ИТМО

К.З. Билятдинов
А.З. Арсеньева
В.В. Меняйло

ТЕХНОЛОГИИ IP-ТЕЛЕФОНИИ

Санкт-Петербург
2022

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

К.З. Билятдинов
А.З. Арсеньева
В.В. Меняйло

ТЕХНОЛОГИИ IP-ТЕЛЕФОНИИ

Учебное пособие

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО
по направлению подготовки (специальности)
11.03.02 - Инфокоммуникационные технологии и системы связи
в качестве учебного пособия для реализации основных профессиональных образовательных программ высшего образования бакалавриата

Санкт-Петербург
2022

УДК.621.396.6.004.12.658.562

Билятдинов К.З., Арсеньева А.З., Меняйло В.В. **Технологии IP-телефонии:** учебное пособие – СПб: ИТМО, 2022. – 161 с.

Рецензент: Карасев Василий Владимирович, кандидат технических наук, доцент (квалификационная категория "доцент практики"), факультет инфокоммуникационных технологий

Учебное пособие посвящено изучению вопросов, связанных с основами современных технологий IP-телефонии. Рассмотрены технологии IP-телефонии во взаимосвязи с инновациями, перспективами и актуальными проблемами функциониования телекоммуникационных сетей, операторов связи, обеспечения информационной безопасности, управления и оценки эффективности.

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

A-MPDU – Aggregation MAC Protocol Data Unit; блок данных протокола MAC агрегации
ASCII – American standard code for information interchange; название таблицы кодировки
AuC – Authentication Centre; система аутентификации
AUSF – Authentication Server Function; функция сервера аутентификации
CMS – Content management system; система управления контентом
COTS – Commercial Off The Shelf; готовый коммерческий продукт
CRM – Customer Relationship Management; система управления взаимоотношениями с клиентами
DEA – Data Envelopment Analysis; анализ свертки данных
DTLS-SRTP – Datagram Transport Layer Security; протокол для шифрования RTP-нагрузки и проверки подлинности
DTMF – Dual-Tone Multi-Frequency; двухтональный многочастотный аналоговый сигнал
E2E – End-to-End; процесс тестирования
ERP – Enterprise Resource Planning; система планирование ресурсов предприятия
GGSN – GPRS Gateway Support Node; шлюзовый узел поддержки GPRS
GMSC – Gateway Mobile Switching Centre; шлюзовый центр мобильной коммутации
G-MSC – Gateway MSC; шлюзовой коммутатор мобильной сети
GSM – Global System for Mobile Communications; глобальный стандарт цифровой мобильной сотовой связи с разделением каналов по времени и частоте
H.323 – набор стандартов для передачи мультимедийных данных по сетям с пакетной передачей
HCI – Hyper-Converged Infrastructure; гиперконвергентная инфраструктура
HLR – Home Location Register; регистр домашнего местонахождения
HLR/HSS (Home Location Register/Home Subscriber Server) – высокопроизводительное и легко адаптируемое решение для построения и модернизации сетей MNO и MVNO
IETF – Internet Engineering Task Force; инженерный совет Интернета
IoT – концепция, направленная на подключение каждого устройства с выходом в Интернет для передачи и обмена данными по сети без вмешательства человека
Insertable Streams – функция, предоставляющая приложениям WebRTC доступ к аудио- и видеокадрам после того, как они были закодированы, но до того, как они были отправлены в сеть
IP-телефония – телефонная связь по Интернет-протоколу
IVR – Interactive Voice Response; интерактивное голосовое меню
LCR – Least Cost Routing System; маршрутизация по критерию наименьшей стоимости
LLC – Logical Link Control; верхний подуровень управления логической связью

MAC – Media Access Control; управление доступом к среде
MCU – Multipoint Control Unit; многоточечный блок управления
MGW – Media Gateway; элемент сети сотовой связи стандарта UMTS
MNO – Mobile Network Operator; оператор сотовой связи
MSC – Mobile Switching Center; коммутатор сетей мобильной связи
MVNA – Mobile Virtual Network Aggregator; агрегатор виртуальных операторов
MVNE – Mobile Virtual Network Enabler; запуск виртуальных операторов
MVNO – Mobile Virtual Network Operator; виртуальный оператор сотовой связи (компания, которая оказывает услуги сотовой связи под своим брендом, но не имеет собственной инфраструктуры и арендует ее у другого оператора)
OSPF – Open Shortest Path First; протокол динамической маршрутизации
P2P – Peer-to-Peer; сетевой протокол
PBX – Private Branch Exchange; «офисная АТС»
PoE – Power Over Ethernet; передача электроэнергии через Ethernet
PS-PC – Payload Shrinking and Packets Coalesce; метод снижения объема бесполезно расходуемой полосы пропускания
RoHC – Robust Header Compression; стандартизированный метод сжатия заголовков пакетов
RRC – Radio Resource Control; протокол управления радиоресурсами
RTCP – Real-Time Transport Control Protocol; протокол управления транспортом в реальном времени
RTP – Real-time Transport Protocol; транспортный протокол реального времени
SDN – Software-Defined Networking; сеть передачи данных, в которой уровень управления сетью отделен от устройств передачи данных и реализуется программно
SDP – Session Description Protocol; протокол описания сеанса
SIP – Session Initiation Protocol; протокол сеансового установления связи
SRTP – Secure Real-time Transport Protocol; безопасный транспортный протокол реального времени
STUN – Session Traversal Utilities for NAT; протокол, который позволяет клиенту, находящемуся за сервером трансляции адресов, определить свой внешний IP-адрес
TCP/IP – сетевая модель передачи данных
TURN – Traversal Using Relay NAT; протокол для ретрансляции трафика через сервер, который находится в публичном Интернете
UDP – User Datagram Protocol; протокол пользовательских датаграмм
VLAN – Virtual Local Area Network; виртуальная локальная сеть
VMS – Video Management Software; программное обеспечение для управления видео
VoiceXML – Voice eXtensible Markup Language, VXML; специальный язык программирования

