені лише основні концепції, необхідні для розуміння можливостей використання Інтернету та протоколу IP для передачі голосових повідомлень. Точне визначення терміна «Інтернет» було дано в жовтні 1995 року FNC (Federal Networking Counsil) в такій формі: Інтернет є частиною глобальної інформаційної системи, яка:

– логічно пов'язана унітарним адресним простором, заснованому на IP-протоколі або на його перспективних розширеннях/послідовниках;

– може підтримувати комунікації, використовуючи Transmission Control Protocol/Internet Protocol(TCP/IP) або його розширення/послідовники і/або IP-сумісні протоколи;

– надає, використовує або робить доступними (для всіх або конфіденційно) сервіси високого рівня, засновані на комунікаціях і пов'язаної з ними інфраструктури.

Творці технології Інтернет виходили з двох основоположних міркувань:

– неможливо створити єдину фізичну мережу, яка дозволить задовольняти потреби всіх користувачів;

– користувачам потрібен універсальний спосіб для встановлення з’єднання один з одним.

У кожній фізичній мережі підключені до неї комп'ютери використовують ту чи іншу технологію (Ethernet, Token Ring, FDDI, ISDN, з'єднання точка-точка, а недавно в цей список були додані мережу ATM і навіть бездротові технології). Між механізмами зв'язку, залежними від даних фізичних мереж і прикладних систем, вбудовано нове програмне забезпечення, яке забезпечує з'єднання різних фізичних мереж один з одним. Деталі цього підключення є «прихованими» користувачами, і вони можуть працювати в одній великій фізичної мережі. Такий спосіб з'єднання безлічі фізичних мереж в єдине ціле називається Інтернет-технологією, на основі якої реалізується однойменний Інтернет. Базовий протокол, на якому побудований Інтернет, називається інтернет-протоколом або IP-протоколом.

Для підключення двох або більше мереж в Інтернеті використовуються маршрутизатори – комп’ютери, які фізично з’єднують мережі між собою і за допомогою спеціального програмного забезпечення передають пакети з однієї мережі в іншу. Інтернет-технології не нав'язують жодної конкретної топології взаємозв'язку. Додавання нової мережі до інтернету не означає підключення її до якоїсь центральної точки комутації або встановлення прямих фізичних зв’язків з усіма, що вже є частиною Інтернету. Маршрутизатор «знає» топологію кадрування Інтернету між технічними фізичними системами, які пов'язані, і на основі адрес фенестрації, передаючи пакет з того чи іншого маршруту. Інтернет використовує універсальні ідентифікатори комп'ютерів (адрес), підключених до нього, тому будь-які дві машини мають можливість взаємодіяти один з одним. Принцип незалежності призначеного для користувача інтерфейсу від фізичної мережі також повинен бути реалізований в інтернеті, тобто повинно бути безліч способів встановлення з'єднань і передачі даних для всіх фізичних мережних

технологій. Інтернет приховує деталі здійснювати підключення до мережі, тому з точки зору кінцевих користувачів і по відношенню до додатків Інтернет – єдина віртуальна мережа, до якої підключені всі комп'ютери, незалежно від їх реальних фізичних підключень (рисунок 1.1). На кожному комп'ютері має бути встановлено програмне забезпечення для доступу в Інтернет, що дозволяє додаткам використовувати Інтернет як єдину фізичну мережу. Основоположним принципом Інтернету є еквівалентність всіх об'єднаних їм фізичних мереж: будь-яка система зв'язку розглядається як компонент Інтернету, незалежно від її фізичних параметрів, розміру переданих пакетів даних і географічного масштабу. Універсальний інтернет заснований на сімействі протоколів TCP/IP і включає протоколи 4-х рівнів зв'язку. Рівень мережевого інтерфейсу відповідає за встановлення мережевого з'єднання в певній фізичної мережі - компонентах Інтернету, до яких підключений комп'ютер. На цьому рівні працюють драйвер пристрою в операційній системі і відповідна мережева карта комп'ютера. Чотири рівня стека протоколів TCP/IP:

– прикладний Telnet, FTP, E-mail і т.д;

– транспортний TCP, VDP;

– мережевий IP, ICMP, IGMP;

– мережевий інтерфейс драйвер пристрою і мережева плата.

Мережевий рівень – основа стека протоколів. Саме на цьому рівні реалізується принцип міжмережевого з'єднання, зокрема маршрутизація пакетів по мережі Інтернет.

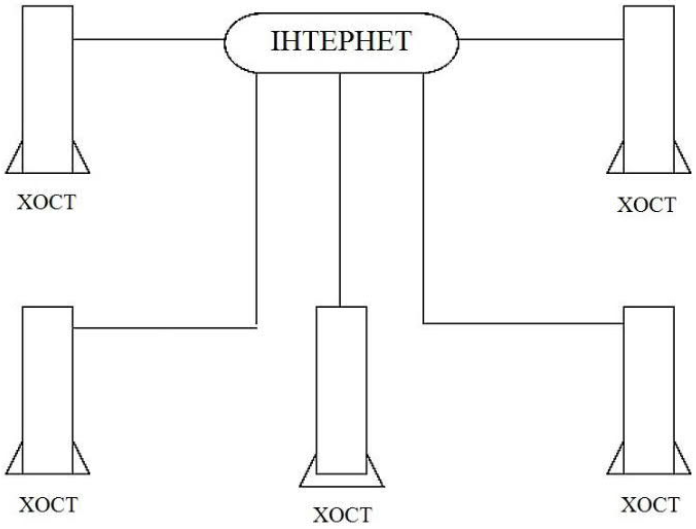

Рисунок 1.1 – Мережа Інтернет з погляду користувача

IP-протокол – це базовий протокол мережевого рівня, що дозволяє встановлювати з'єднання. Він використовується обома протоколами транспортного рівня – TCP і UDP. Протокол IP визначає базову одиницю передачі даних в Інтернеті – IP-дейтаграмму, що вказує точний формат всієї інформації, що проходить через мережу TCP/IP. Програмне забезпечення рівня IP виконує функції маршрутизації, вибираючи шлях даних для фізичних мережевих підключень. Підтримуються спеціальні таблиці для визначення маршруту; вибір здійснюється на основі мережевого адреси, до якого підключений кінцевий комп'ютер. Протокол IP визначає маршрут окремо для кожного пакету даних, що не гарантує надійної доставки в бажаному порядку. Він встановлює пряме відображення даних на більш низький фізичний рівень передачі і, таким чином, реалізує високоефективну доставку пакетів. На мережевому рівні протокол IP реалізує ненадійну службу доставки пакетів від системи до системи без встановлення з'єднання (служба доставки пакетів без встановлення з'єднання). Це означає, що все, що вам потрібно для доставки посилок, буде зроблено, але ця доставка не гарантовано. Пакети можуть губитися, передаватися неправильно, дублюватися і так далі. Протокол IP не гарантує надійність зв'язку. Немає ніякого механізму аутентифікації між відправником і отримувачем або між хост-комп'ютерами. Немає контролю

помилок для поля даних, тільки контрольна сума для заголовка. Також не підтримується повторна передача, немає управління потоком. Про виявлені помилки можна повідомляти за допомогою протоколу ICMP (Internet Control Message Protocol). Надійна передача даних реалізує наступний рівень, транспорт, на якому два основні протоколи, TCP і UDP, обмінюються даними між машиною, що відправляє пакети, і машиною призначення. Рівень додатки - це клієнт-серверний додаток, засноване на протоколах нижчого рівня. На відміну від протоколів трьох інших рівнів, протоколи прикладного рівня мають справу з деталями конкретного додатка і «не цікавляться» тим, як дані передаються по мережі. Серед основних додатків TCP/IP, доступних майже у всіх реалізаціях: протокол емуляції терміналу Telnet, протокол передачі файлів FTP, протокол електронної пошти SMTP, протокол управління мережею SNMP, який використовується в протоколі передачі гіпертексту HTTP у всесвітній павутині (WWW) і так далі оскільки деталі фізичних підключень приховані від додатків в Інтернеті, рівень додатків абсолютно не «дбає», однак, про те, що клієнт працює в мережі Ethernet, а сервер підключений до мережі Token Ring.

Між кінцевими системами може бути кілька десятків маршрутизаторів і безліч проміжних фізичних мереж різного типу, але додаток буде сприймати цей конгломерат як єдину фізичну мережу. Це визначає головну силу і привабливість інтернет-технологій і IP. На основі протоколу IP побудований не тільки Інтернет, а й будь-які інші мережі передачі даних (локальні, корпоративні), які можуть мати або не мати доступу до глобальної мережі Інтернет. Універсальність і гнучкість IP-мереж дозволяє використовувати їх не тільки для передачі даних, але і для іншої мультимедійної інформації. Останнім часом для передачі голосових повідомлень використовуються IP-мережі.

«Класичні» телефонні мережі, що зображено на рисунку 1.2, засновані на технології комутації каналів, яка для кожної телефонної розмови вимагає виділеного фізичного з'єднання.

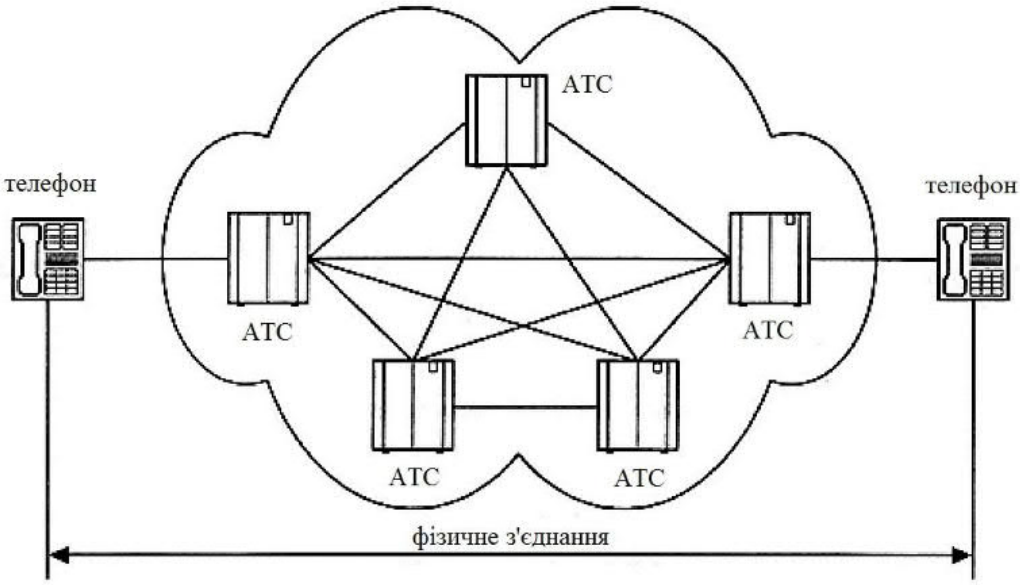

Рисунок 1.2 – З'єднання в «класичній» телефонній мережі

Отже, одна телефонна розмова - це одне фізичне з'єднання телефонних каналів. В цьому випадку аналоговий сигнал шириною 3,1 кГц передається на найближчу АТС, де він мультиплексуюча за технологією тимчасового поділу з сигналами, які надходять від інших абонентів, підключених до цієї АТС. Потім груповий сигнал передається по мережі міжстанційних каналів. Після досягнення пункту призначення PBX сигнал демультиплексується і досягає пункту призначення. Основним недоліком телефонних мереж з комутацією каналів є неефективне використання смуги частот каналу, під час пауз на мові канал не несе ніякої корисної навантаження.

Перехід від аналогових до цифрових технологій став важливим кроком в появі сучасних цифрових телекомунікаційних мереж. Одним з таких кроків в розвитку цифрової телефонії став перехід на комутацію пакетів. У мережах з комутацією пакетів блоки інформації, які не залежать від фізичного носія, передаються по каналах зв'язку. Такими блоками можуть бути пакети, кадри або осередки (залежно від протоколу), але в будь-якому випадку вони передаються по загальній мережі, причому – за окремими віртуальних каналах, незалежно від фізичного оточення. Кожен пакет ідентифікується заголовком, який може

містити інформацію про використаний ним канал, його походження (тобто про джерело або відправника) та пункти призначення (про одержувача або приймача).

У IP-мережах всі дані – голос, текст, відео, комп'ютерні програми або інформація в будь-якій іншій формі – передаються пакетами. Кожен комп'ютер і термінал такої мережі має свою унікальну IP-адресу, і передані пакети направляються одержувачу відповідно до цієї адреси, зазначеним в заголовку. Дані можуть передаватися одночасно між багатьма користувачами і процесами по одній лінії. У разі виникнення проблем IP-мережі можуть змінити маршрут для обходу несправних ділянок. Протокол IP не вимагає виділеного каналу для сигналізації. На першому етапі оцифровується голос. Потім оцифровані дані аналізуються і обробляються для зменшення фізичного обсягу даних, переданих одержувачу. Як правило, на цьому етапі відбувається придушення непотрібних пауз і фонового шуму, а також стиснення. На наступному етапі отримана послідовність даних розділяється на пакети і до неї додається протокольна інформація – адреса одержувача, порядковий номер пакету, якщо вони не доставляються послідовно, і додаткові дані для виправлення помилок. При цьому відбувається тимчасове накопичення необхідної кількості даних для утворення пакету до його безпосередньої відправки в мережу (рисунок 1.3)

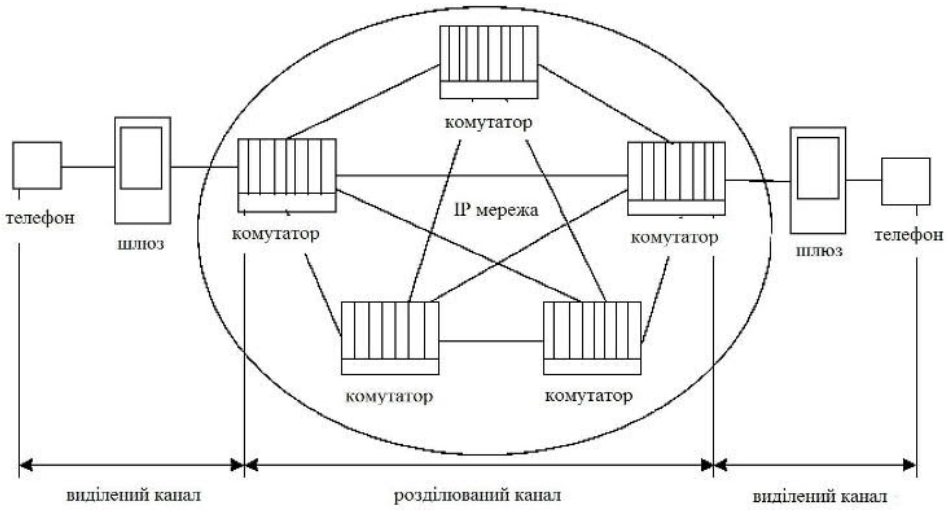

Рисунок 1.3 – З'єднання в мережі з комутацією пакетів

Оператори мереж з комутацією пакетів отримують переваги спільного використання телекомунікаційної інфраструктури за самою своєю природою. Простіше кажучи, вони можуть продати більше, ніж насправді, на основі статистичного аналізу мережі. Оскільки передбачається, що абоненти не будуть використовувати весь платний діапазон цілодобово і щодня, можна буде обслуговувати більше абонентів без розширення магістральної інфраструктури. Оборот і прибуток зростають. Іншими словами, абонент, який оплатив смугу 64 кбіт/с, використовує канал в середньому тільки на 25%. Таким чином, оператор може продати доступний ресурс чотириразовому кількості користувачів, не перевантажуючи свою мережу. Цей сценарій приносить користь як покупцеві, так і продавцеві, оскільки оператор збільшує свій дохід і знижує абонентську плату за рахунок зниження витрат. Це виграшне рішення вже визнано в світі передачі даних і тепер починає використовуватися на ринку телефонії.

В даний час в IP-телефонії існує два основних способи передачі голосових пакетів по IP-мережі: через глобальну мережу Інтернет (Інтернет-телефонія); використання мережевої передачі даних по виділених каналах (IP-телефонія). У першому випадку пропускна здатність безпосередньо залежить від завантаження інтернет-пакетів, що містять дані, голос, графіку і так далі, а значить, затримки проходження пакетів можуть бути різними. При використанні виділених каналів виключно для голосових пакетів може бути гарантована фіксована (або майже фіксована) швидкість передачі даних. У зв'язку з широким розповсюдженням Інтернету впровадження системи Інтернет-телефонії становить особливий інтерес, хоча слід визнати, що в цьому випадку якість телефонного зв'язку не гарантовано оператором. Для здійснення міжміського (міжнародного) зв'язку з використанням телефонних серверів організація або оператор зв'язку повинні мати сервер в тих місцях, де і звідки плануються дзвінки. Вартість такого підключення на порядок менше вартості телефонної розмови по звичайних телефонних лініях. Ця різниця особливо велика для міжнародних переговорів.

Загальний принцип роботи телефонних серверів Інтернет-телефонії наступний: з одного боку сервер підключений до телефонних ліній і може бути підключений до будь-якого телефону світу, з іншого боку, сервер підключений до Інтернету і може підключитися до будь-якого комп'ютера в світі. Сервер приймає стандартний телефонний сигнал, оцифровує його (якщо він з самого початку не є цифровим), значно стискає його, розбиває на пакети і відправляє через Інтернет в пункт призначення з використанням протоколу IP. Для пакетів, що надходять з мережі на телефонний сервер і що йдуть по телефонній лінії, операція виконується в зворотному порядку. Обидві операції (вхід сигналу в телефонну мережу і його вихід з телефонної мережі) відбуваються практично одночасно, що дозволяє вести повнодуплексний розмову. За допомогою цих основних операцій можна створити безліч різних конфігурацій. Наприклад, дзвінок з телефону на комп'ютер або з комп'ютера на телефон може здійснюватися за допомогою одного телефонного сервера. Для організації телефонного зв'язку необхідні два сервера. Основним стримуючим фактором для масштабного впровадження IP-телефонії є відсутність в IP-протоколі механізмів для забезпечення гарантованої якості обслуговування, що робить його ще не найнадійнішим засобом транспортування голосового трафіку.

Сам протокол IP не гарантує доставку пакетів, а також час їх доставки, що викликає такі проблеми, як «порушений голос» і просто збої в розмові. Сьогодні ці проблеми вирішуються: організації зі стандартизації розробляють нові протоколи, виробники випускають нове обладнання, але на цьому рівні сумісність і стандартизація вже не такі хороші, як мовні пакети. Можна відзначити, що якщо всередині приватної корпоративної мережі деяка втрата якості передачі голосу при великому завантаженні ресурсів цілком допустима, за умови, що в середньому це цілком задовільно, то в разі загальнодоступних мереж все набагато серйозніше. Оскільки оператор надає деяку послугу і бере за неї гроші, він зобов'язаний гарантувати її якість. Навіть якщо замовник погоджується (хоча в умовах жорсткої конкуренції на ринку телекомунікацій це

маловірогідно), час від часу він може поскаржитися в разі серйозних або тривалих проблем. Оператор змушений стежити за якістю послуг, що надаються, що в разі їх масштабного надання вимагає відповідного апаратного і програмного забезпечення, що досить дорого і доступно не у всіх частинах мережі. З точки зору масштабованості IP-телефонія здається закінченим рішенням. Оскільки, з'єднання на основі протоколу IP може починатися (і закінчуватися) в будь-якій точці мережі від абонента до шини. Відповідно, в IP-телефонію в мережі можна вводити сайт за сайтом, що, до речі, вигідно з точки зору міграції, так як вона може здійснюватися «зверху вниз», «знизу вгору» або за іншою схемою. Рішення IP-телефонії характеризуються певним модульним кількістю і ємністю різних вузлів шлюзу, гейткипера - можна збільшувати практично незалежно, відповідно до поточних потреб. Ми не будемо брати в розрахунок проблеми збільшення ресурсів мережевої інфраструктури, так як вузли самої мережі можуть бути незалежними від системи IP-телефонії, а також можуть поєднувати свої функції.

1.2. Типологія IP-телефонії

Мережі IP-телефонії надають можливості для викликів чотирьох основних типів:

«Від телефону до телефону» (рисунок 1.4). Виклик йде із звичайного телефонногоапарату до АТС, на один з виходів якої підключений шлюз IP-телефонії, і через IP-мережу доходить до іншого шлюзу, який здійснює зворотні перетворення;

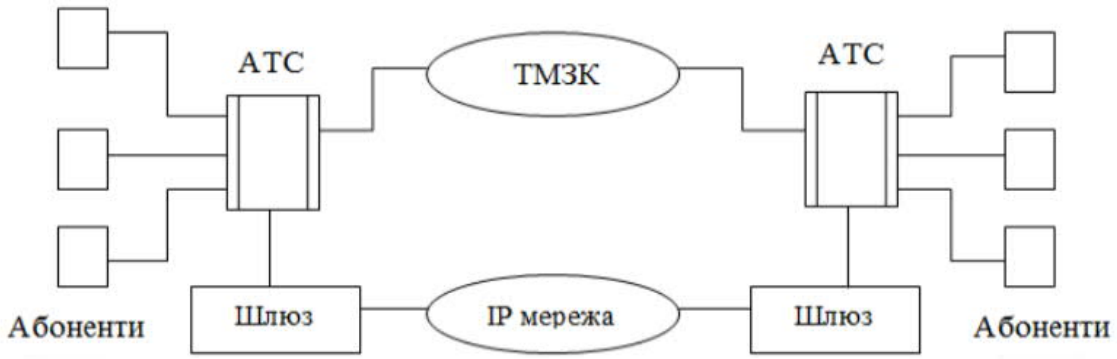

Рисунок 1.4. – Типологія «Від телефону до телефону»

«Від комп'ютера до телефону» (рисунок 1.5). Мультимедійний комп’ютер, що має програмне забезпечення IP-телефонії, звукову плату (адаптер), мікрофон і акустичні системи, підключається до IP-мережі або до мережі Інтернет, і з іншого боку шлюз IP-телефонії має сполучення через АТС із звичайним телефонним апаратом;

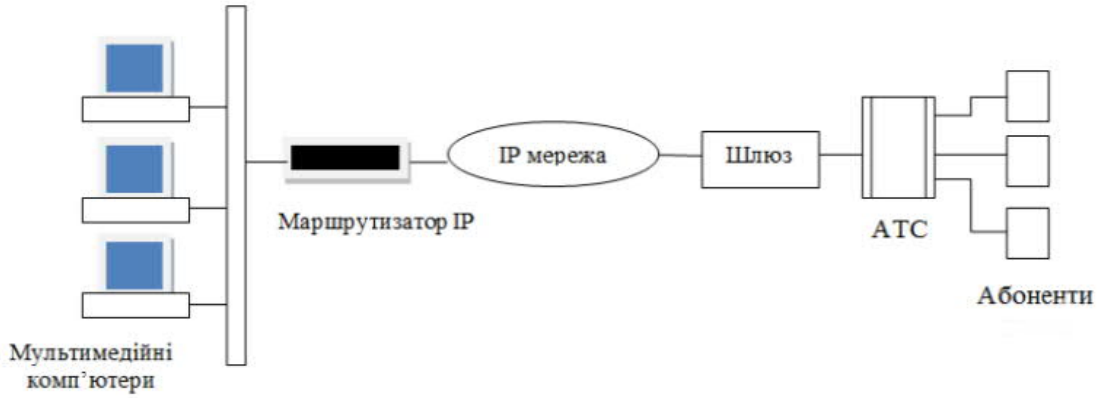

Рисунок 1.5. – Типологія «Від комп’ютера до телефону»

«Від комп'ютера до комп'ютера» (рисунок 1.6). У цьому випадку з’єднання встановлюється через IP-мережу між двома мультимедійними комп'ютерами, обладнаними апаратними та програмними засобами для роботи з IP-телефонією;

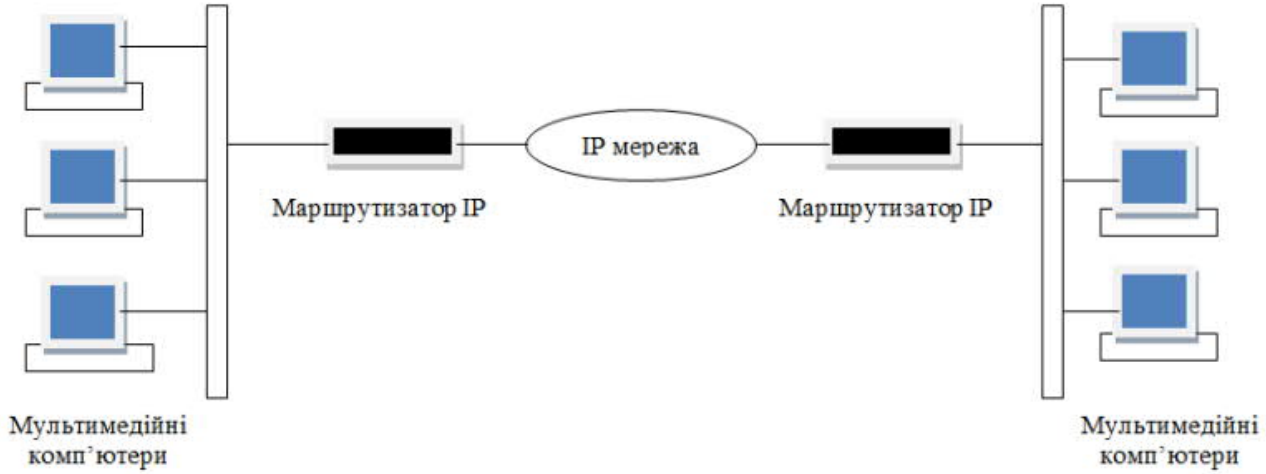

Рисунок 1.6. – Типологія «Від комп'ютера до комп'ютера»

«Від WEB-браузера до телефону» (рисунок 1.7). З розвитком мережі Інтернет став можливий доступ і до мовним послуг. Наприклад, на WEB-сторінці деякої компанії в розділі «Контакти» розміщується кнопка «Виклик», натиснувши на яку можна здійснити мовне з'єднання з представником даної компанії без набору телефонного номера. Вартість такого дзвінка для викликає користувача входить у вартість роботи в мережі Інтернет

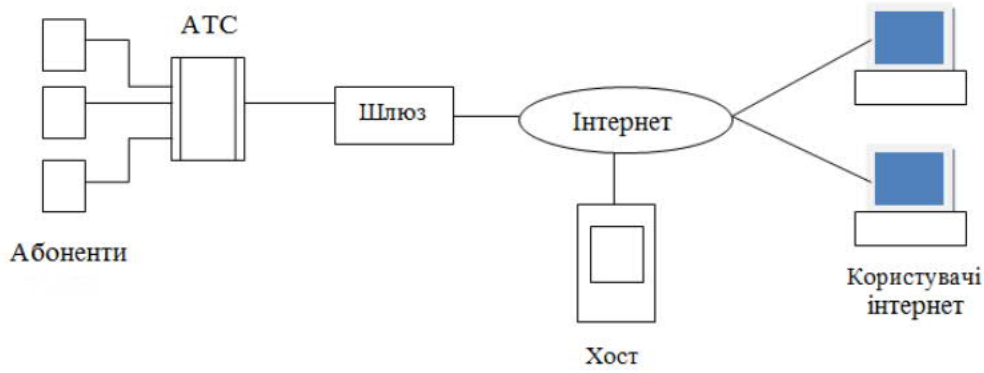

Рисунок 1.7. – Типологія «Від WEB-браузера до телефону»

Характеристики шлюзів IP-телефонії. У загальному випадку IP-телефонія заснована на двох основних операціях: перетворення двостороннього аналогового мови в цифрову форму всередині пристрою кодування і

декодування (кодека) і упаковці в пакети для передачі IP. Ці функції найчастіше виконуються автономними шлюзовими пристроями, які мають кілька різновидів. Це можуть бути виділені пристрої або підключення маршрутизатори / комутатори з вбудованим апаратним і програмним забезпеченням шлюзу. Інший тип автономного устрою - це пристрій, в якому шлюз об'єднаний з віддаленим доступом і пулом модемів (Рисунок. 1.8).

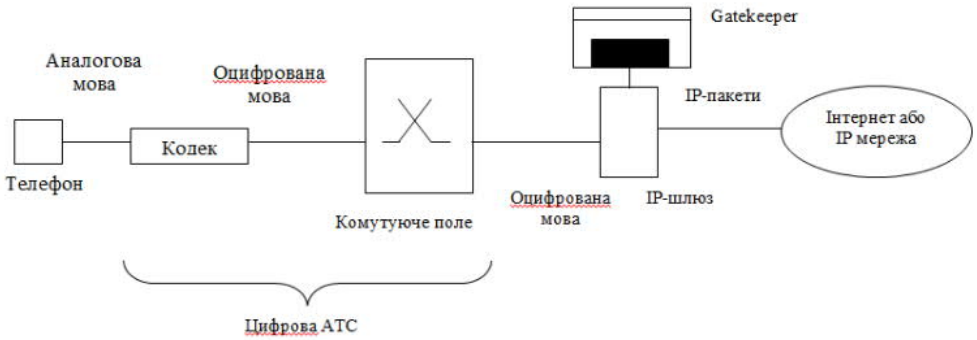

Рисунок. 1.8. – Положення шлюзу в мережі IP-телефонії

Незалежно від методу апаратної реалізації шлюзи IP-телефонії можуть мати ряд характеристик, які перераховані нижче. Сумісність зі стандартом H.323: основний протокол для роботи IP-обладнання. Переважна більшість виробників прийняли протокол, описаний ITU-T в рекомендації H.323v2, яка стандартизує мультимедійну зв'язок в мережах з комутацією пакетів. Користувачі мультимедійних персональних комп'ютерів з програмним забезпеченням H.323 можуть підключатися до такої системи шлюзу. Виклики можуть бути спрямовані на підтримку шлюзів H.323 від інших виробників. В результаті дана система буде забезпечувати інтеграцію мови, відео і даних в реальному часі для додатків з організації спільної роботи в робочих групах, наприклад Microsoft NetMeeting. Стандарти, відмінні від H.323, використовують у своїй роботі шлюзи CX950 Access Switch компанії Memotec Communications Inc., F-50 IP і F-200. IP-компанії Neura Communications Inc., VIP Gateway від Nortel Networks, мережеві станції Network Exchange 2201/2210 фірми Netrix Corp. Доступність механізмів

резервування ресурсів: підтримка будь-якої схеми пріоритизації (протокол RSVP або DS-байт), що дозволяє вибирати пріоритет між переданим мовою або даними, є важливими характеристиками шлюзу. Протокол RSVP дозволяє маршрутизаторів утримувати частину смуги пропускання для організації голосового трафіку. IPT (Ericsson Inc.), Netblazer 8500 (Digi International), Packetstar IP Gateway 1000 (Lucent Technologies Inc.), Vocaltec Telephony Gateway (Vocaltec Communications Ltd.), Webphone Gateway Exchange (Netspeak Corp.) не мають цієї можливості. Підтримка основних телефонних інтерфейсів і типів сигналів тривоги є важливими критеріями при оцінці характеристик шлюзів, існує велика кількість різноманітних телефонних інтерфейсів, підтримуваних IP-шлюзом (E1, PRI, BRI) і аналоговим зокрема, а також підтримка основних типів телефонної сигналізації: CAS, DTMF , PRI і ACS №7. Підтримка апаратних механізмів відповідно до рекомендації H.235 відіграє значну роль. Шлюзи, що підтримують передачу мови через Frame Relay, виробляються компаніями 3COM (Pathbuilder S200 Voice Access Switch), Cisco (серії 2600, 3600), Motorola (Vanguard 6560/6520), Newbridge Networks Corp. (MainStreetXpress 36100 VoIP Gateway) і іншими. Режим ATM підтримують шлюзи, що випускаються фірмами Lucent Technologies (Packetstar IP Gateway 181000), Cisco (серія 2600, 3600), Ascend Communications (MultiVoice Gateway), Motorola Vanguard 6560/6520 Multiservice Access Device та інші.