VoIP – Voice over Internet Protocol; технологии для доставки голосовых сообщений и мультимедийных сеансов по сетям Интернет-протокола (IP), таким как Интернет, региональные, ведомственные или локальные вычислительные сети
VoIP-кодек – технология, совмещающая в себе процесс сжатия и обратный процесс
VSaaS – Video Surveillance as a Service; видеонаблюдение как услуга
WebRTC – Web Real Time Communications; веб-коммуникации в реальном времени
Автоматический распределитель вызовов (англ. Automatic Call Distributor, ACD) — технология, которая распределяет вызовы клиентов в порядке их поступления следующему доступному подходящему агенту
АТС – автоматическая телефонная станция
ВОЗ – Всемирная организация здравоохранения
МСЭ (ITU) – Международный союз электросвязи
Тональный набор (тональный сигнал) (англ. Dual-Tone Multi-Frequency, DTMF) — звуки (тональные сигналы), генерируемые телефоном при нажатии цифр
ТСОП – телефонная сеть общего пользования (PSTN – public switched telephone network)

ВВЕДЕНИЕ

IP-телефония является устоявшейся технологией, которую используют как современный бизнес, так и обычные пользователи по всему миру. Технология позволяет поддерживать голосовую и текстовую связь через глобальную сеть интернет. Преимущества IP-телефонии позволили работать и учиться, не выходя из дома. Дешевизна связи, основанной на сети Интернет, является большим плюсом для современного бизнеса, которому зачастую необходимо создать коммуникационную связь между несколькими удаленными офисами.

Реалии современности и необходимость всегда быть на связи сделали технологию IP-телефонии одной из самых востребованных в последнее время. Востребованные технологии всегда обладают большими инвестициями и быстро развиваются.

Перед исследованием инноваций в технологии IP-телефонии необходимо определить предметную область исследования и провести ее анализ. Для этого в учебном пособии рассмотрен и доказан тезис о том, что технология IP-телефонии на данный момент является одной из самых востребованных и перспективных.

После этого рассказывается о том, на чем основывается технология IP-телефонии. Рассмотрение основ технологии позволит лучше понять доступные векторы развития. В этом разделе исследованы технологические преимущества IP-телефонии и ее отличия от протокола IP. Анализ существующих кодеков и протоколов телефонии позволяет определить текущие проблемы построения сете коммуникации посредством этой технологии.

После изучения основ технологии необходимо уделить внимание современным технологиям IP-телефонии. Развитие кодеков и протоколов решает множество проблем качества предоставляемых услуг. Самым популярным стандартом IP-телефонии является стандарт WebRTC [54]. Он описывает передачу потоковых аудиоданных, видеоданных и контента между браузерами или другими поддерживающими его приложениями в режиме реального времени. Кроме стандарта WebRTC, в разделе рассмотрена IVR-система. Проанализированы существующие приложения для аудио и видеосвязи, сформирована современная картина текущего состояния технологий IP-телефонии.

После описания текущего состояния рассматриваются перспективы развития технологии в целом. Одним из современных представлений технологии VoIP является технология Voice over LTE, позволяющая передавать голос пользователя через мобильный интернет LTE. Такое стало возможным благодаря сетям нового поколения 4G и 5G. Технология VoLTE является перспективной среди операторов связи как в России, так и в мире [106].

Большую роль в развитии VoLTE сыграл новый тип операторов мобильной связи – виртуальные операторы связи. Выход новых мобильных операторов на рынок с текущей конкуренцией практически невозможен из-за больших проблем с построением собственной инфраструктуры [106]. Поэтому новые игроки рынка арендуют инфраструктуру существующих операторов связи.

Виртуальные операторы связи также популярны в среде IoT. Интернет вещей уже давно использует технологию IP-телефонии. Например, IP-камеры видеонаблюдения способны передавать звук посредством VoIP.

Учебное пособие может быть использовано при изучении курса «Технологии IP-телефонии» в рамках направления подготовки бакалавров «11.03.02 - Инфокоммуникационные технологии и системы связи». Пособие соответствует учебной программе и структуре курса. После каждого раздела пособия предлагаются вопросы для самопроверки.

В интересах эффективного применения данного пособия в учебном процессе по дисциплине «Технологии IP- телефонии» в соответствии с рабочей программой дисциплины представляется целесообразным комплексное рассмотрение вопросов технологических основ реализации интернет протоколов в современных сетях передачи данных с детализацией модификаций протоколов динамической маршрутизации, веб-коммуникаций в реальном режиме времени, протокола для шифрования RTP-нагрузки и проверки подлинности, а также процессов интеграции VoIP и IoT.

Рекомендации преподавателям:

- при подготовке и проведении лекций – в начале изучения дисциплины акцентировать внимание студентов на теоретических основах (в достаточной мере изложенных в разделе 1 и в параграфах 2.1 – 2.8), а далее на этом базисе приступить к детальному изучению основных вопросов курса, подробно изложенных в параграфах 2.9, 2.10, 2.11, разделах 3 4, 5 и 6;

- при подготовке и проведении практических занятий – особое внимание обратить на разделы 3, 5 и 6 в интересах совершенствования услуг виртуальных операторов связи;

- при подготовке и проведении лабораторных занятий – использовать материалы параграфов 1.2 (1.2.6), 2.9, 3.6 и 4.6 для оценки эффективности тестируемых технологий и приложений, а также для определения и обоснования трендов развития данной предметной области.

Рекомендации студентам:

- после каждой лекции во время самостоятельной работы для совершенствования знаний и компетенций предлагается составлять индивидуальный опорный конспект кратких ответов на вопросы самопроверки по соответствующему разделу пособия;

- в последующем данный конспект Вы сможете использовать при подготовке к экзамену по дисциплине;

- материалы разделов 2, 3, 4 и 5 рекомендуется системно использовать в качестве теоретического базиса и обоснования результатов решения задач при подготовке и выполнении практических и лабораторных работ.

Таким образом, предлагаемое учебное пособие будет Вашим надёжным помощником не только при изучении данного курса, но и при решении практических задач в сфере инфокоммуникационных технологий.