1.3. Сучасні телефонні системи

Основним на даний момент є «класичний» аналоговий зв'язок. При цьому використовуються звичайні телефони. Зв'язок між ними здійснюється за допомогою мідних кабелів. Кожен дзвінок здійснюється за допомогою оператора фіксованого зв'язку або АТС. Це найпростіше і поширене підключення.

PBX (Private Branch eXchange) – це тип телефонної системи, яка централізує завдання перемикання телефонних ліній і маршрутизації дзвінків всередині організації. Замість того, щоб безпосередньо підключати телефони до ліній, вони підключаються до системи PBX, яка автоматично призначає виклики лініях. У минулому телефонні системи PBX керувалися оператором вручну – в системі, відомої як PMBX (Private Manual Branch eXchange), або приватний портативний телефон. Звідси сцени, де людина підключає і переміщує дроти на комутаторі. В даний час завдання комутації автоматизована, що робить використання телефонних станцій набагато зручніше. Ці автоматизовані версії називаються телефонними системами PABX (Private Automated Branch eXchange). Існують також системи IP PBX, які працюють за тими ж принципами, але маршрутизують дзвінки через Інтернет, а не за традиційними телефонними лініями.

Далі буде розглянуто деякі загальні питання по телефонах PBX, плюси і мінуси, а також рекомендації про те, чи підходить PBX саме вам.

Великою перевагою телефонної системи PBX є те, що вона централізує завдання вибору лінії для виклику, замість того, щоб вимагати, щоб кожен телефон мав свою власну виділену лінію. Це спрощує масштабованість і потенційну економію, оскільки вам потрібно тільки достатня кількість ліній для одночасної обробки максимальної кількості викликів.

Кількість ліній, необхідних для більшості підприємств, менша за кількість необхідних телефонів. У цій системі додати новий телефон так само просто, як підключити пристрій до системи PBX.

Ще однією перевагою телефонних систем PBX є можливість мати один основний номер для вашого бізнесу, при цьому певні телефони ідентифікуються за додатковими номерами, а не по власним унікальним номерам. Це може значно спростити процес дзвінка для клієнтів, оскільки їм потрібно запам'ятати або зберегти тільки один номер телефону. Це також дає більш уніфікований і професійний вид.

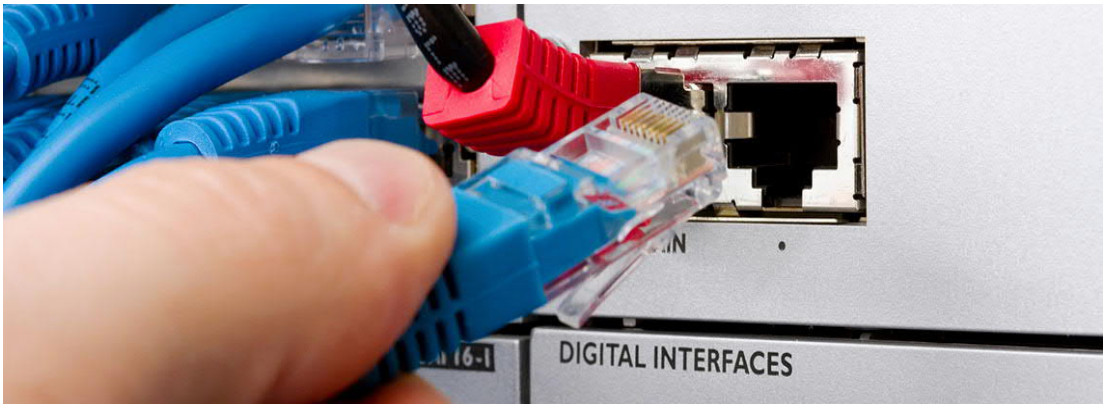

Рисунок 1.9. – Сервер PBX

Сервер PBX – це мозок системи PBX. Коли користувач робить телефонний дзвінок, сервер АТС визначає, як правильно маршрутизировать дзвінок. Існує два основних типи серверів PBX: для традиційних систем PBX, які працюють по телефонних лініях, і для телефонних систем IP PBX, які працюють через Інтернет.

В обох випадках результат однаковий. Сервер відправляє виклик через відповідний канал для підключення користувача. Різниця в тому, що традиційна система використовує комутатор і стандартні телефонні лінії, тоді як система IP PBX використовує комп'ютерний сервер та підключення до Інтернету.

Апаратна частина PBX в основному складається з телефонних пристроїв, кабелів і самого комутатора, який часто розміщується в шафі. Комутатори можуть варіюватися від відносно невеликих і компактних пристроїв, призначених для малого бізнесу, до великих, складних і дорогих комерційних систем для великого бізнесу.

Система IP PBX матиме комп'ютерний сервер, на якому працює система, а не комутатор, і в результаті зазвичай більш компактна.

PBX відноситься до типу телефонної системи комутації і маршрутизації, яка може працювати як на традиційному стаціонарному телефоні, так і через Інтернет. VoIP, з іншого боку, являє собою комбінацію апаратного і програмного

забезпечення, яка дозволяє вам здійснювати телефонні дзвінки через Інтернет, а не за традиційними телефонними лініями.

Системи VoIP відмінно підходять для малого бізнесу, тому що вони зазвичай більш економічні, ніж традиційні телефонні системи.

Для тих, хто хоче об'єднати переваги систем VoIP і PBX, IP PBX може стати відмінним і надійним телефонним рішенням для малого бізнесу. У цих системах використовуються технології VoIP і PBX для забезпечення більшої масштабованості та інтеграції програмного забезпечення.

Точно так же віртуальна АТС підключається до Інтернету таким чином, щоб уніфікувати зв'язок між різними носіями. Віртуальне або Інтернет-з'єднання може включати такі функції, як візуальна голосова пошта, автовідповідач, IVR або відеоконференцзв'язок.

Порівняння IP PBX та траційних PBX систем.

IP PBX - це система VoIP, тобто вона відправляє голосові сигнали через Інтернет, а не за стандартними телефонними лініями. Традиційна система PBX використовує стандартні телефонні лінії, підключення телефонною компанією. IP PBX (також відома як PBX voice) зазвичай є набагато більш економічним і гнучким вибором, оскільки не вимагає великої кількості спеціалізованого обладнання.

Виклики маршрутизируются через сервер, і сервер навіть не обов'язково повинен бути на місці, що також може спростити обслуговування і заощадити місце. Послуги VoIP не вимагають наявності центрального офісу, через який приймає вхідні дзвінки.

При передачі голосу по IP звук передається через Інтернет через шлюз VoIP. Весь цей процес зв'язку, включаючи все обладнання, здійснюється через постачальника послуг VoIP, що спрощує доступ до передових технологій для малих і середніх підприємств. Провайдери можуть допомогти вам налаштувати мережу, в якій ви зможете скористатися цими функціями.

Хостинговая АТС - це система IP-АТС, розташована за межами підприємства. Підтримується сторонніми сервісами. Транкінг SIP відноситься до процесу підключення системи IP PBX до комутованої телефонної мережі загального користування (PSTN), щоб дозволити вихідний набір на телефонах, відмінних від IP. Якщо ваша АТС встановлена, а не на хості, система транкинга SIP повинна обслуговуватися вашим підприємством. Хостинговая АТС має ряд переваг:

– Зниження початкових витрат – немає необхідності купувати і встановлювати сервери на місці і підключати транкінговий службу. Зазвичай все, що вам потрібно, це IP-телефони і стабільне широкосмугове з'єднання.

– Більш проста масштабованість. Системи PBX з розміщенням набагато простіше масштабувати, ніж локальну систему. Якщо ви підете на місце, ви будете нести відповідальність за оновлення обладнання, що означає додавання серверів і налаштування системи для розміщення більшої кількості телефонів. Це може бути складно і часто вимагає IT-фахівця.

– Спрощене обслуговування. Для настройки мережі PBX на місці потрібно, щоб ваш IT-відділ виконував всі роботи з технічного обслуговування і ремонту. Постачальники хост-АТС роблять все це за вас, тому єдине, про що вам потрібно турбуватися – це додавати користувачів і підтримувати свої телефони за допомогою простого у використанні програмного забезпечення АТС.

З іншого боку, локальна АТС дозволяє краще контролювати вашу систему, зберігаючи її всередині компанії. Це може бути великою перевагою для деяких власників бізнесу, але вам доведеться порівняти це з перевагами хостингу.

У світі бізнес-телефонії ключові телефонні системи, більш відомі як ключові системи, являють собою більш просту альтернативу системам PBX. У них не так багато ліній і менше автоматизованих функцій. До появи VoIP і інших віртуальних опцій власникам бізнесу зазвичай доводилося вибирати між цими двома різними системами. Сьогодні існують більш досконалі комунікаційні рішення, які роблять ці дві традиційні системи застарілими.

Хмарна телефонна система.

Хмарна телефонна система - це телефонна система VoIP, розташована в одному або декількох захищених віддалених центрах обробки даних. Доступ до сервера і телефонної системі здійснюється через Інтернет. Хост PBX (приватна телефонна станція) є прикладом хмарної телефонної системи.

Ці системи пропонують функції повною телефонної системи без необхідності витрат на простір і обладнання, які часто виникають при установці на місці. Система хмарної АТС може пропонувати утримуваний контент, переклад викликів, автоматичних помічників, конференц-зв'язок і багато іншого.

Їх також легше масштабувати, тому що немає фізичного обладнання для поновлення або установки. Також легко додавати або переміщати розширення, коли співробітники додаються або переміщуються в новий офіс або робоче місце.

Щоб знайти відповіді на загальні питання про хмарних телефонних системах, зрозуміти переваги і недоліки цих систем і визначити, чи може це бути рішення, необхідне вашому бізнесу, розгляньте основні переваги.

Хмарні телефонні системи пропонують кілька основних переваг у порівнянні з традиційними установками на місці:

– Низька попередня вартість – оскільки він розміщений у постачальника послуг, вам не потрібно турбуватися про обслуговування і щоденному обслуговуванні вашої хмарної телефонної системи. Вам також не потрібно турбуватися про купівлю та встановлення обладнання, яке є одним з основних перешкод для роботи телефонної системи на місці. Співробітники представляють користувачів в комунікаційному програмному забезпеченні, але у вас є вибір: оновити нові телефонні лінії або настільні телефони, щоб додати їх в офіс. Це забезпечує значну економію в порівнянні зі старими телефонними системами.

– Простота використання – вносити зміни та адмініструвати телефонну систему легко завдяки порталам управління, пропонованих постачальниками

послуг. Цей контроль може бути особливо помітний при обслуговуванні. Через хмарну систему провайдер хостингу несе відповідальність за обслуговування та забезпечення роботи системи. У малих підприємств може не бути ресурсів для підтримки телефонної системи, що робить цю послугу величезною допомогою. Веб-додатки, які багато хмарні телефонні системи використовують для управління, також зазвичай дуже зручні для користувача, тому користувачі можуть легко налаштовувати свої власні переваги без допомоги IT-спеціаліста.

– Масштабованість. Масштабування за допомогою хмарної телефонної системи так само просто, як увійти в систему і додати користувача і телефон. Це головна перевага для швидкозростаючих малих підприємств. Будь-яка компанія з декількома співробітниками і телефонами буде дуже корисна. Кожен співробітник, як в офісі, так і за його межами, – це просто новий користувач програмного забезпечення для бізнес-комунікацій, і немає необхідності в додатковому устаткуванні. Це робить його дуже масштабованим рішенням: ви платите тільки за те, що вам потрібно, і додаєте місця/ліцензії у міру зростання ваших потреб.

– Легкий віддалений доступ – ви не підключені до якого-небудь фізичного місця для зв'язку з хмарної телефонною системою. Все, що вам потрібно, це працююче підключення до Інтернету і програма для IP-телефону або програмного телефону. Це відмінно підходить не тільки для віддалених співробітників, але і для підприємств з кількома офісами, оскільки вам потрібен тільки один адміністратор, а не по одному для кожної філії. Багато постачальників хмарних послуг також пропонують веб-додатки і мобільні додатки для легкого доступу та використання. Це робить хмарні телефони надзвичайно практичним рішенням для уніфікованих комунікацій. Дослідження показали, що компанії, які використовують Інтернет-телефони, можуть збільшити продуктивність праці співробітників на 3,9 години в тиждень, підтримуючи простоту зв’язку.

– Надійність – завдяки так званому географічному резервуванню – наявність декількох серверів у різних фізичних місцях, які виконують роль резервних копій один для одного – простої у постачальників хмарних телефонів надзвичайно низькі. Це, звичайно, критично важливо для бізнесу. Якщо телефони – це ваша основна лінія спілкування з клієнтами та клієнтами, ця додаткова надійність є головною перевагою хмарних комунікацій.

Недоліки послуг хмарної телефонії:

– Відсутність контролю - ви перебуваєте під владою хостингової компанії та постачальника хмарних послуг. Якщо служба відключиться або у хоста виникнуть проблеми з сервером, ваші телефони можуть перестати працювати. Незважаючи на те, що хмарні телефонні системи мають чудову надійністю, ні один провайдер не може гарантувати 100% безперебійну роботу. Важливо продумати плани резервного копіювання на випадок виходу з ладу.

– Залежність від підключення до Інтернету. Ви залежите від надійності вашого інтернет-провайдера (ISP) не тільки по відношенню до доступу в Інтернет, а й доступу по телефону. Якщо у вашого інтернет-провайдера виникнуть проблеми, ви ризикуєте втратити телефонний зв'язок. Інтернет-телефони використовують швидкість завантаження і вивантаження близько 100 кбіт/с на пристрій під час голосових викликів, так що майте це на увазі.

– Інше обладнання. Оскільки хмарні телефонні системи є системами VoIP, для їх використання вам знадобиться інший тип телефону, званий IP-телефоном. Якщо у вас більша організація з великою кількістю традиційних телефонів, перехід на хмару може спричинити значні витрати.

1.4 Висновки до розділу

В даному розділі розглянуто загальні принципи побудови мережі інтернет

та IP-протоколів. IP-телефонія стала своєрідним стадандартом телефонного зв’язку. Основні переваги IP-телефонії:

– зручність

– відносна надійність

– відносно невисока вартість порівняно з аналоговим зв’язком

Недоліки IP-телефонної мережі аналогічні до інших сервісів, що використовують IP-протоколи:

– сприйнятливість до вірусних атак;

– DoS-атак;

– можливість несанкціонованого віддаленого доступу.

VoIP як складова IP-телефонії також набула своєї популярності. Здебільшого його використовують в малому та середньому бізнесі. Розглянуто типології IP-телефонії, і тут можна виділити 4 основні типи:

– від телефону до телефону;

– від комп'ютера до телефону;

– від комп'ютера до комп'ютера;

– від WEB-браузера до телефону.

Розглянуто сучасні телефонні системи. Проаналізовано класичний аналоговий зв’язок PBX. Який на даний момент автоматизований і не потребує втручання людини. Так як раніше переключення відбувалось вручну. Розглянуто сучасні хмарні телефонні системи. Основною її перевагою є можливість приймати дзвінки з будь-якого девайсу. Недоліком є необхідність бути постійно підключеним до мережі інтернет.

2. ОПТИМІЗАЦІЯ ТА ПРОТОКОЛИ ЗАХИСТУ IP-ТЕЛЕФОНІЇ

2.1 Показники якості IP-телефонії

Традиційні телефонні мережі коммутируют електричні сигнали з гарантованою смугою пропускання, достатньою для передачі сигналів голосового спектру. При фіксованій смузі пропускання сигналу, що передається вартість одиниці часу зв'язку залежить від відстані та місця розташування пунктів виклику і місця відповіді. IP-телефонія – один з напрямків передачі даних, де важлива динаміка передачі сигналу, що забезпечується сучасними методами кодування і передачі інформації, а також збільшенням пропускної спроможності каналу, що призводить до успішної конкуренції IP-телефонії з традиційні телефонні мережі. Основними складовими якості IP-телефонії є:

– якість мови;

– діалог;

– можливість користувача зв'язуватися і розмовляти з іншим користувачем в реальному часі і повнодуплексному режимі;

– розбірливість;

– чистота і тональність мови;

– відлуння;

– рівень гучності мови;

– якість сигналізації;

– час встановлення виклику;

– час завершення;

– DTMF – визначення і фіксація сигналів багаточастотного набору номера.

В даний час найбільш поширені два методи вимірювання якості мови: суб'єктивне тестування і машинне тестування. Суб'єктивне тестування характеризується участю студентів, які оцінюють здатність різних систем кодування відтворювати складні фрази. Прикладами є ACR (Absolute Category

Rating) або MOS (Mean Opinion Score). Машинне тестування характеризується наявністю електронної системи, яка передає цифровий мовної файл через пристрій кодування/стиснення, а потім робиться математичне порівняння вихідного сигналу з вхідним. Як приклади можна привести ITU методи P.861: PSQM, що рекомендуються (Perceptual Speech Quality Measurement) і G.107 E Model, або R Factor (коефіцієнт R, об'єктивна міра якості передачі в телефонних мережах на основі електронної моделі). Суб'єктивні оцінки не можна точно співвіднести з характеристиками мережі, використовуваними при проектуванні і експлуатації мереж. Їх не можна точно порівняти з процесами, реалізованими в термінальному обладнанні (тобто оффлайн). В даному випадку мова йде про алгоритми стиснення, схемах кодування, механізми захисту інформації, відновлення даних. Але слід зазначити, що суб'єктивні оцінки використовувалися протягом багатьох років як єдиний підхід до оцінки якості в телефонних мережах і в деякій мірі залишаються актуальними і сьогодні. Машинне тестування (об’єктивний підхід) дозволяє описати показники якості при передачі мови в пакетній формі (Рекомендація МСЕ G.107). При використанні підходу суб'єктивної оцінки якості обслуговування при передачі мови первинним критерієм якості аудіо і відеоінформації є сприйняття якості послуги користувачем. Найбільш широко використовується методика суб'єктивної оцінки якості описана в рекомендації МСЕ P.800 (початкова редакція відноситься до 1993 р.) і відома як методика MOS(Mean Opinion Score). Відповідно до неї якість мови, що отримується при проходженні сигналу від джерела звукового сигналу до отримувача через систему зв'язку, оцінюється як середнє арифметичне від всіх оцінок, що виставляються експертами після прослуховування тестованого тракту передачі. Експертні оцінки визначаються відповідно до наступної п’ятибальної шкали: 5 – відмінно, 4 – добре, 3 – прийнятно, 2 – погано, 1 – неприйнятно. Оцінки 3,5 балу і вище відповідають стандартній і високій телефонній якості, 3,0-3,5 – прийнятній якості, 2,5-3,0 – синтезованому звуку. Для передачі мови з хорошою якістю доцільно

орієнтуватися на значення MOS не нижче 3,5 балів. Об'єктивний підхід заснований на так званій E-моделі, яка відкрила новий напрямок в оцінці якості послуг, пов'язаних з вимірюванням характеристик терміналів і мереж. Після створення E-моделі було проведено значну кількість тестів, в яких змінився рівень спотворення мережевих факторів. Дані цих тестів були використані в E-моделі для розрахунку об'єктивних оцінок. Результатом розрахунків по E-моделі є число, зване R-фактором («рейтинг-фактор»). Значення R-фактора однозначно зпівставляються з оцінками MOS. Відповідно до E-моделі R-фактор визначається в діапазоні значень від 0 до 120, де 120 відповідає найвищому рівню якості. При розрахунку R-фактора враховується 20 параметрів, в тому числі: однонаправлена затримка; коефіцієнт втрати пакетів; втрата даних через переповнення буфера тремтіння; спотворення, що вносяться при перетворенні аналогового сигналу в цифровий і подальшому стисненні (обробка сигналу в кодеках); вплив луни і ін. Все це говорить про те, що E-модель і R-фактор можна використовувати для об'єктивної оцінки якості мови в технології VoIP. Розрахунок R-фактора актуальний для випадку, коли спотворення сигналу в каналі не враховуються, а обраховуються спотворення, що виникають при перетворенні реальної мови в електричний сигнал (і навпаки). Теоретичне (досяжне) значення R-фактора зменшується від 120 до 93,2, що відповідає оцінці MOS, рівній 4,4. Тобто при використанні E-моделі оцінка 4,4 в системі MOS являється максимально можливою оцінкою якості мови в мережі без спотворень. Величина R-фактора змінюється від 120 до 93,2, що відповідає оцінці MOS – 4,4. Значення R-фактора визначається по наступній формулі:

$$R = R_0 - I_s - I_d - I_e + A \qquad (1.1)$$

де $R_0 = 93{,}2$ – початкове значення R-фактора;

I_s – спотворення, що вносяться кодеками і шумами в канал;

I_d – спотворення за рахунок сумарної наскрізноїзатримки в мережі;

I_e – спотворення, що вносяться обладнанням, включаючи і втрати пакетів;

A – фактор переваги.

Наприклад, мобільні користувачі можуть погодитися на низький рівень якості, отримавши додаткові зручності. У більшості випадків передбачається, що розрахунок параметра R-фактора А дорівнює нулю. Кожен з компонентів виразу 1 в тій чи іншій мірі впливає на якість мови в пакетних мережах. Таким чином, при обчисленні I_s – значення R-фактора зменшується, що викликано спотвореннями, спровокованими в кодеку при пакетування мовного сигналу. Слід зазначити, що якість передачі мови в мережах з комутацією пакетів в останні роки було значно покращено за рахунок створення ефективних кодеків, що забезпечують хорошу розбірливість мовного сигналу на приймаючій стороні. Ці методи включають:

– методи ефективного кодування мови (рекомендації МСЕ-Т серії G.7xx);

– механізми придушення пауз (механізм кодування мови при переривистій передачі, відомий як Voice Activity Detection, VAD);

– механізми ехоподавлення (рекомендація МСЕ G.164) і ехокомпенсації (рекомендації МСЕ G.165 і G.168);

– механізми маскування помилок(packet loss concealment), що забезпечують компенсацію пропусків в мовному потоці, викликаних втратою окремих пакетів.

На додаток до вищесказаного слід зазначити, що затримка доставки пакета визначається часом передачі пакета від джерела до одержувача. Затримка залежить від мережевого трафіку і доступних мережевих ресурсів, таких як пропускна здатність, під час доставки. Мова з точки зору інформаційного ресурсу – дуже чутливий тип трафіку, тому що якщо ви перевищите допустиме значення затримки пакета, він буде відкинутий. В результаті при великій кількості втрачених пакетів якість мовлення погіршується, що відображено в наведеній вище формулі для R-фактора, де вплив затримки враховується за допомогою компонента I_d. В результаті досліджень якості мовного сигналу в 60-

х роках минулого століття було виявлено, що людина починає відчувати затримки мовного сигналу, що перевищують 150 мс, і відчуває помітний дискомфорт, якщо затримка перевищує 250 мс. Пізніше за підтримки МСЕ були проведені дослідження впливу затримки в мережі на якість телефонних розмов. Ці результати відображені в рекомендації МСЕ G.114, згідно з якою рекомендується, щоб поріг затримки для передачі мови становив 150 мс. Із затримкою в 300 мс розмова розбивається на фрагменти, які неможливо пов'язати в мову.

2.2. Економія обсягу даних

Формат цифрових даних для передачі голосового сигналу у вигляді 8-бітних відліків, які передаються зі швидкістю 8000 відліків в секунду, визначає потребу в смузі пропускання телефонної мережі на рівні 64 Кбіт / с для кожного телефонного виклику. У традиційних телефонних мережах на основі TDM часовий інтервал зарезервований для передачі кожного виклику у всіх проміжних каналах. Доступність попередньо зарезервованого ресурсу відповідно до основним принципом мереж з комутацією каналів робить непотрібними будь-які заходи щодо зменшення загального обсягу переданих даних. У VoIP ситуація інша, тому що замість резервування ресурсів для кожного виклику за загальними каналах передаються IP-пакети, кожен з яких містить зразки конкретного телефонного дзвінка. У цьому випадку зменшення загального обсягу переданих даних може знизити навантаження на канал або передати по ньому більше одночасних розмов.

Для зменшення обсягу голосових даних використовується стиснення, так звані – кодеки. Відправник кодує вихідні зразки цифрового голосу, для яких потрібна смуга пропускання 64 Кбіт / с, в результаті чого зменшується обсяг і,

відповідно, для їх передачі потрібна менша смуга пропускання. На стороні одержувача процедура зворотна - зі стислих даних відновлюються вихідні дані, які вже використовуються для відтворення голосового сигналу. Слово «кодек» утворене з початкових літер слів «кодування» і «декодування» і означає набір двох функцій, які при спільному використанні на різних кінцях шляху передачі мовних даних забезпечують скорочення обсягу даних. переданий.

На перший погляд може здатися, що кодеки схожі на відомі програми архівування файлів, такі як zip або rar. Насправді це не так, основні відмінності кодеків від програм архівування полягають в наступному:

– програми архівування опрацьовують файл в цілому, в тойчас як кодеки обробляють потокові дані, тобто такі, які постійно надходять;

– час роботи програми архівування не регламентується, суттєве збільшення часу на стискання певного файлу зазвичай некритично, в той час як тривалість обробки голосових даних кодеком додається до загальної затримки передачі голосу до співрозмовника і не може перевищувати прийнятної межі;

– програми архівування забезпечують 100% збереження інформації, файл до архівації і файл, який було відновлено зархіву, повністю ідентичні, в той час як кодеки враховують природу голосового сигналу і можуть привносити незначне погіршення якості з метою економії даних.

З точки зору вивчення характеристик мовних кодів слід зазначити, що на сьогоднішній день існує досить великий набір ефективних кодеків з різними характеристиками. У таблиці 1.1 показані характеристики кодеків, які відповідають стандартам ITU-T. Історично перший тип кодека, відомий як G.711 (версії G.711a і G.711u, швидкість виведення 64 кбіт / с), перетворює аналоговий сигнал в високоякісний цифровий без використання стиснення. Для його нормальної роботи потрібна значна смуга пропускання каналу зв'язку в порівнянні з кодеками, в яких інформація стискається. В даний час ця проблема вирішується використанням цифрових сигнальних процесорів (DSP), на основі яких можна створювати ефективні кодеки з низькими вимогами до пропускної

здатності. Щоб збільшити пропускну здатність каналу зв'язку, був розроблений ряд низькошвидкісних кодеків, які мають більш низькі вимоги до пропускної здатності і, отже, дозволяють організувати більше з'єднань на одному і тому ж каналі зв'язку. Хоча це перевага вельми сумнівно, оскільки розбірливість мови знижується, затримки збільшуються, а якість мовлення стає більш чутливим до втрати пакетів.

Таблиця 1.1 - Характеристики кодеків за стандартами МСЕ-Т

Кодек	Потрібна пропускна здатність, Кбіт/с	Якість передачі голосу за 5-бальною шкалою	Типове використання
1	2	3	4
G.711	64,0	4,3	Передача розмов
G.726r32	32,0	3,8	
G.736r24	24,0	3,75	
G726r16	16,0	3,7	
G.728	16,0	3,75	
iLBC	13,3 або 15,2	4,14	Використання в мережах з нестабільною якістю передачі пакетів
GSM Full Rate	13,0	3,5	Голосові меню, голосова пошта
G.729a	8,0	3,7	Передача розмов
G.723r63	6,3	3,7	Передача голосу та мультимедіа
G.723r53	5,3	3,65	

Продовження таблиці 1.1

1	2	3	4
G.722	64,0	4,5	Передача сигналу ширшого спектру – до 7кГц, та кращої якості кодування – 14 біт на відлік
G.722.1	32,0 або 24,0	4,09	Передача сигналу ширшого спектру – до 7кГц, та кращої якості кодування – 14 біт на відлік
G.722.2	16,0	3,98	Системи сумісного передачі голосу і файлів зі змінними умовами швидкості передачі даних

Існує велике розмаїття кодеків, які розрізняються такими па-раметрами, як рівень стиснення даних, складність обробки, ступінь погіршення якості, оптимальні умови використання. Деякі кодеки мають статус стандартних, вони описані документами ITU(International Telecommunication Union) і позначаються кодами виду G.7xx(наприклад, G.711, G.726, G.729 та ін.). Також існують фірмові кодеки, використання яких вимагає використання обладнання певного

виробника на обох кінцях шляху передачі голосових даних. Що стосується передачі голосу по VoIP, важливо пам'ятати, що передані дані включають не тільки цифрові свідчення, але і бізнес-інформацію, включаючи заголовки IP-пакетів і кадри канального рівня. Для визначення необхідної пропускної здатності мережі недостатньо використовувати значення, перераховані в таблиці 1.1, але до них слід додати пропускну здатність для накладних витрат - передачі службової інформації. У якості прикладу наведемо розрахунок потрібної пропускної спроможності Ethernet мережі для передачі однієї голосової розмови з використанням кодеку G.711.

Вихідні данні:

– тривалість фрагменту розмови, який передається одним IP-пакетом (визначає затримку передачі голосу) – 20 мс;

– розмір заголовку контейнера протоколу транспортуванняголосу (Real-time Transport Protocol або RTP) – 12 байт;

– розмір заголовку датаграми транспортного протоколу UDP – 8 байт;

– розмір заголовку пакета протоколу IP – 20 байт;

– розмір заголовку та контрольної інформації фрейму Ethernet – 18 байт.

Для фрагмента розмови тривалістю 20 мс потрібно 0,02 х 8000 = 160 вибірок, тобто 160 байт голосових даних. Після додавання накладних витрат на кадри RTP, UDP, IP і Ethernet ми отримуємо загальний розмір кадру 218 байт. Передача фрагментів тривалістю 20 мс вимагає їх відправки зі швидкістю 1 / 0,02 = 50 кадрів в секунду. Для передачі 50 кадрів за 218 байт в секунду потрібно пропускна здатність мережі 10900 байт/с або 87,2 Кбіт/с. Як бачите, фактична необхідна смуга пропускання (87,2 Кбіт/с) на 36% вище за швидкість, необхідної для передачі тільки голосових даних (64 Кбіт/с). Частку накладних витрат можна зменшити, збільшивши тривалість фрагмента, переданого в одному пакеті, але це збільшить затримку передачі голосу і негативно позначиться на якості обслуговування. Слід зазначити, що паралельно з кожним сеансом зв'язку між абонентами RTP для передачі голосу між ними також передаються пакети з

службовою інформацією протоколу управління RTP (RTCP), але їх вклад в загальну необхідну смугу пропускання мережі незначний. При використанні кодеків з високим рівнем економії голосових даних, таких як кодек G.729a, що забезпечує передачу голосу зі швидкістю 8 Кбіт/с, частка службових даних зростає ще більше - при тривалості фрагмента в одному пакеті 20 мс необхідна смуга пропускання складе 31,2 Кбіт/с, тобто накладні витрати будуть 290%, а при збільшенні тривалості фрагмента в пакеті до 30 мс – 23,5 Кбіт/с і 193% відповідно. Однак у порівнянні з кодеком G.711 економія як і раніше значна - 23,5 Кбіт/с проти 87,2 Кбіт/с на кожен телефонний дзвінок.