Раздел 1. АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Вычислительные сети

Технологии IP-телефонии основаны на вычислительных сетях. Для целостного понимания целесообразно выбрать определение вычислительной сети во избежание неоднозначности. В данном пособии используется определение вычислительной сети из межгосударственного стандарта ГОСТ 24402-88 [86]:

Вычислительная сеть – взаимосвязанная совокупность территориально рассредоточенных систем обработки данных, средств и (или) систем связи и передачи данных, обеспечивающая пользователям дистанционный доступ к ее ресурсам и коллективное использование этих ресурсов.

1.1.1. История вычислительных сетей

В 60-х годах XX века взаимодействие с ЭВМ осуществлялось посредством пакетной обработки данных. Программы и данные для программ последовательно считывались с перфокарт. Результат обработки данных получали в распечатанном на бумаге виде [78].

Следующим этапом в развитии ЭВМ стало использование терминалов, которые представляли собой периферийные устройства ввода информации, такие как клавиатура, и периферийные устройства вывода, такие как экран и принтер. Тем самым был реализован режим передачи данных онлайн. Терминалы были подключены к ЭВМ, которая в режиме разделения времени выполняла программы разных пользователей. Одним из первых примеров гражданского использования подобных сетей стала система резервирования авиабилетов, разработанная в IBM для компании American Airlines. Система имела 1200 терминалов-телетайпов в территориально рассредоточенных агентствах.

Глобальная сеть Интернет основана на идее так называемого «мозгового треста». Цель – надежный обмен данными между узлами сети на случай частичного ее разрушения в результате боевых действий. Для этого сеть должна иметь структуру отдельных сегментов при отсутствии централизации. Сообщение в сети должно быть поделено на фрагменты (пакеты) и передаваться по разным ветвям сети. Сбор сообщения осуществляется на машине получателя сообщения. Данные идеи были положены в основу создания сети ARPANET, состоящей изначально из четырех узлов. В результате развития идеи разбиения сообщения на пакеты были разработаны протоколы TCP и IP. Начало существования Интернет в США датируется 1986 годом. Общедоступным Интернет стал в 1989 году [78].

В целях повышения надежности доставки сообщений по сети было начато развитие коммерческих сетей общего пользования. Программное обеспечение таких сетей легло в основу стандарта X.25. Первой подобной сетью считается TELENET.

В 1980 году ЭВМ, разработанная в Институте системного анализа РАН (ИСА), использовалась для доступа советских ученых к иностранным банкам данных. Коллектив, создавший ЭВМ, о которой говорилось ранее, стал основой

Национального центра автоматизированного обмена информацией (НЦАО) в Институте автоматизированных систем (ИАС). Этот институт участвовал в создании вычислительной сети Академии наук СССР и Академий наук союзных республик, так называемой АКАДЕМСЕТИ, которая базировалась на протоколах X.25. В результате к 1986 году была создана вычислительная сеть общего пользования ИАСНЕТ [85].

Параллельно с созданием ИАСНЕТ в Институте атомной энергии энтузиастами была начата работа над созданием вычислительной сети для общения ученых-физиков. За основу были взяты протоколы телеобработки в UNIX-ЭВМ. В результате в 1991 году была введена в эксплуатацию коммерческая сеть RELCOM, которая стала частью Интернет. Полный набор IP-услуг появился в 1994 году.

В начале 1990-х годов в РФ начался бурный рост сетей общего пользования. В течение апреля 1992 года через сеть ИАСНЕТ прошло около 17 000 запросов на информацию из РФ. Более тысячи часов длились сеансы связи через сети DATAPAK, TRT с использованием узла RADIUS, что составляло примерно 10–15 % от общей загрузки сети в тот же период.

1.1.2. Классификация вычислительных сетей

Вычислительные сети можно классифицировать по различным характеристикам. Такими характеристиками могут являться:

- тип передачи данных,
- размер вычислительной сети.

В свою очередь, обозначенные выше категории могут быть поделены на подкатегории [112]. По типу передачи данных различают:

- широковещательные сети,
- сети с передачей от узла к узлу.

Вычислительные сети можно классифицировать по размеру на:

- персональные сети,
- локальные сети,
- муниципальные сети,
- глобальные сети.

Широковещательные сети имеют один канал связи со всеми распределенными сетевыми устройствами. Аналогией широковещательной сети можно считать диалог людей в комнате, в которой находятся несколько человек. Каждый человек может получить сигнал, а отреагирует на сигнал человек, которому он был адресован. Короткие сообщения (пакеты) получаются всеми машинами. Поле адреса в пакете указывает, кем сообщение должно быть получено. При получении пакета машина проверит поле адреса. Если адрес пакета совпадает с адресом машины, машина производит дальнейшую обработку [112]. Пакеты, адресованные другим машинам, игнорируются.

Широковещательные сети также позволяют генерировать пакет одновременно для всех машин. В этих целях используется специальный код в поле адре-

са [112]. Пакет с таким кодом будет обработан всеми машинами в вычислительной сети. Данный тип коммуникации называется широковещательной передачей. Некоторые системы передачи также предоставляют возможность отправлять сообщения на подмножество машин в сети, и это называется многоадресной передачей. Одним из возможных систем реализации может быть резервирование одного бита в качестве признака многоадресной передачи. Оставшееся количество бит в поле адреса будет характеризовать номер группы. Каждая машина может «подписаться» на одну, несколько или все группы. Когда пакет отправляется в конкретную группу, она будет доставлена всем машинам, которые являются членами этой группы.

Вычислительные сети с передачей сообщения от узла к узлу состоят из большего количества соединенных машин, так называемых пар. Перед доставкой сообщения в подобных сетях пакет проходит через некоторое количество промежуточных машин. В вычислительных сетях может быть несколько путей от отправителя к получателю. В сетях с таким типом передачи данных применяются алгоритмы маршрутизации [112].

Персональные вычислительные сети (personal area network, PAN) определяются как сети, состоящие из устройств вблизи человека. В качестве среды передачи данных наиболее часто используется электромагнитное излучение. В качестве примера таких сетей можно привести комбинацию ЭВМ, клавиатуры и мыши, поддерживающую соединение по стандарту IEEE 802.15.1 (Bluetooth).