На закінчення, що стосується кодеків, дуже бажано, щоб кінцеві пристрої розмовляють абонентів підтримували один і той же набір кодеків. Якщо умова відповідності кодеків не виконується, потрібно перетворення між кодеками на шляху голосових даних. Ця процедура вимагає продуктивних сигнальних процесорів, збільшує затримку сигналу і погіршує його якість (оскільки будь-яка обробка погіршує вихідний сигнал). Зазвичай в телефонній мережі, керованої однієї технічної та адміністративної групою, визначається єдиний базовий кодек, за допомогою якого відбуваються всі розмови. У разі зв'язку абонентів різних телефонних мереж з різними кодеками, необхідно підтримувати кодеки обох мереж кінцевими пристроями абонентів (з яких під час розмови буде обраний той, який забезпечує максимальну якість), або для перетворення між кодеками на стику телефонних мереж.

2.3. Протоколи безпеки IP-телефонії

Актуальність безпечної передачі інформації в мережах VoIP зростає з розвитком IP-телефонії. Для забезпечення безпеки IP-телефонії розроблений ряд

методів. Приділимо увагу протоколу розподілу ключів ZRTP, як одному з найбільш перспективних і ефективних.

Послуги VoIP все частіше використовуються в мережах передачі даних. Устаткування для передачі голосової інформації по IP-мереж проводиться низкою відомих компаній, таких як Cisco, LinkSys, AddPac, GrandStream, D-Link і інші. Протоколи сигналізації SIP, H. 323, MGCP, H.248 використовуються в IP-телефонії для встановлення і підтримки з'єднань.

Голос в мережах IP-телефонії передається з використанням протоколів RTP/RTCP (Real-time Transport Protocol та Real-Time Transport Control Protocol), описаних в RFC 3550. Протокол RTP використовується для інкапсуляції в IP-пакети голосової і мультимедійної інформації, а протокол RTCP використовується для передачі керуючої інформації, управління якістю передачі і забезпечення зворотного зв'язку для потоку RTP. Коли один кореспондент дзвонить іншому, спочатку тестується протокол SIP, який дозволяє встановити з'єднання між кореспондентами. Як тільки один з кореспондентів знімає трубку, починає працювати протокол RTP/RTCP.

У зв'язку з загальнодоступністю використовуваних каналів передачі голосової інформації в IP-мережах конфіденційність VoIP-сервісів стає особливо важливою. Є два можливих підходи до цього: формування прямого захищеного каналу між кореспондентами (наприклад, VPN-тунель) і використання спеціальних протоколів безпеки для IP-сервісів.

Перший метод широко використовується при побудові віртуальних корпоративних мереж. Однак для його реалізації кореспонденти повинні підтримувати політику VPN, що не характерно для всіх пристроїв VoIP(Таблиця 2.1).

Спеціальні протоколи для захисту IP-телефонії можна розділити на три категорії:

– протоколи захисту сигналізації (Secured SIP);

– протоколи захисту медіа (SRTP);

– протоколи генерації/поширення ключів для протоколів захисту мультимедіа (MIKEY, SDES, ZRTP, DTLS).

Таблиця 2.1 - Обладнання захищеної IP-телефонії

Виробник	Продукт	Реалізація	Протоколи			Підтримка VPN
			Захист з'єднання	Захист медіатрафіку	Розподілення ключів	
D-Link	DVG-5008S	Апаратна	SIP/TlS	Немає даних	SDES	PPTP
AddPack	AP200	Апаратна	SIP/TlS	SRTP	SDES	Немає даних
LinkSys	Cisco SPA112	Апаратна	SIP/TlS	SRTP	SDES	Без підтримки VPN
Grandstream	GXW400x	Апаратна	SIP/TlS	SRTP	SDES	
UM-Labs	RC-2100	Апаратна	SIP/TlS	SRTP	ZRTP/SDES	
CounterPath	Eye-beam	Програмна	SIP/TlS	SRTP	SDES	
3XC	3CX	Програмна	SIP/TlS	SRTP	Нет данных	
Asterisk	IP PBX	Програмна	SIP/TlS	SRTP	ZRTP/SDES	
FreeSwitch	IP PBX	Програмна	SIP/TlS	SRTP	ZRTP/SDES	
Phoner	Softphone	Програмна	SIP/TlS	SRTP	ZRTP	

Протоколи захисту сигналізації призначені для захисту інформації про телефонні номери та абонентів, а також про підтримувані кодеки.

Для безпечної передачі медіаданих широко використовується протокол реального часу SRTP(Secure Real-time Transport Protocol). Він реалізує функції криптогафічного захисту голосових повідомлень на основі алгоритму шифрування AES. Криптографічний захист голосових пакетів здійснюється в реальному часі і не змінює ймовірносно-часові характеристики протоколу RTP. Але для того, щоб цей алгоритм працював, ви повинні спочатку згенерувати криптографічні ключі. Це завдання вирішується протоколом розподілу ключів.

Основні завдання протоколу SRTP:

– шифрування переданих голосових даних;

– аутентифікація переданих повідомлень;

– захист від передачі повторюваних пакетів;

– збереження пропускної здатності, стискання заголовків RTP.

Протокол SRTP містить два компоненти – фактичний протокол SRTP для передачі і криптографічного захисту мультимедійних файлів і протокол SRTCP (протокол безпечного управління передачею в реальному часі) для управління сеансами мультимедіа. Алгоритми аутентифікації і шифрування можуть виконуватися незалежно один від одного. Отже, опція можлива, коли шифрування відключено і SRTP використовується тільки для аутентифікації. Однак аутентифікація повідомлень в SRTP є обов'язковим і не може бути відключена. Протоколи третьої групи призначені для генерації і розподілу ключів шифрування медіаінформації між кореспондентами. Ви можете використовувати протоколи MIKEY, SDES, ZRTP, DTLS для вирішення цієї проблеми.

Для протоколу SRTP кореспондентам, які беруть участь в обміні, потрібен ключовий матеріал. Специфікація SRTP описує отримання ключового матеріалу на основі головного ключа і додаткового сеансового ключа, але не описує обмін ключами між користувачами. Пропонується використовувати окремо

розроблені протоколи. Одним з таких протоколів, який дозволяє обмінюватися ключами для SRTP між кореспондентами по відкритих каналах зв'язку, є протокол ZRTP. До завдань цього протоколу входять:

– генерація ключових параметрів SRTP-сесії;

– забезпечення конфіденційності повідомлень протоколу;

– аутентифікація кореспондентів;

– захист від атаки-вторгнення посередині як з використанням, так і без використання інфраструктури відкритих ключів.

При встановленні захищеного VoIP-з'єднання протокол ZRTP працює відразу після завершення роботи протоколу SIP. І тільки після успішного завершення роботи протоколу ZRTP починається передача медіатрафіку по протоколу SRTP.

Протокол ZRTP передбачає роботу кореспондентів за принципом точка-точка, з можливістю використання протоколу в багатопотоковому режимі, коли необхідно організувати кілька захищених медіапотоків (наприклад, голосу та відео). Також є можливість працювати з легальним посередником, яким може виступати, наприклад, корпоративна телефонна станція. Для роботи з протоколом ZRTP кожен з кореспондентів повинен мати унікальний ідентифікатор (ZID), а обладнання повинно підтримувати однакові набори криптографічних алгоритмів.

Особливістю ZRTP є те, що всі дані передаються в пакетах, подібних RTP. Це змушує несумісні з ZRTP пристрої просто відхиляти пакети ZRTP, тому вони не впливають на встановлене з'єднання.

Для перевірки цілісності кожне передане повідомлення ZRTP містить код CRC, а також код аутентифікації повідомлення (MAC), який обчислюється з використанням хеш-функцій. Аргументом хеш-функції є захищене повідомлення, ключ – це спеціальний параметр, який передається (для більшості повідомлень) в наступному повідомленні. Алгоритм гешування узгоджений на першій фазі протоколу. (Таблиця 2.2).

Помилка в хеш-повідомленні зазвичай означає виявлення атаки MiTM(Man in The Middle), оскільки спотворення через помилки каналу виявляються при перевірці контрольної суми CRC пакета ZRTP.

В таблиці 2.2 показано криптографічні набори протоколу ZRTP.

Таблиця 2.2 - Криптографічні набори протоколу ZRTP

Криптографічні функції	Обов'язкова підтримка		Опціональна підтримка	
	Алгоритм	Довжина ключа, біт	Алгоритм	Довжина ключа, біт
Шифрування даних	AES	128	AES	256
			TwoFish	128, 192, 256
Автентифікація повідомлень	HMAC-SHA1	32, 80	Skein-512-MAC	32, 64
Хеш-функція	SHA-256, SHA-384	256, 384	NIST SHA-3	256, 384
Обмін ключами	DH 3k	–	EC 25, EC 38, DH 2k	–
Автентифікація кореспондентів	PGP X.509v3	–	–	–

Для аутентифікації кореспондентів, а також виключення атаки MiTM протокол ZRTP предбачає використання короткого аутентифікаційного рядка(SAS, Short Authentication String). SAS розраховується обома кореспондентами за спеціальним алгоритмом і може використовуватися для словесного порівняння безпосередньо під час з'єднання (побачив-сказав-порівняв). Для контролю цілісності кожне передане повідомлення ZRTP містить код CRC, а також код аутентифікації MAC-повідомлення (Message Authentication Code), який вираховується за допомогою хеш-функцій. Як аргумент хеш-функції використовується захищене повідомлення, ключ - це

спеціальний параметр, який передається (для більшості повідомлень) в наступному повідомленні. Алгоритм хешування узгоджений на першій фазі протоколу. Помилка в хеш-повідомленні зазвичай означає виявлення атаки MiTM, оскільки спотворення через помилки каналу виявляються при перевірці контрольної суми CRC пакета ZRTP.

2.4 Висновки до розділу

IP-телефонія – це один з напрямків передачі даних, де важлива динаміка передачі сигналу. Успішність конкуренції з традиційними телефонними мережами забезпечується сучасними методами кодування і передачі інформації, а також збільшенням пропускної здатності каналу. Основні складові якості IP-телефонії є:

– можливість користувача зв'язуватися і розмовляти з іншим користувачем в реальному часі

– якість мови(розбірливість, рівень гучності);

– якість сигналізації;

– час встановлення та завершення виклику;

– чистота і тональність мови.

Для зменшення обсягу голосових даних використовується стиснення, так звані – кодеки. Спочатку може здатись, що кодеки схожі на програми архівування такі як WinRar, 7z, але це далеко не так. Основні відмінності:

– програми архівування опрацьовують весь файл повністю, а кодеки оброблять дані, які постійно надходять;

– збільшення часу архівування зазвичай некритично, на відмінно від кодеків, в яких збільшення часу обробки голосу зазвичай погіршує зв’язок;

– програми архівування забезпечують збереження 100% інформації, в той час як кодеки можуть привносити незначне погіршення якості з метою економії даних.

Для безпечної передачі медіаданих широко використовується протокол реального часу SRTP. Основні завдання протоколу SRTP:

– шифрування переданих голосових даних;

– аутентифікація переданих повідомлень;

– захист від передачі повторюваних пакетів;

– збереження пропускної здатності, стискання заголовків RTP.

Протокол ZRTP, який дозволяє обмінюватися ключами для SRTP між кореспондентами по відкритих каналах зв'язку. До завдань цього протоколу входять:

– генерація ключових параметрів SRTP-сесії;

– забезпечення конфіденційності повідомлень протоколу;

– аутентифікація кореспондентів;

– захист від MiTM як з використанням, так і без використання інфраструктури відкритих ключів.

При встановленні захищеного VoIP-з'єднання протокол ZRTP працює відразу після завершення роботи протоколу SIP. І тільки після успішного завершення роботи протоколу ZRTP починається передача медіатрафіку по протоколу SRTP.

3 IP-ТЕЛЕФОНІЯ НА БАЗІ ASTERISK

3.1. Встановлення ОС, налаштування середовища для Asterisk та SIP

Asterisk – платформа комп'ютерної телефонії, що поширюється за ліцензією GPU GPL. Завдяки комерційній підтримці ліцензія GNU GPL Asterisk активно розвивається і підтримується тисячами людей з всьої планети.

Для налаштування системи Asterisk потрібно встановити ОС Linux. В моєму випадку ОС було встановлено з образу CentOS-7-i386-Minimal-1611.iso.

Спочатку підготовуємо середовище для встановлення(рисунок 3.1), розширюємо bash, встановлюємо vim та пакет wget.

```
yum install bash-completion vim-enhanced wget
```

Рисунок 3.1. – Команда для налаштування середовища.

Встановлюємо утиліти для компіляції програм(Рисунок 3.2) та оновлюємо пакети в системі до останніх версій(Рисунок 3.3).

```
yum groupinstall -y Development Tools
```

Рисунок 3.2. – Встановлення утиліт

```
yum update
```

Рисунок 3.3. – Оновлення пакетів

Для подальшої роботи потрібно відключити SElinux. Для цього в файлі /etc/sysconfig/selinux потрібно вказати SELINUX=disabled. Після чого перезавантажуємо систему Linux командою reboot.

Подальше налаштування потребує збирання залежностей Asterisk. Спочатку встановимо DAHDI (Digium/Asterisk Hardware Device Interface)(Рисунок 3.4), LibPRI для підтримки системи сигналізації ISDN(Рисунок 3.5) та PJProject для підтримки драйвера PJSIP(Рисунок 3.6).

```
cd /usr/src
wget http://downloads.asterisk.org/pub/telephony/dahdi-linux-complete/dahdi-linux-complete-current.tar.gz
tar xvfz dahdi-linux-complete-current.tar.gz
rm -f dahdi-linux-complete-current.tar.gz
cd dahdi-linux-complete-2.11.1+2.11.1/
make all && make install && make config
```

Рисунок 3.4. – Встановлення DAHDI

```
cd /usr/src
wget http://downloads.asterisk.org/pub/telephony/libpri/libpri-current.tar.gz
tar xvfz libpri-current.tar.gz
rm -f libpri-current.tar.gz
cd libpri-1.6.0/
make && make install
```

Рисунок 3.5. – Підключення бібліотек libPRI

```
cd /usr/src
wget http://www.pjsip.org/release/2.6/pjproject-2.6.tar.bz2
tar xvfj pjproject-2.6.tar.bz2
rm -f pjproject-2.6.tar.bz2
cd pjproject-2.6
./configure CFLAGS="-DNDEBUG -DPJ_HAS_IPV6=1" --prefix=/usr --enable-shared --disable-video --disable-sound
make dep && make && make install
```

Рисунок 3.6. – Встановлення PJProject драйвера

Очікуємо завершення встановлення необхідних програм для подальшого налаштування(Рисунок 3.7).

```
libpjsua2.so.2 (libc6) => /lib/libpjsua2.so.2
libpjsua2.so (libc6) => /lib/libpjsua2.so
libpjsua.so.2 (libc6) => /lib/libpjsua.so.2
libpjsua.so (libc6) => /lib/libpjsua.so
libpjsip.so.2 (libc6) => /lib/libpjsip.so.2
libpjsip.so (libc6) => /lib/libpjsip.so
libpjsip-ua.so.2 (libc6) => /lib/libpjsip-ua.so.2
libpjsip-ua.so (libc6) => /lib/libpjsip-ua.so
libpjsip-simple.so.2 (libc6) => /lib/libpjsip-simple.so.2
libpjsip-simple.so (libc6) => /lib/libpjsip-simple.so
libpjnath.so.2 (libc6) => /lib/libpjnath.so.2
libpjnath.so (libc6) => /lib/libpjnath.so
libpjmedia.so.2 (libc6) => /lib/libpjmedia.so.2
libpjmedia.so (libc6) => /lib/libpjmedia.so
libpjmedia-videodev.so.2 (libc6) => /lib/libpjmedia-videodev.so.2
libpjmedia-videodev.so (libc6) => /lib/libpjmedia-videodev.so
libpjmedia-codec.so.2 (libc6) => /lib/libpjmedia-codec.so.2
libpjmedia-codec.so (libc6) => /lib/libpjmedia-codec.so
libpjmedia-audiodev.so.2 (libc6) => /lib/libpjmedia-audiodev.so.2
libpjmedia-audiodev.so (libc6) => /lib/libpjmedia-audiodev.so
libpjlib-util.so.2 (libc6) => /lib/libpjlib-util.so.2
libpjlib-util.so (libc6) => /lib/libpjlib-util.so
libpj.so.2 (libc6) => /lib/libpj.so.2
libpj.so (libc6) => /lib/libpj.so
```

Рисунок 3.7. – Процес встановлення драйверів та бібліотек

Для наступних настройок потрібно встановити бібліотеку jansson для підтримки формату json. Команда для виконання встановлення зображена на рисунку 3.8.

```
cd /usr/src
wget -O jansson.tar.gz http://www.digip.org/jansson/releases/jansson-2.10.tar.gz
tar vxfz jansson.tar.gz
rm -f jansson.tar.gz
cd jansson-2.10/
autoreconf --force --install
./configure
make && make install
```

Рисунок 3.8. – Команда для встановлення бібліотеки

Далі вибираємо налаштування через menuselect(рисунок 3.9), вибираємо підтримку MySQL(Рисунок 3.10) та встановлюємо Asterisk(Рисунок 3.11).

```
cd /usr/src
wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-13-current.tar.gz
tar xvfz asterisk-13-current.tar.gz
rm -f asterisk-13-current.tar.gz
cd asterisk-13.15.0/
contrib/scripts/get_mp3_source.sh
contrib/scripts/install_prereq install
./configure
make menuselect
```

Рисунок 3.9. –Вибір налаштувань в menuselect для Asterisk.

```
• Add-ons: format_mp3, res_config_mysql, app_mysql и cdr_mysql
```

Рисунок 3.10. – Підключення MySQL

```
make
make install
make config
ldconfig
```

Рисунок 3.11. Безпосереднє встановлення Asterisk.

Для роботи з даною платформою потрібно створити конфігураційні файли(Рисунок 3.12), користувача(Рисунок 3.13), та в файлі /etc/sysconfig/asterisk розкоментувати рядки(Рисунок 3.14).

```
make samples
```

Рисунок 3.12. – Створення конфігурайних файлів

```
useradd -m asterisk
chown asterisk. /var/run/asterisk
chown -R asterisk. /etc/asterisk
chown -R asterisk. /var/{lib,log,spool}/asterisk
chown -R asterisk. /usr/lib/asterisk
```

Рисунок 3.13. – Створення користувача

```
AST_USER="asterisk"
AST_GROUP="asterisk"
```

Рисунок 3.14. – Рядки, що потрібно розкоментувати

Після чого запускаємо Asterisk командою «service asterisk start» та перевіряємо роботу командою «asterisk –r». Результат перевірки зображено на рисунку 3.15.

```
Asterisk 13.15.0, Copyright (C) 1999 - 2014, Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 13.15.0 currently running on asterisk-centos (pid = 25939)
asterisk-centos*CLI>
```

Рисунок 3.15. – Результат перевірки

Налаштуємо журнал подій, який необхідний для роботи програми fail2ban. Для цього у файлі /etc/asterisk/logger.conf потрібно розкоментувати рядок «dateformat=%F %T ; ISO 8601 date format». Після чого включаємо Asterisk Security Framework у файлі logger.conf, аналогічно до попереднього розкоментовуємо рядок «security => security». В даному випадку інформація буде записуватись в файл security. У файлі /etc/asterisk/asterisk.conf змінюємо рівень деталізації на 9 в рядку «verbose = 9» після чого перезапускаємо Asterisk і перевіряємо командою «asterisk-centos*CLI> core show settings»(Рисунок 3.16).

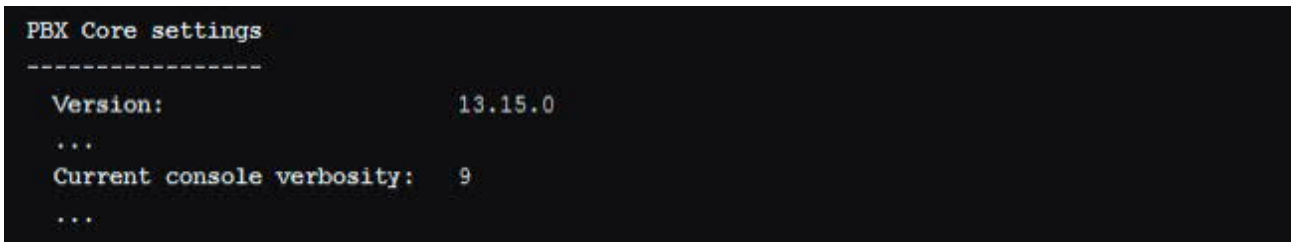

Рисунок 3.16. – Результат виконання перевірки

Після перевірки є доцільним налаштувати ротацію логів. Ротація логів – це процес архівації логів, видалення застарілих логів і всього що з цього витікає. Даний процес потрібний для того, щоб у Вас не закінчилось місце на диску від переповнення тими самими логами, а також служба потрібна для захисту від дублювання логів, особливо, кол лог-файл займає багато місця.

В папці «/etc/logrotate.d» створюємо файл asterisk(Рисунок 3.17).

```
/var/log/asterisk/security
/var/log/asterisk/messages
{
        daily
        rotate 30
        compress
        missingok
        notifempty
        create 644 asterisk asterisk
        postrotate
                asterisk -rx 'reload'
        endscript
}
```

Рисунок 3.17. – Створення файлу asterisk

Запускаємо logrotate для перевірки його роботи командою «logrotate -f /etc/logrotate.d/asterisk» та командою «ls -l /var/log/asterisk/» пеервіряємо його роботу. Результат перевірки зображений на рисунку 3.18.

```
итого 20
drwxr-xr-x 2 asterisk asterisk   6 Апр 22 21:32 cdr-csv
drwxr-xr-x 2 asterisk asterisk   6 Апр 22 21:32 cdr-custom
drwxr-xr-x 2 asterisk asterisk   6 Апр 22 21:32 cel-custom
-rw-r--r-- 1 asterisk asterisk 994 Апр 23 12:57 messages
-rw-r--r-- 1 asterisk asterisk 542 Апр 23 12:50 messages.1.gz
-rw-r--r-- 1 root     root     432 Апр 23 12:57 queue_log
-rw-r--r-- 1 asterisk asterisk 244 Апр 23 12:57 security
-rw-r--r-- 1 asterisk asterisk 131 Апр 23 12:50 security.1.gz
```

Рисунок 3.18. – Результат перевірки logrotate

Далі будемо створювати користувачів, для цього сворюємо файл users.conf(Рисунок 3.19)

```
mkdir /etc/asterisk/sip
touch /etc/asterisk/sip/users.conf
```

Рисунок 3.19. – Створення файлу users.conf

Після чого створюємо шаблон та вносимо користувачів(Рисунок 3.20).

```
[users](!)
type=friend
nat=no
dtmfmode=rfc2833
qualify=yes
canreinvite=no
disallow=all
allow=alaw
allow=ulaw
call-limit=2
deny=0.0.0.0/0.0.0.0
permit=192.168.1.0/24

[101](users)
defaultuser=101
secret=101
context=manager
host=dynamic

[102](users)
defaultuser=102
secret=102
context=manager
host=dynamic

[201](users)
defaultuser=201
secret=201
context=sales
host=dynamic
```

Рисунок 3.20. – Створення користувачів та шаблону

Файл з налаштуваннями користувачів підключаємо в sip.conf командою «#include sip/users.conf». Після чого перезапускаємо та перевіряємо налаштування(Рисунок 3.21) з списком користувачів(Рисунок 3.22).

```
asterisk-centos*CLI> sip reload
 Reloading SIP
  == Parsing '/etc/asterisk/sip.conf': Found
  == Parsing '/etc/asterisk/sip/users.conf': Found
  == Parsing '/etc/asterisk/users.conf': Found
  == Using SIP CoS mark 4
  == Parsing '/etc/asterisk/sip_notify.conf': Found
```

Рисунок 3.21. – Перевірка налаштувань

```
asterisk-centos*CLI> sip show users
Username                  Secret          Accountcode      Def.Context     ACL  Forcerport
101                       101                              manager         Yes  No
102                       102                              manager         Yes  No
204                       204                              sales           Yes  No
203                       203                              sales           Yes  No
202                       202                              sales           Yes  No
201                       201                              sales           Yes  No
```

Рисунок 3.22. – Перевірка списку користувачів

Потрібно підключити провайдера для подальших налаштувань. Створюємо файл trunk.conf для налаштувань sip trunk(Рисунок 3.23).

```
[zadarma]
host=sip.zadarma.com
insecure=invite,port
type=friend
fromdomain=sip.zadarma.com
disallow=all
allow=alaw
allow=ulaw
dtmfmode=auto
secret=PASSWORD
defaultuser=74XXXX
trunkname=zadarma
fromuser=74XXXX
callbackextension=74XXXX
context=zadarma-in
qualify=400
directmedia=no
nat=force_rport,comedia
```

Рисунок 3.23. – Налаштування в файлі trunk.conf

Підключаємо файл з налаштуваннями sip trunk в sip.conf командою «#include trunk/trunk.conf».

Перевіряємо налаштування та перевіряємо список пірів(Рисунок 3.24)

```
asterisk-centos*CLI> sip show peers
Name/username             Host                                  Dyn Forcerport Comedia    ACL Port
101/101                   (Unspecified)                          D  No         No          A  0
102/102                   (Unspecified)                          D  No         No          A  0
201/201                   (Unspecified)                          D  No         No          A  0
202/202                   (Unspecified)                          D  No         No          A  0
203/203                   (Unspecified)                          D  No         No          A  0
204/204                   (Unspecified)                          D  No         No          A  0
301/301                   (Unspecified)                          D  No         No          A  0
302/302                   (Unspecified)                          D  No         No          A  0
401/401                   (Unspecified)                          D  No         No          A  0
402/402                   (Unspecified)                          D  No         No          A  0
501/501                   192.168.1.101                          D  No         No          A  5060
zadarma/74XXXX            185.45.152.161                            Yes        Yes            5060
12 sip peers [Monitored: 2 online, 10 offline Unmonitored: 0 online, 0 offline]
```

Рисунок 3.24. – Список пірів

3.2. Налаштування логіки обробки дзвінків та створення голосового меню

Щоб продовжити роботу з телефонією потрібно налаштувати логіку дзвінків, в моєму випадку, буде налаштовано Dialplan. Для цього створюємо контексти для обробки дзвінків:

– call-local – внутрішні дзвінки;

– call-in – вхідні дзвінки;

– call-out – вихідні дзвінки.

Після чого робимо резервну копію файлу extensions.conf і створюємо новий файл для налаштування Dialplan.(Рисунок 3.25).

```
mv extensions.conf extensions.conf.default
touch extensions.conf
```

Рисунок 3.25. Створення нового файлу

Після чого вносимо наступні контексти, зображені на рисунку 3.26 в новий файл.

```
[general]
static=yes
writeprotect=no

[globals]

[default]

;внутрішні лінії
[call-local]
exten => _XXX,1,Dial(SIP/${EXTEN})
exten => _XXX,n,Hangup()

;вихідні дзвінки на зовнішні лінії
[call-out]
exten => _XXX.,1,Dial(SIP/${EXTEN}@zadarma)
exten => _XXX.,n,Hangup()

;вхідні дзвінки з зовнішніх ліній
[call-in]
exten => YYYYYY,1,Dial(SIP/101)

[manager]
include => call-local
include => call-out
```

Рисунок 3.26. – Файл extensions

Перевіряємо дзвінки по внутрішній лінії(Рисунок 3.27).

```
asterisk-centos*CLI>
  == Using SIP RTP CoS mark 5
    -- Executing [102@manager:1] Dial("SIP/101-0000002a", "SIP/102") in new stack
  == Using SIP RTP CoS mark 5
    -- Called SIP/102
    -- SIP/102-0000002b is ringing
    -- SIP/102-0000002b answered SIP/101-0000002a
    -- Channel SIP/102-0000002b joined 'simple_bridge' basic-bridge <70ea55b8-8b22-42e3-9add-50c67bdf8
    -- Channel SIP/101-0000002a joined 'simple_bridge' basic-bridge <70ea55b8-8b22-42e3-9add-50c67bdf8
       > Bridge 70ea55b8-8b22-42e3-9add-50c67bdf80ab: switching from simple_bridge technology to native
       > Locally RTP bridged 'SIP/101-0000002a' and 'SIP/102-0000002b' in stack
       > Locally RTP bridged 'SIP/101-0000002a' and 'SIP/102-0000002b' in stack
    -- Channel SIP/102-0000002b left 'native_rtp' basic-bridge <70ea55b8-8b22-42e3-9add-50c67bdf80ab>
    -- Channel SIP/101-0000002a left 'native_rtp' basic-bridge <70ea55b8-8b22-42e3-9add-50c67bdf80ab>
  == Spawn extension (manager, 102, 1) exited non-zero on 'SIP/101-0000002a'
  == Using SIP RTP CoS mark 5
    -- Executing [101@manager:1] Dial("SIP/102-0000002c", "SIP/101") in new stack
  == Using SIP RTP CoS mark 5
    -- Called SIP/101
    -- SIP/101-0000002d is ringing
    -- SIP/101-0000002d answered SIP/102-0000002c
    -- Channel SIP/101-0000002d joined 'simple_bridge' basic-bridge <10e80012-fb40-47ab-be85-7d76cb584
    -- Channel SIP/102-0000002c joined 'simple_bridge' basic-bridge <10e80012-fb40-47ab-be85-7d76cb584
       > Bridge 10e80012-fb40-47ab-be85-7d76cb584588: switching from simple_bridge technology to native
       > Locally RTP bridged 'SIP/102-0000002c' and 'SIP/101-0000002d' in stack
       > Locally RTP bridged 'SIP/102-0000002c' and 'SIP/101-0000002d' in stack
    -- Channel SIP/101-0000002d left 'native_rtp' basic-bridge <10e80012-fb40-47ab-be85-7d76cb584588>
    -- Channel SIP/102-0000002c left 'native_rtp' basic-bridge <10e80012-fb40-47ab-be85-7d76cb584588>
  == Spawn extension (manager, 101, 1) exited non-zero on 'SIP/102-0000002c'
```

Рисунок 3.27. – Перевірка внутрішньої лінії

Перевірка дзвінків на зовнішні лінії(Рисунок 3.28).

```
sterisk-centos*CLI>
 == Using SIP RTP CoS mark 5
   -- Executing [XXXXXX@manager:1] Dial("SIP/101-00000035", "SIP/XXXXXX@zadarma") in new stack
 == Using SIP RTP CoS mark 5
   -- Called SIP/XXXXXX@zadarma
   -- SIP/zadarma-00000036 is ringing
   -- SIP/zadarma-00000036 answered SIP/101-00000035
   -- Channel SIP/zadarma-00000036 joined 'simple_bridge' basic-bridge <d19036d2-735c-4c43-b2b5-9ac8d3
   -- Channel SIP/101-00000035 joined 'simple_bridge' basic-bridge <d19036d2-735c-4c43-b2b5-9ac8d3b040
      > Bridge d19036d2-735c-4c43-b2b5-9ac8d3b040f6: switching from simple_bridge technology to native
      > Locally RTP bridged 'SIP/101-00000035' and 'SIP/zadarma-00000036' in stack
      > Locally RTP bridged 'SIP/101-00000035' and 'SIP/zadarma-00000036' in stack
   -- Channel SIP/101-00000035 left 'native_rtp' basic-bridge <d19036d2-735c-4c43-b2b5-9ac8d3b040f6>
 == Spawn extension (manager, XXXXXX, 1) exited non-zero on 'SIP/101-00000035'
   -- Channel SIP/zadarma-00000036 left 'native_rtp' basic-bridge <d19036d2-735c-4c43-b2b5-9ac8d3b040f
```

Рисунок 3.28. – Результат перевірки

Далі додаємо функцію запису дзвінків. За замовчуванням фунцкція включена але є можливість її виключити під час розмови. Записи будуть зберігатись в формат mp3. Для підтримки цього формату потрібно встановити в систему пакет lame. Команда для встановлення зображена на рисунку 3.29.

```
cd /usr/src/
wget https://downloads.sourceforge.net/project/lame/lame/3.99/lame-3.99.5.tar.gz
tar vxfz lame-3.99.5.tar.gz
rm -f lame-3.99.5.tar.gz
cd lame-3.99.5
./configure
make && make install
```

Рисунок 3.29. – Встановлення пакету lame

В нашій умовній компанії буде використовуватись 3 рівня:

– головне меню(1-й рівень) – вітання та пропозиція дзвінку на додатковий номер для набору в конкретний відділ компанії;

– меню відділу продаж(2-й рівень) – пропозиція зв’язатись з фахівцем конкретної групи;

– меню відділу закупівлі(2-й рівень) – пропозиція зв’язатись з фахівцем із закупівель;

– меню вибору додаткового номеру(3-й рівень)

– меню для питань пов’язаних з доставкою(2-й рівень) – пропозиція з’єднатись з фахівцем для уточнення питань комплектації та доставки.