Локальными вычислительными сетями (ЛВС, или LAN) называют соединенные ЭВМ в пределах небольшого здания. Подобные сети распространены в офисах для объединения рабочих станций и предоставления совместного доступа к ресурсам, таким как принтеры или файловые сервера. В качестве среды передачи данных используются как беспроводные соединения, такие как IEEE 802.11 (Wi-fi), так и соединения через кабель, которые могут быть изготовлены из меди или оптоволокна. Как правило, проводные ЛВС работают на скоростях от 100 Мбит/с до 10 Гбит/с. Стандарт IEEE 802.3 (Ethernet) наиболее широко применяется в проводных ЛВС. Соединение проводной сети обычно производится путем подключения узлов к коммутатору, которое обеспечивает надежную и безопасную передачу данных [108].

Есть возможность разбиения больших ЛВС на меньшие, виртуальные ЛВС (VLAN). Использование виртуальных ЛВС ограничивает число получателей широковещательных пакетов.

Муниципальные сети (metropolitan area network, MAN) объединяют ЭВМ в пределах одного города или населенного пункта [108]. Многие муниципальные вычислительные сети были образованы на базе кабельного телевидения. Схема подобной вычислительной сети продемонстрирована на рисунке 1.1. Обычно муниципальная сеть является соединением множества ЛВС в одну большую сеть.

Вычислительные сети, охватывающие значительные географические области, называются глобальными сетями (wide area network, WAN) [108]. Глобальные вычислительные сети состоят из подсетей. У глобальных сетей есть

сходство с ЛВС. Различия ЛВС и глобальных вычислительных сетей заключаются в разделении ответственности за подсети. ЛВС на предприятиях часто контролируется самими предприятиями. За подсети в глобальных сетях ответственны сетевые провайдеры и телефонные компании. В ЛВС обычно используется одна сетевая технология, тогда как в глобальных вычислительных сетях применяются маршрутизаторы – устройства, которые направляют данные в другие сети на основании таблиц маршрутизации [108]. Примерами глобальных сетей являются Интернет, ARPANET, спутниковые сети, сети мобильной телефонной связи.

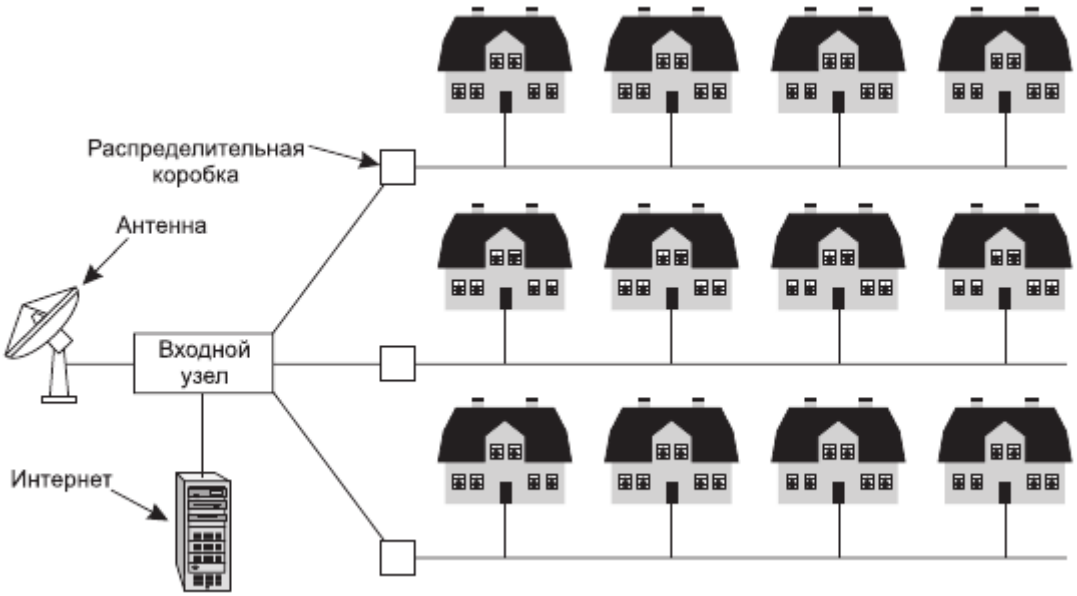


Рисунок 1.1. Муниципальная сеть на базе кабельного телевидения

1.1.3. Современное состояние вычислительных сетей

Инновации в вычислительных сетях не прекращают внедряться. Производится высокоскоростное сетевое оборудование. Увеличивается скорость передачи данных как в сетях доступа, так и в магистральных сетях. С начала 2000-х годов идет развертывание широкополосного домашнего доступа в Интернет с использованием оптоволоконных технологий. Самые различные группы пользователей потребляют множество IP-сервисов. Широко распространены общественные беспроводные сети доступа в Интернет через 4G- и 5G-сети операторов сотовой связи. Количество беспроводных устройств, подключенных к сети Интернет, превышает количество проводных устройств.

1.2 IP-телефония

1.2.1. Общие сведения об IP-телефонии

IP-телефония – технология, позволяющая использовать Интернет или любую другую IP-сеть в качестве средства организации и ведения международных телефонных разговоров и передачи факсов в режиме реального времени. Интер-

нет-телефония – частный случай IP-телефонии, когда в качестве линий передачи телефонного трафика (т.е. голоса) используется сеть Интернет [58]. На английском языке IP-телефония называется VoIP (Voice Over IP), именно эта аббревиатура чаще всего встречается в Интернете [3].

Технология IP-телефонии зародилась в масштабах корпоративной сети. Очень часто крупным компаниям требуется собственная корпоративная телефонная сеть, и до недавнего времени им приходилось выбирать только из двух альтернатив: либо создавать собственные линии связи, либо арендовать телефонные линии и номера у операторов связи. Первый вариант требует больших финансовых вложений, служб ремонта, а второй проигрывает в том, что очень часто плата за междугородную и международную связь оказывается слишком дорогой. Теперь, с появлением IP-телефонии, у корпораций появился третий способ организации корпоративной сети (рисунок 1.2) – с минимальными вложениями в создание линий связи и дешевыми тарифами на телефонные услуги. Конечно, стоимость оборудования IP-телефонии нельзя назвать низкой, но она не идет ни в какое сравнение со стоимостью первого и второго вариантов [64]. Начиная с середины и до конца 1990-х годов Интернет и протокол TCP/IP привели к изменениям в отрасли телефонии и связи. Интернет-протокол стал средством передачи почти всех данных. Мировой рынок VoIP находится на подъеме за счет таких преимуществ, как недорогая связь, недорогие скорости передачи данных и наличие мощной сетевой инфраструктуры [1].

Рисунок 1.2. Пример подключения оборудования в IP-телефонии

1.2.2. Преимущества IP-телефонии

IP-телефония имеет гибкую настройку и обладает множеством достоинств. С ее помощью можно:

- осуществлять бесплатные сообщения и звонки внутри сети;
- производить переадресацию звонков;
- передавать более одного телефонного звонка в рамках высокоскоростного телефонного подключения;

– привязывать звонки к нескольким адресам;
– вести протоколирование разговоров;
– определять номер звонящего;
– выбирать самый выгодный тариф, подключиться к любому количеству операторов;
– присваивать короткие номера выбранным абонентам;
– объединять абонентов в общую сеть, устанавливать на ней бесплатные звонки;
– организовывать конференции, интегрироваться с другими сервисами через интернет, включая видеозвонок, вебинары и т.п. [88].

Стоимость вызова в IP-телефонии определяется по так называемой «системе с минимальной стоимостью маршрутизации звонка» (Least Cost Routing System, LCR), которая основана на том, что осуществляется проверка пункта назначения каждого телефонного звонка, как только он сделан внутри сети, что дает потребителю самую низкую цену. Протоколы IP-телефонии обеспечивают регистрацию клиентского устройства (шлюз, терминал или IP-телефон) на сервере провайдера, вызов или переадресацию вызова, установление соединения, передачу имени и номера абонента [64]. В настоящее время широкое распространение получил протокол SIP – протокол сеансового установления связи, обеспечивающий передачу голоса, видео, сообщений систем мгновенного обмена сообщений и произвольной нагрузки. Для сигнализации протокол SIP обычно использует порт 5060 протокола установления соединения UDP [95].

1.2.3. Принцип работы IP-телефонии

Когда пользователь разговаривает с другими пользователями, используемые им слова переформатируются в сжатые объемы данных. После этого пакеты отправляются через Интернет другой стороне. Когда потоки информации поступают к получателю, она расшифровывается в аудиоданные оригинала. В простейшем телефонном звонке связь между участниками диалога устанавливается через телефонную станцию для разговора. Звуки голоса передаются по нужным телефонным каналам, по линиям, выделенным для связи. При запросе подключения к передаче через Интернет сжатые потоки информации передаются в Интернет с окончательным адресом получателя. Любой пакет информации проходит собственный путь до адресата по различным маршрутам. Для адресата информационные пакеты переформатируются и расшифровываются в звуковые сигналы исходного сообщения.

В случае интернет-телефонии, как уже упоминалось, в качестве линии передачи используются обычные пути передачи данных в Интернете. IP-телефония находится в состоянии ожидания как линия сбора данных о трафике с выделенных цифровых каналов. Для простых звонков на телефон требуются разветвленные сетевые телефонные станции, которые закреплены каналами телефонии, использующими оптоволоконные передатчики и спутники связи. Большие расходы

на операторов мобильной связи предоставляют электрическую связь между городами. Такие подключения станций, обслуживающих телефоны, дают большую нагрузку и снижение производительности, а также временной интервал потребляемого простоя во время разговора. На существующих телефонных каналах и станциях в большинстве случаев и осуществляет свою работу интернет-телефония.

Одной из главных особенностей интернет-телефонии является то, что она работает на современной системе сжатия звуковых сигналов и позволяет использовать весь емкостный запас каналов, созданный для телефонии [64].

По этой причине объемы информации от множества запросов и их различных вариаций имеют возможность в одно и то же время и по одному каналу направляться адресату. Работает это так: один из пользователей посылает звуковые сигналы своему собеседнику, сигнал начинает обрабатываться, проходя обработку шифраторов, посылается с помощью интернета данными пакета в настоящем времени. При этом максимальная задержка звукового посыла составляет 300–400 миллисекунд и зависит лишь от того, сколько времени потребуется для того, чтобы оборудование расшифровало и создало нормальный звуковой сигнал. В наше время были разработаны технологии, которые позволяют свести потерю мощности сигнала в сети к минимуму и не допустить того, чтобы соединение исчезло. За счет этого тратится в разы меньше денежных средств [58].

Для реализации IP-телефонии существует несколько протоколов, например:

- протокол инициации сеанса (SIP),
- H.323,
- транспортный протокол реального времени (RTP),
- протокол управления транспортом в реальном времени (RTCP),
- безопасный транспортный протокол реального времени (SRTP),
- протокол описания сеанса (SDP).

Для передачи сигнала требуются специальные инструменты – IP-шлюзы. Они представляют собой устройства, с помощью которых можно транслировать информацию из разных типов сети и связывать их между собой. IP-шлюзы имеют связь с телефонными линиями и позволяют соединиться с любыми телефонными точками мира, а также работать с интернетом; через них могут быть связаны компьютеры, которые подключены к Интернету. Телефонный сигнал оцифровывается шлюзом, уменьшается в объемах, делится на части и передается через IP-сеть по назначенному пути при использовании протокола TCP/IP. После этого разбитые пакеты данных проходят по еще одному шлюзу, где происходят преобразования в телефонный вызов.

Стандартный шлюз VoIP (рисунок 1.3) представляет собой устройство, которое подключается к телефонной сети [3, 15]. Главная задача голосового шлюза – запись и преобразование человеческой речи в цифровой код, который будет передан адресату.

Кодирование человеческого голоса происходит при помощи импульсно-кодовой модуляции. На входе звуки речи преобразуются в цифровой сигнал, который фрагментируется на отдельные пакеты и передается посредством IP-протокола. На принимающей стороне полученные пакеты проходят процедуру декодирования и преобразуются в синтезированную речь. Передать голосовой сигнал можно на любые устройства – браузер или другую компьютерную программу (например, Skype), а также на мобильные и городские стационарные телефоны.