Описуємо вищевказане меню(Додаток А).

Файли для голосового меню зберігаємо в директорію /var/lib/asterisk/sounds/en/ivr(рисунок 3.30).

```
[root@asterisk-centos en]# ls -l /var/lib/asterisk/sounds/en/ivr
итого 1156
-rw-r--r-- 1 asterisk asterisk 171404 Май  7 10:56 buyingmenu-1.wav
-rw-r--r-- 1 asterisk asterisk 158924 Май  7 10:57 buyingmenu-2.wav
-rw-r--r-- 1 asterisk asterisk 105164 Май  7 10:54 holiday.wav
-rw-r--r-- 1 asterisk asterisk  42124 Май  7 11:00 input-order-number.wav
-rw-r--r-- 1 asterisk asterisk 208524 Май  7 10:52 mainmenu.wav
-rw-r--r-- 1 asterisk asterisk  40204 Май  7 10:53 make-a-choice.wav
-rw-r--r-- 1 asterisk asterisk 239564 Май  7 10:55 salesmenu.wav
-rw-r--r-- 1 asterisk asterisk 175244 Май  7 10:58 warehousemenu.wav
-rw-r--r-- 1 asterisk asterisk  30284 Май  7 10:51 welcome.wav
```

Рисунок 3.30. – Файли голосового меню

Після чого слідує перевірка даних налаштувань з голосовим меню(Рисунок 3.31).

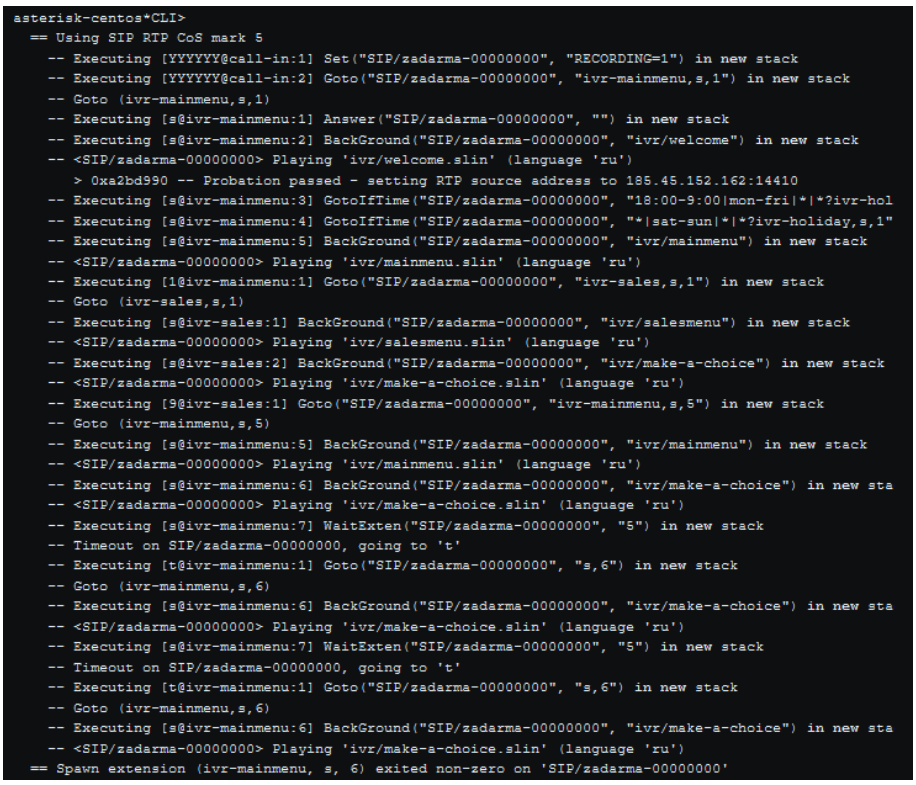

Рисунок 3.31. – Перевірка голосового меню

Потрібно налаштувати вивід голосових повідомлень. Для програвання встановимо пакет Festival.(Рисунок 3.32).

```
cd /usr/src
wget http://www.cstr.ed.ac.uk/downloads/festival/2.4/speech_tools-2.4-release.tar.gz
wget http://www.cstr.ed.ac.uk/downloads/festival/2.4/festival-2.4-release.tar.gz
tar zxvf festival-2.4-release.tar.gz
tar zxvf speech_tools-2.4-release.tar.gz
cd speech_tools
./configure
make && make install
cd ..
cd festival
./configure
make && make install
```

Рисунок 3.32. – встановлення пакету Festival

Додамо шлях до бінарного файлу festival, Команда: «export PATH=$PATH:/usr/src/festival/bin/». Встановлюємо мовні файли на рисунку 3.33.

```
mkdir /usr/src/festival/lib/voices/
mkdir /usr/src/festival/lib/voices/russian/
cd /usr/src/
wget http://sourceforge.net/projects/festlang.berlios/files/msu_ru_nsh_clunits-0.5.tar.bz2
tar xjfv msu_ru_nsh_clunits-0.5.tar.bz2
mv /usr/src/msu_ru_nsh_clunits/ /usr/src/festival/lib/voices/russian
```

Рисунок 3.33. – Встановлення мовних файлів

Далі додаємо на початок файлу /usr/src/festival/lib/languages.scm наступний код на рисунку 3.34.

```
((equal? language 'russian)
    (language_russian))
```

Рисунок 3.34. – Фрагмент потрібного коду

Конфігураційний файл /etc/asterisk/festival.conf на рисунку 3.35.

```
[general]
host=localhost
port=1314
usecache=yes
cachedir=/var/lib/asterisk/festivalcache/
festivalcommand=(tts_textasterisk "%s" 'file)(quit)\n
```

Рисунок 3.35. – Конфігураційний файл

Для перевірки статусу замовлення можна використовувати скрипт checkstatus.php(Рисунок 3.36)

```
<?php
$conn = mysql_connect("localhost", "mysql_user", "mysql_password");
mysql_select_db("myshop");
//пошук статуса за номером телефону клієнта і номером замовлення
$sql = "SELECT status FROM orders WHERE phone = ".$argv[1]." AND order_id = ".$argv[2];
$result = mysql_query($sql);
$row = mysql_fetch_assoc($result);
echo 'SET VARIABLE ORDERSTATUS '.$row["status"];
?>
```

Рисунок 3.36. – Скрипт checkstatus

3.3. Деталізований звіт про виклики та додаткові функції Asterisk

Для збереження всіх даних по будь-якому дзвінку, одних логів буде недостатньо так як в такому випадку вони будуть займати великий простір на накопичувачі. Для вирішення цього питання встановимо MySQL сервер. В SQL всі дані будуть зберігатись більш структуровано і сама база даних буде займати менше простору так як все буде зберігатись в один файл. Команда для встановлення MySQL server на рисунку 3.37.

```
wget https://dev.mysql.com/get/mysql57-community-release-el7-11.noarch.rpm
rpm -ivh mysql57-community-release-el7-11.noarch.rpm
yum install mysql-server
```

Рисунок 3.37. – Встановлення MySQL

Перегляд статистики дзвінків буде відбуватись в веб-інтерфейсі CDR Viever. Команда для встановлення та налаштування веб-сервера на рисунку 3.38.

```
cd /usr/src/
wget https://nginx.org/download/nginx-1.13.0.tar.gz
tar vxfz nginx-1.13.0.tar.gz
cd nginx-1.13.0/
./configure
make && make install
useradd -r nginx
ln -s /usr/local/nginx/conf/ /etc/nginx
ln -s /usr/local/nginx/sbin/nginx /usr/sbin/nginx
wget -O /etc/init.d/nginx https://gist.github.com/sairam/5892520/raw/b8195a71e944d46271c8a49f2717f70bc
chmod +x /etc/init.d/nginx
```

Рисунок 3.38. – Встановлення та налаштування веб-сервера

Створюємо файл /lib/systemd/system/nginx.service(Рисунок 3.39).

```
[Unit]
Description=The NGINX HTTP and reverse proxy server
After=syslog.target network.target remote-fs.target nss-lookup.target

[Service]
Type=forking
PIDFile=/run/nginx.pid
ExecStartPre=/usr/sbin/nginx -t
ExecStart=/usr/sbin/nginx
ExecReload=/bin/kill -s HUP $MAINPID
ExecStop=/bin/kill -s QUIT $MAINPID
PrivateTmp=true

[Install]
WantedBy=multi-user.target
Запускаем сервер:
systemctl enable nginx
systemctl start nginx
```

Рисунок 3.39. – Створення файлу

Встановлюємо PHP командою «yum install php-fpm systemctl start php-fpm».

Налаштування веб-сервера на рисунку 3.40.

```
user  nginx;
worker_processes  1;
error_log  logs/error.log;
pid        /run/nginx.pid;
events {
    worker_connections  1024;
}
http {
    include       mime.types;
    default_type  application/octet-stream;
    sendfile        on;
    keepalive_timeout  65;
    server {
        listen       80;
        server_name  192.168.1.201;
          root /var/www;
        location / {
            index  index.html index.htm;
        }
        error_page   500 502 503 504  /50x.html;
        location = /50x.html {
            root   html;
        }
        location ~* \.php$ {
            include fastcgi_params;
            fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
            fastcgi_pass 127.0.0.1:9000;
            try_files $uri @yii =404;
        }
    }
}
```

Рисунок 3.40. – Налаштування веб-сервера

Встановлюємо програму для керування БД. Команда для встановлення «cd /var/www/ wget https:// github.com /vrana /adminer /releases /download /v4.3.1 /adminer-4.3.1-mysql.php -O adminer.php». Входимо в adminer за адресою 192.168.0.201/adminer.php, створюємо базу asteriskcdr і користувача з дозволомна запис даний в цю базу asteriskuser, а також таблицю, куди будуть зберігатись всі дані(Рисунок 3.41).

```
CREATE TABLE `cdr` (
  `id` int(11) unsigned NOT NULL auto_increment,
  `calldate` datetime NOT NULL default '0000-00-00 00:00:00',
  `clid` varchar(80) NOT NULL default '',
  `src` varchar(80) NOT NULL default '',
  `dst` varchar(80) NOT NULL default '',
  `dcontext` varchar(80) NOT NULL default '',
  `channel` varchar(80) NOT NULL default '',
  `dstchannel` varchar(80) NOT NULL default '',
  `lastapp` varchar(80) NOT NULL default '',
  `lastdata` varchar(80) NOT NULL default '',
  `duration` int(11) NOT NULL default '0',
  `billsec` int(11) NOT NULL default '0',
  `start` datetime NULL default NULL,
  `answer` datetime NULL default NULL,
  `end` datetime NULL default NULL,
  `disposition` varchar(45) NOT NULL default '',
  `amaflags` int(11) NOT NULL default '0',
  `accountcode` varchar(20) NOT NULL default '',
  `uniqueid` varchar(32) NOT NULL default '',
  `userfield` varchar(255) NOT NULL default '',
  PRIMARY KEY  (`id`),
  KEY `calldate` (`calldate`),
  KEY `accountcode` (`accountcode`),
  KEY `uniqueid` (`uniqueid`),
  KEY `dst` (`dst`),
  KEY `src` (`src`)
);
```

Рисунок 3.41. – Створення бази, користувача і таблиці

Налаштовуємо підключення до MySQL в файлі /etc/asterisk/cdrmysql.conf(Рисунок 3.42).

```
[global]
hostname=localhost
dbname=asteriskcdr
table=cdr
password=asterisk_password
user=asterisk_user
port=3306
```

Рисунок 3.42. – Команди для підключення MySQL

Відключаємо стандартне логування дзвінків в файлі /etc/asterisk/cdr.conf. Для цього потрібно закоментувати рядки на рисунку 3.43.

```
;[csv]
;usegmtime=yes    ; log date/time in GMT.  Default is "no"
;loguniqueid=yes  ; log uniqueid.  Default is "no"
;loguserfield=yes ; log user field.  Default is "no"
;accountlogs=yes  ; create separate log file for each account code. Default is "yes"
```

Рисунок 3.43. – Команди в файлі cdr.conf

Перезапускаємо Asterisk, та встановлюємо CDR Viever(Рисунок 3.44).

```
cd /var/www/html
wget https://github.com/g613/asterisk-cdr-viewer/raw/master/asterisk-cdr-viewer-latest.tgz
tar xzfv asterisk-cdr-viewer-latest.tgz
```

Рисунок 3.44. – Встановлення CDR Viever

Налаштовуємо підключення до бази даних в файлі include/config.inc.php(Рисунок 3.45).

```
$db_type = 'mysql';
$db_host = 'localhost';
$db_port = '3306';
$db_user = 'asterisk_user';
$db_pass = 'asterisk_password';
$db_name = 'asteriskcdr';
$db_table_name = 'cdr';
$db_options = array();
```

Рисунок 3.45. – Підключення до БД

Розширюємо макрос запису дзвінків для можливості роботи з базою даних в файлі /etc/extension.conf(Рисунок 3.46).

```
;MixMonitor
[macro-recording]
exten => s,1,GoToIf($["${RECORDING}" = "1"]?yes:no);
exten => s,n(yes),Set(fname=${STRFTIME(${EPOCH},,%Y)}/${STRFTIME(${EPOCH},,%Y-%m)}/${STRFTIME(${EPOCH}
exten => s,n,Set(fname=${STRFTIME(${EPOCH},,%Y)}/${STRFTIME(${EPOCH},,%Y-%m)}/${STRFTIME(${EPOCH},,%Y-
exten => s,n,Set(DIR_RECORDS=/var/spool/asterisk/monitor/)
exten => s,n,NoOp(Dir  - ${STRFTIME(${EPOCH},,%Y)}/${STRFTIME(${EPOCH},,%Y-%m)}/${STRFTIME(${EPOCH},,%
exten => s,n,Set(monopt=nice -n 19 /usr/local/bin/lame -b 32  --silent "${DIR_RECORDS}${fname}.wav"  "
exten => s,n,Set(CDR(filename)=${fname}.mp3);
exten => s,n,Set(CDR(realdst)=${called});
exten => s,n,MixMonitor(${DIR_RECORDS}${fname}.wav,b,${monopt});
exten => s,n(no),Verbose(Exit record);
```

Рисунок 3.46. – Команда розширення макросу

Налаштуємо паркування дзвінка (рисунок 3.47).