Многие модели голосовых шлюзов, помимо передачи голоса, способны выполнять множество других функций: маршрутизацию, управление передаваемым трафиком, его анализ [109].

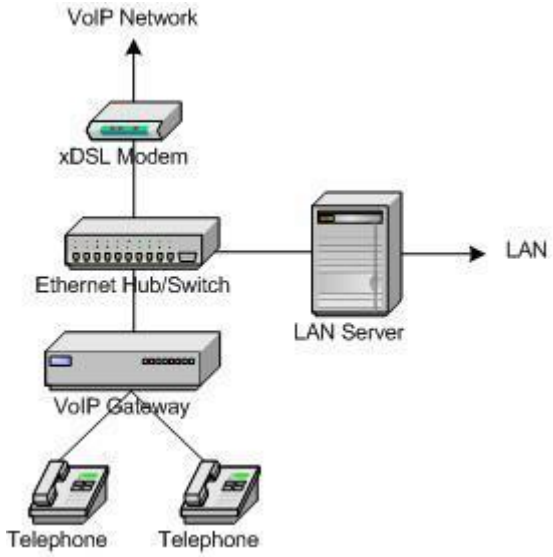


Рисунок 1.3. Шлюз VoIP

GSM-шлюз (сотовый шлюз) необходим в сети, где постоянно совершают звонки с аналоговых телефонов на мобильные. Это могут быть службы доставки, банки, интернет-магазины, страховые компании, службы такси. GSM-шлюз позволяет снизить расходы на звонки с аналогового телефона на сотовый.

1.2.4. Виртуальные операторы

С инженерной точки зрения виртуальный оператор (MVNO) представляет собой схему реализации виртуальной сети на основе имеющейся радиопередающей инфраструктуры сотовых операторов. Вся физическая часть находится в плоскости MNO – сотового оператора, а виртуальный оператор, руководствуясь базой данных с информацией об абонентах этой сети, использует регистр HLR, центр аутентификации (AuC) и коммутирующий сервис (MSC), который может подключаться к телефонной сети общего пользования. Коммутирующий сервис виртуального оператора взаимодействует с контроллером базовой станции (Base Station Controller), который объединяет базовые станции, содержит всю логику

управления и присоединяется к центру коммутации подвижной связи MSC. Последний уже непосредственно управляет соединением между абонентами.

Есть целый ряд тенденций, потенциально способных увеличить спрос на использование MVNO. Это развитие IoT, корпоративных сетей и систем мобильных платежей. Они генерируют не столько большой трафик (например, видео-контент), сколько большое количество мелких транзакций. Опросы датчиков через Интернет и удаленные команды, сверка версий файлов с совместным доступом, обычные и push-уведомления, логи GPS-трекинга, SMS с кодами подтверждений – все это выгоднее передавать по специфическому тарифному плану через виртуальную сеть, объединяющую сильные стороны разных магистральных провайдеров.

1.2.5. Рекомендации по организационно-техническим мероприятиям для виртуального оператора

Виртуальные операторы могут столкнуться с проблемами защиты персональных данных абонентов [114] и ограниченности пропускной способности канала сотовой связи операторов. Если в определенном секторе появляется абонент, активно использующий трафик, у абонентов поблизости снижается скорость. Как правило, виртуальные операторы, у которых нет возможности расширить емкость сети или построить базовую станцию, могут только ограничить скорость «активному» абоненту. Это приводит к потере абонента, который потребляет много трафика, так как актуальность этого MVNO для него пропадает.

В таком случае виртуальному оператору рекомендуется реагировать на перегрузку в конкретном секторе, анализировать абонентов по типам потребления в режиме реального времени и перераспределять трафик, чтобы снизить нагрузку на сеть. При этом необходимо учитывать множество параметров – что именно, в каком объеме и с какого ресурса потребляет абонент, какой у него тариф и как давно он им пользуется, мешает ли он остальным абонентам, и т.д. Таким образом, за счет управления трафиком можно повысить емкость сети и одновременно сохранить лояльность клиентов [77].

Виртуальный оператор должен активно взаимодействовать с разработчиками мобильных виртуальных сетей (MVNE). Это компания, которая предоставляет сетевую инфраструктуру и сопутствующие услуги, такие как подготовка, администрирование, система поддержки операций и система поддержки бизнеса (OSS/BSS), чтобы позволить операторам виртуальных сетей предлагать услуги своим клиентам. MVNE не поддерживает отношения с клиентами [13].

Виртуальный оператор должен использовать хранилища данных, которые поддерживают бизнес-аналитику и системы Business Intelligence для постоянной аналитики данных по клиентской базе. На основе этой информации MVNO сможет предлагать правильные продукты и своевременно проводить оптимизацию.

При работе с разнообразными устройствами и трафиком (видео, аудио) виртуальный оператор должен опираться на концепцию DCN, т.е. введение вы-

деленного ядра сети сотовой связи. По мере увеличения сети она наполняется большим количеством разнообразных устройств, что впоследствии снижает эффективность существующей архитектуры. В связи с этим консорциум 3GPP предусмотрел возможность существования нескольких ядер в сети, чтобы обеспечить гибкость, оптимизировать управление и передать обслуживание трафика наиболее подходящему ядру [71].

1.2.6. Анализ качества и эффективности в IP-телефонии

Для управления информационными пакетами, передаваемыми по сети, разработана технология QoS (Quality of Service, англ. качество обслуживания). QoS – это набор технологий, которые запускают высокоприоритетные приложения и трафик при лимитированной пропускной способности. Это означает, что более важный трафик будет обработан быстрее, а задержки по сети будут минимальны.

Измерения, касающиеся QoS, включают:

- пропускную способность,
- задержку,
- частоту ошибок.

Благодаря технологии QoS можно научить маршрутизатор разделять пропускаемый трафик (рисунок 1.4), и тогда ни потоковое видео, ни звонок в Skype не будут «заикаться».

Рисунок 1.4. Разделение пропускаемого трафика в IP-сети

Механизмы QoS для упорядочивания пакетов и выделения полосы пропускания предназначены для:

- управления очередями,
- управления полосой пропускания.