Паркування виклику – це перенаправлення дзвінка в спеціальний слот для утримання, абонент в цей момент прослуховує музику.

```
[manager]
include => call-local-manager
include => call-local
include => call-out-world
include => parkedcalls

[sales]
include => call-local-manager
include => call-local
include => call-out-ua
include => parkedcalls

[buyings]
include => call-local-manager
include => call-local
include => call-out-ua
include => parkedcalls

[warehouse]
include => call-local-manager
include => call-local
include => parkedcalls

[it]
include => call-local
include => parkedcalls

[reception]
include => call-local-manager
include => call-local
include => call-out-ua
include => parkedcalls
```

Рисунок 3.47. – Налаштування паркування викликів

Буде доцільним дозволити користувачам використовувати функцію переводу виклику. Щоб користувачі змогли скористатись функцією паркування потрібно додати у виклики Dial() параметр t(Рисунок 3.48).

```
;внутрішні лінії за виключенням manager
[call-local]
exten => _[2-6],1,Set(RECORDING=0)
exten => _[2-6],n,Macro(recording,${CALLERID(num)},${EXTEN})
exten => _[2-6]XX,n,Dial(SIP/${EXTEN},20,t)
exten => _[2-6],n,Hangup()
```

Рисунок 3.48. – Налаштування функції паркування

Після завершення налаштувань перевіряємо паркування викликів. Результат в додатку Б.

3.4 Висновки до розділу

В даному розділі розглянуто налаштування середовища для Asterisk. та SIP. Розроблено та налаштовано логіку обробки дзвінків, створено голосове меню. Початково, встановлено операційну систему Linux.

Встановлено DAHDI. Підключено бібліотеки libPRI, jansson. Втановлено драйвер PJProject. Встановлено програми для компіляції. Встановлено Asterisk та включено підтримку MySQL. Створено конфігураційні файли для налаштувань Asterisk, веб-сервера CDR Viever. Налаштовано логіку обробки дзвінків. Створено голосове меню. Додано можливість збору деталізованої інформації про виклики із допомогою баз MySQL.

ВИСНОВКИ

В даній кваліфікаційній роботі розглянуто основні принципи роботи мереж інтернет та IP-протоколів.

1. IP-телефонія стала своєрідним стадандартом телефонного зв'язку. Основні переваги IP-телефонії:

– зручність

– відносна надійність

– відносно невисока вартість порівняно з аналоговим зв'язком

Недоліки IP-телефонної мережі аналогічні до інших сервісів, що використовують IP-протоколи:

– сприйнятливість до вірусних атак;

– DoS-атак;

– можливість несанкціонованого віддаленого доступу.

VoIP як складова IP-телефонії також набула своєї популярності. Здебільшого його використовують в малому та середньому бізнесі. Розглянуто типології IP-телефонії. Існує 4 основні типи які описані в розділі 1

Розглянуто сучасні телефонні системи. Проаналізовано класичний аналоговий зв'язок PBX. Який на даний момент автоматизований і не потребує втручання людини. Так як раніше переключення відбувалось вручну. Розглянуто сучасні хмарні телефонні системи. Основною її перевагою є можливість приймати дзвінки з будь-якого девайсу. Недоліком є необхідність бути постійно підключеним до мережі інтернет. Автоматизація процесів обслуговування клієнтів і зниження витрат за рахунок цього – фактор, який сприяє розвиткові інтерактивних голосових сервісів. Отже, потреба в забезпеченні конфіденційності, цілісності, доступності та спостережливості інформації буде тільки зростати.

2. Успішність конкуренції з традиційними телефонними мережами забезпечується сучасними методами кодування і передачі інформації, а також збільшенням пропускної здатності каналу. Основні складові якості IP-телефонії є:

– можливість користувача зв'язуватися і розмовляти з іншим користувачем в реальному часі

– якість мови(розбірливість, рівень гучності);

– якість сигналізації;

– час встановлення та завершення виклику;

– чистота і тональність мови.

Для зменшення обсягу голосових даних використовується стиснення, так звані – кодеки. Спочатку може здатись, що кодеки схожі на програми архівування такі як WinRar, 7z, але це далеко не так. Основні відмінності:

– програми архівування опрацьовують весь файл повністю, а кодеки оброблять дані, які постійно надходять;

– збільшення часу архівування зазвичай некритично, на відмінно від кодеків, в яких збільшення часу обробки голосу зазвичай погіршує зв’язок;

– програми архівування забезпечують збереження 100% інформації, в той час як кодеки можуть привносити незначне погіршення якості з метою економії даних.

Для безпечної передачі медіаданих широко використовується протокол реального часу SRTP. Основні завдання протоколу SRTP:

– шифрування переданих голосових даних;

– аутентифікація переданих повідомлень;

– захист від передачі повторюваних пакетів;

– збереження пропускної здатності, стискання заголовків RTP.

Протокол ZRTP, який дозволяє обмінюватися ключами для SRTP між кореспондентами по відкритих каналах зв'язку. До завдань цього протоколу входять:

– генерація ключових параметрів SRTP-сесії;

– забезпечення конфіденційності повідомлень протоколу;

– аутентифікація кореспондентів;

– захист від MiTM як з використанням, так і без використання інфраструктури відкритих ключів.

При встановленні захищеного VoIP-з'єднання протокол ZRTP працює відразу після завершення роботи протоколу SIP. І тільки після успішного завершення роботи протоколу ZRTP починається передача медіатрафіку по протоколу SRTP.

3. В даному розділі розглянуто налаштування середовища для Asterisk. та SIP. Розроблено та налаштовано логіку обробки дзвінків, створено голосове меню. Початково, встановлено операційну систему Linux.

Встановлено DAHDI. Підключено бібліотеки libPRI, jansson. Втановлено драйвер PJProject. Встановлено програми для компіляції. Встановлено Asterisk та включено підтримку MySQL. Створено конфігураційні файли для налаштувань Asterisk, веб-сервера CDR Viever. Налаштовано логіку обробки дзвінків. Створено голосове меню. Додано можливість збору деталізованої інформації про виклики із допомогою баз MySQL.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Джонатан Девідсон, Джеймс Пітерс, Манож Бхатія, Сатіш Калідінді, Судіпто М. Основи передачі голосовихданих по мережах IP (IP Voice over IP Fundamentals); Вільямс, 2007.

2. Гольдштейн Б. С., Пінчук А. В., Суховицький А. Л. IP-телефонія: Радіо і зв'язок, 2008.

3. НопінС. В., ШаховВ. Г. Аналіз захищеності абонентських систем IP-телефонії від несанкціонованого доступу // Інформаційні технології. 2008. No11. Ст. 67-74.

4. Сайт про IP-телефонію - Режим доступу: http://ukash.idhost.kz.

5. Комп’ютерна документація і софт -Режим доступу: http://www.winsov.ru/net036.php.

6. Методичні вказівки щодо проходження виробничої практики для студентів напряму підготовки «Комп’ютерна інженерія» / Укл. О.М.Березький, Л.О.Дубчак, Г.М. Мельник, І.В. Ігнатєв, Ю.М. Батько – Тернопіль, ТНЕУ, 2014.- 11 с.

7. Дипломне проектування за напрямами підготовки "Прикладна математика", "Комп’ютерна інженерія", "Програмна інженерія" [Текст]: навч.-метод. посіб. / Є.С. Сулема; за заг. ред. І.А. Дички. –К.:НТУУ"КПІ",2011. –224 с.

8. Описание общей структуры АТС [Електронний ресурс] Режим доступу: https://studbooks.net/855236/tehnika/opisanie_obschey_struktury#12.

9. Семенов А. Б. Структурированные кабельные системы / Семенов А. Б., Стрижаков С. К., Сунчелей И. Р. – М.: ДМК-Пресс, 2002. - 640 с.

10. Новиков Ю. В. Локальные сети: Архитектура, алгоритмы, проектирование / Новиков Ю. В., Кондратенко С. В. – М.: ЭКОМ, 2002. - 311 с.

11. Яковина В.С. Основи безпеки комп’ютерних мереж: Навчальний посібник / В.С. Яковина. – Львів: НВФ "Українські технології", 2008. – 396 с.

12. Документація з настройки обладнання фірми Cisco. [Електронний ресурс]: http://www.cisco.com

13. Теорія телетрафіку / В.Я. Воропаєва, В.І. Бессараб, В.В. Турупалов, В.В. Червинський. – Донецьк: ДВНЗ «ДонНТУ», 2011. –202 с.

14. RFC 3261. J. Rosenberg, H. Schulzrinn, G.Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. SIP: Session Initiation Protocol. – IETF, June 2002.

15. RFC 3550. D.Schulzrinne, S.Casner, R.Frederick, V.Jacobson. RTP: A Transport Protocol for Real-Time Applications. – IETF, July 2003.

16. RFC 3711. M.Baugher D.McGrew, M.Naslund, E.Carrara, K.Norrman. The Secure Real-time Transport Protocol (SRTP). – IETF, March 2004.

17. RFC 3830. J.Arkko, E.Carrara, F.Lindholm, M.Naslund, K.Norrman. MIKEY: Multimedia Internet KEYing. – IETF, August 2004.

18. RFC 4568. F.Andreasen, M.Baugher, D.Wing. Session Description Protocol (SDP), Security Descriptions for Media Streams. – IETF, July 2006.

19. RFC 5764. D.McGrew, E.Rescorla. Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP). – IETF, May 2010.

20. RFC 6189. P.Zimmermann, A.Johnston, J.Callas. ZRTP: Media Path Key Agreement for Unicast Secure RTP. – IETF, April 2011.

21. Ковцур М.М., Никитин В.Н., Юркин Д.В. Протоколы обеспечения безопасности VoIP- телефонии. – Защита информации. Инсайд, 2012,№3, с.74–81.

22. Гольдштейн Б.С. и др. IP-телефония / Б.С. Гольдштейн, А.В. Пинчук, А.Л. Суховицкий. – М.: Радио и связь, 2001 – 336 с.

23. Росляков А.В. и др. IP-телефония / А.В. Росляков, М.Ю. Самсонова, И.В. Шибаева. – М.: Эко-Трендз, 2003. – 252 с.

24. Network Working Group Request for Comments: 3261 [Електронний ресурс]. – Режим доступу: http://www.ietf.org/rfc/rfc3261.txt.

25. Kuhn Richard D. Security Considerations for Voice Over IP Systems. Recommendations of the national Institute of Standards and Technology / Richard Kuhn D., Walsh Thomas J., Fries Steffen. – NIST Special Publication 800-58, 2005. – 100 p.

26. SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS. Infrastructure of audiovisual services – Systems aspects Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals. ITU-T Recommendation H.235, 2001 – 85 p. [Електронний ресурс]. – Режим доступу: http://www.itu.int/rec/T-REC-h.

27. Практические аспекты защиты корпоративных сетей IP-телефонии [Електронний ресурс] / А. Лукацкий. – Режим доступу: http://www.pabx.ru/publications/more.html?id=723.

28. Porter T. Practical VoIP security / Porter Thomas, Jan Kanclirz Jr., Rockland MA.: SyngressPublishing Inc., 2006.– 592 p. – Режим доступу: http://www.skype.co.ua/content/view/90/16/.

29. Сущность и результаты исследований свойств перспективных стандартов цифровой подписи x9.62-1998 и распределения ключей x9.63-199x на эллиптических кривых [Електронний ресурс] / М.Ф. Бондаренко, И.Д.Горбенко, Е.Г. Качко, А.В. Свинарев, Т.А. Гриненко. – Режим доступу: http://kiev-security.org.ua/box/19/84.shtml/.

30. Инфраструктура открытых ключей как основа обеспечения информационной безопасности национальных, ведомственных и коммерческих систем информационных технологий / М.Ф. Бондаренко, И.Д. Горбенко, С.П. Черных и др. // Радиотехника. – 2002. – № 126. – С. 5 – 17.

31. IP-телефония. Обзор технологии (Електронний ресурс) / Режим доступу URL: http://newcom.com.ua/content/ru/articles/index.php?article=1 – Загол. з екрана.

32. Информационная безопасность – Википедия // Википедия – свободная библиотека [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/Информационная_безопасность.

33. IP-телефония. Обзор технологии (Електронний ресурс) / Режим доступу URL: http://newcom.com.ua/content/ru/articles/index.php?article=1 – Загол. з екрана.

34. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Издательский дом «Вильямс», 2003. – 1104 с. Бабкин В.В. и др. Оптимизационная задача выбора речевого и канального кодирования / В.В. Бабкин, А.А. Ланнэ, В.С. Шаптала // Труды 7-ой международной конференции и выставки ЦОС и ее применения DSPA. – 2005. – С. 28 – 32.

35. Баричев С.Г. и др. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М.: Горячая линия – Телеком, 2001. – 144 с.

36. Безопасность Skype в корпоративной среде [Електронний ресурс] / А. Доля. – Режим доступу: http://www.citcity.ru/security/articles/.

37. Уязвимости Skype [Електронний ресурс]. – Режим доступу: www.pgpru.com.

38. Рынок call-центров 2009: готовность устоять против кризиса (Електронний ресурс) / Режим доступу URL: https://adm.cnews.ru/reviews/free/call2009/articles/construction.shtml – Загол. з екрана.

39. ISDN интерфейс PRI (Електронний ресурс) / Спосіб доступу URL: https://adm.cnews.ru/reviews/free/call2009/articles/construction.shtml – Загол. з екрана.

40. IP-телефония: основы и принципы. 1 часть - Технология будущого (Електронний ресурс) / Режим доступу URL: https://adm.cnews.ru/reviews/free/call2009/articles/construction.shtml – Загол. з екрана.

41. Голос как инструмент управления. Требования к современной платформе IVR(Електронний ресурс) / Спосіб доступу URL: http://www.billing.ru/guest/node/303 - Загол. з екрана.

42. Межсетевые экраны Cisco ASA 5580(Електронний ресурс) / Режим доступу URL: http://www.mototelecom.ru/katalog/setevoe-oborudovanie/mezhsetevye-ekrany/asa5580/- Загол. з екрана.

43. Сущность и результаты исследований свойств перспективных стандартов цифровой подписи x9.62-1998 ираспределения ключей x9.63-199x на эллиптических кривых [Електронний ресурс] / М.Ф. Бондаренко, И.Д.Горбенко, Е.Г. Качко, А.В. Свинарев, Т.А. Гриненко. – Режим доступу: http://kiev-security.org.ua/box/19/84.shtml/.

44. Информационная безопасность – Википедия // Википедия – свободная библиотека [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/Информационная_безопасность.

45. White paper. VoIP security and Privacy. Making PC Platforms and Networks Higly Secure.Printed inUSA/1105/PMS/LKY/PP/150 Intel, 2006 – 8 p.

46. Ботюк А.О. и др. Переваги асиметричної криптографії / А.О. Ботюк, М.П. Карпінський, Я.І. Кінах // Збірник доповідей Другої наук.-техн. конф. “Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні”. – Київ: НТУУ ”КПІ”, 2000. – С. 242 – 244.

47. Коблиц Н. Курс теории чисел и криптографии. – М.: ТВП, 2001 – 270 с.

48. Практические аспекты защиты корпоративных сетей IP-телефонии [Електронний ресурс] / А. Лукацкий. –Режим доступу: http://www.pabx.ru/publications/more.html?id=723.

49. Березький О.М., Дубчак Л.О., Мельник Г.М. Методичні рекомендації до виконання кваліфікаційної роботи з освітнього ступеня “Магістр”. Спеціальність: 123 - Комп’ютерна інженерія. Магістерська програма - Комп’ютерна інженерія"/ Під ред. О.М. Березького. Тернопіль:ЗУНУ,2020.32 с.

50. Гураль І.В., Дубчак Л.О. Методичні вказівки до оформлення курсових проектів, звітів про проходження практики, випускних кваліфікаційних робіт для студентів спеціальності «Комп’ютерна інженерія»/Під ред. О.М. Березького. Тернопіль: ТНЕУ, 2019. 33 с.