Необходимо разделить трафик с помощью инструментов классификации. Так организации смогут контролировать доступность ресурсов для приоритетных приложений. Трафик может быть классифицирован по порту, IP-адресу или с использованием более сложного подхода, такого как приложение или пользо-

ватель. Затем для инструментов управления очередями и управления полосой пропускания назначают правила для обработки потоков трафика, характерных для классификации, которую они получили при входе в сеть и расчётов их корреляции [115].

Механизм организации очереди предназначен для хранения пакетов в потоках трафика до тех пор, пока сеть не будет готова их обработать. Это гарантирует, что наиболее важные приложения не будут лишены пропускной способности в сети из-за приложений с меньшим приоритетом.

Механизм управления пропускной способностью измеряет и контролирует потоки трафика, чтобы избежать перегруженности сети. Этот механизм включает в себя:

- формирование трафика,
- ограничение скорости,
- увеличение полезной полосы пропускания,
- алгоритм планирования,
- другие методы для обеспечения пропускной способности.

В зависимости от поставщика QoS перечисленными средствами можно управлять и объединять их в блоки.

Каждый день корпоративные сети передают огромный объем трафика. Часть этого трафика имеет решающее значение для успеха бизнес-операций. Особенно это может быть важно для IP-телефонии. Поэтому, когда возникает переполнение очереди на сетевых устройствах, QoS необходим, чтобы увеличить скорость обработки данных и убрать переполнение буфера памяти на сетевых устройствах.

Большинство организаций используют протокол передачи файлов (FTP) и приложения для видеоконференций, такие как Zoom или GoToMeeting. Хотя оба показателя важны для производительности сотрудников, пакеты FTP не так чувствительны к задержкам, как пакеты передачи голоса по Интернет-протоколу (VoIP). В случае задержки FTP-пакеты все равно будут доставлены без изменений. Но задержанный VoIP-пакет приведет к разобщенным видеозвонкам и сорванным деловым встречам.

Настройка QoS в IP-телефонии важна для бизнеса, ведь качество связи влияет на количество звонков и, соответственно, конверсию.

Чтобы не допустить помехи связи и задержки звука, можно настроить приоритизацию для данных IP-телефонии. Перед настройкой необходимо обратить внимание на характеристики роутера и максимальный размер очереди обработки пакетов. Если канал узкий, то буфер устройства будет переполняться, а новые пакеты будут удаляться, и приоритизация трафика в таком случае бесполезна: необходимо проложить дополнительные маршруты.

Настроить приоритезацию в IP-телефонии можно или в веб-интерфейсе роутера (по протоколу SIP/RTP, по портам, по типу трафика), или непосредственно в приложении для звонков. Единственный минус – не все роутеры под-

держивают приоритет по заголовку, настройка будет зависеть от устройства и сервиса [95].

Технология QoS помогает поддерживать производительность сети, гарантировать бесперебойную передачу трафика, а также регулярно оценивать состояние IT-инфраструктуры компании. QoS в IP-телефонии влияет на количество и качество звонков, а значит, на конверсию [118].

1.2.7. Применение IP-телефонии

Сегодня доступ к Интернету осуществляется с мобильных телефонов, которые поддерживают технологии высокоскоростного Интернета. Это означает, что звуковой сигнал из канала VoIP может поступать сразу на IP-телефон, подключенный к IP-сети, либо на мобильный телефон мобильного оператора сети, либо на телефон, подключенный к обычной сети. Совместимость мобильных номеров оказывает влияние на IP-телефонию, на коммерческое применение VoIP. Телефонные системы для бизнеса теперь могут предложить компаниям гораздо больше, чем стандартные телефонные звонки. IP-телефония положила начало разработке унифицированных коммуникационных решений, которые могут предоставить полный коммуникационный пакет «все в одном», работающий в одной сети и на одной платформе. Это означает, что предприятия могут легко управлять звонками, использовать видеоконференции, сотрудничать, общаться в чате и т.д. с помощью одной службы. Эти решения также позволили пользователям совершать телефонные звонки VoIP через свои смартфоны и компьютеры с использованием либо приложений, либо веб-клиентов [58].

Преимущества IP-телефонии в корпоративной среде многочисленны, но в основном сводятся к соображениям стоимости, связанным с инфраструктурой и ежемесячными счетами за телекоммуникационные услуги. Современные решения VoIP PBX, такие как 3CX, позволяют компаниям запускать систему на существующем непатентованном оборудовании, а также на недорогих машинах, таких как мини-ПК. Традиционные телефонные системы и проприетарные решения VoIP предполагают широкомасштабную реализацию закрытых архитектур, которые требуют больших финансовых затрат и гораздо более сложны в управлении, настройке и обслуживании. Системы IP-телефонии с открытыми стандартами также гораздо проще и экономичнее масштабировать.

Технология VoIP уже получила широкое распространение во многих отраслях по всему миру. Возможность совершать бесплатные внутренние звонки между сотрудниками в высшей степени полезна, но некоторые отрасли получают больше преимуществ из-за характера их бизнеса. Любая организация, которая использует множество национальных и международных звонков, выиграет от внедрения офисных телефонных систем VoIP. Поскольку такие звонки могут быть дорогими, система VoIP может значительно снизить стоимость [5].

Назовем сферы, которые уже сейчас активно используют IP-телефонию.

– Обслуживание клиентов. Для большинства предприятий обслуживание клиентов сосредоточено вокруг телефона. Клиенты звонят в компании, чтобы решать проблемы, устранять неполадки и получать персонализированные

решения. Все колл-центры могут использовать технологию VoIP для снижения операционных расходов. Также с ее помощью можно минимизировать время ожидания, автоматически перенаправляя звонки свободным агентам, иметь доступ к голосовой почте через электронную почту, обучать агентов с помощью функции мониторинга звонков в реальном времени, собирать данные о звонках, чтобы оценить производительность каждого отдельного оператора [60].

- Электронная коммерция. Конкуренция в сфере электронной коммерции жесткая. Клиенты хотят, чтобы их вопросы были решены в течение нескольких минут. Система VoIP может помочь предприятиям электронной коммерции достичь этого. Индивидуальная система VoIP для индустрии электронной коммерции предлагает некоторые уникальные функции, в том числе записи звонков для проверки претензий, мобильные возможности для полного мобильного опыта, автосекретарь для маршрутизации звонков на бесплатного агента. Интеграция управления взаимоотношениями с клиентами позволяет агентам по обслуживанию клиентов немедленно получать данные о клиентах, включая недавние покупки и статус доставки [72].
- Финансовые учреждения. VoIP для финансов может обеспечить большие преимущества благодаря уникальным функциям: управление несколькими офисами с виртуальными расширениями, обучение агентов и повышение качества звонков с помощью записи звонков и мониторинга звонков в реальном времени, отправление и получение факсов с возможностями виртуального факса.
- Туристические агентства. Туристические агенты зарабатывают исключительно за счет качества услуг, которые они предлагают клиентам. Система VoIP может стать определяющим фактором успеха турагента. Она предлагает возможность отправлять текстовые сообщения для продвижения услуг или специальных предложений для постоянных клиентов, быстро отвечать клиентам, получая голосовые сообщения по электронной почте, переадресовывать звонки и оставаться на связи с клиентами, даже не находясь рабочем месте, быстро найти доступного оператора и переадресовать вызов, успокаивая клиентов с помощью музыки на удержании [97].
- Недвижимость. В сфере недвижимости у каждого клиента есть альтернативы. Агент по недвижимости должен предоставить потенциальным покупателям большой опыт, чтобы закрыть продажи. Системы VoIP помогают агентам по недвижимости добиться успеха следующими способами: создание облачной платформы для поддержания связи с клиентами, использование виртуальных номеров в различных целях, обмен изображениями между агентом и клиентом, чтобы поддерживать разговор, не переключаясь на электронную почту или WhatsApp.
- Здравоохранение. Услуги VoIP предоставляются в крупных больницах, но также могут быть полезны для клиник, центров по уходу за престарелыми и домов престарелых. Использование беспроводных устройств VoIP может

создать безопасную среду для связи. VoIP для сектора здравоохранения предлагает возможность точного перевода звонков в нужное отделение или даже на отдельных врачей и медсестер, индивидуальные меню для быстрых решений (нажмите 1 для выставления счетов, нажмите 2 для встреч и т. д.), более короткое время ожидания (что имеет решающее значение для лучшего ухода за пациентами), вывод информации о пациенте по запросу посредством интеграции электронных медицинских карт [84]. Еще в 2005 г. все государства-члены Всемирной организации здравоохранения (ВОЗ) взяли на себя обязательства по реализации стратегии обеспечения всеобщего охвата населения медицинской помощью. Данная стратегия подразумевает, в частности, внедрение электронного здравоохранения (англ. eHealth) в поддержку привычного формата медицинского обслуживания. Электронное здравоохранение играет ключевую роль в предоставлении медицинских услуг населению отдаленных территорий, а также малообеспеченным гражданам посредством применения телемедицины (англ. telehealth) и мобильной медицины (англ. mHealth) [82].

Резюме

Вычислительные сети были созданы как надежный и безотказный инструмент связи сегментов сети, функционирующий при частичном разрушении линий связи. В процессе развития сетевой инфраструктуры были разработаны различные протоколы взаимодействия в вычислительных сетях. Вычислительные сети удобно делить по размеру. Обычно различают локальные, муниципальные и глобальные вычислительные сети. Первой общедоступной глобальной вычислительной сетью стала сеть Интернет.

На данный момент современные сети строятся на базе стека протоколов TCP/IP. Интернет является глобальной сетью соединенных вычислительных сетей, построен на базе стека протоколов TCP/IP. Интернет включает частные, публичные, академические, бизнес- и государственные сети. Вычислительная сеть Интернет использует медные, оптоволоконные и беспроводные соединения. Преимущественное большинство звонков с использованием технологий IP-телефонии проходит через сеть Интернет.

Стек протоколов TCP/IP включает протокол сетевого (3-го) уровня модели OSI и TCP/IP IP (Internet Protocol). Протокол IP используется в протоколах IP-телефонии.

IP-телефония позволяет использовать существующую инфраструктуру глобальной сети Internet для связи с получателем сообщения на другом континенте, что упрощает и удешевляет коммуникацию в организациях с филиалами в разных географических местоположениях. IP-телефония может быть использована для передачи аудио- и видеоинформации, что упрощает передачу сообщения, когда требуется визуальный контакт с получателем или отправителем сообщения, например, в случае общения глухонемых людей. Качество поставляемых услуг

растет, а именно происходит уменьшение времени задержки пакетов, IP-телефония продолжает развиваться.

Вопросы для самопроверки

1. В чем заключаются основы классификация вычислительных сетей?
2. Каковы функции маршрутизаторов в муниципальных вычислительных сетях (metropolitan area network, MAN)?
3. Каковы основы и принципы технологии IP-телефонии?
4. Перечислите наиболее важные преимущества применения технологии IP-телефонии.
5. Каковы функции стандартного шлюза VoIP?
6. Поясните понятие и место виртуального оператора связи в современном мире.
7. В чем заключаются организационно-технические мероприятия для виртуального оператора связи по решению проблемы ограниченности пропускной способности арендуемого канала сотовой связи?
8. Поясните понятие качества связи в IP-телефонии.
9. Поясните понятие эффективности в IP-телефонии.
10. В чем сущность стека протоколов TCP/IP?

Раздел 2. ОСНОВЫ ТЕХНОЛОГИИ IP-ТЕЛЕФОНИИ

2.1 Общие сведения об IP-телефонии

IP-телефония – это вид связи, который использует Интернет для обмена голосовыми сообщениями, факсом и другими типами информации по сетям на основе IP [89]. Традиционно информация передавалась по коммутируемой телефонной сети общего пользования (ТСОП) и основывалась на выделенных соединениях с коммутацией каналов. IP-телефония упрощает этот процесс и передает информацию в виде пакетов через Интернет или локальную сеть, минуя проблемы ТСОП.

Технология IP-телефонии позволяет передавать голосовой и мультимедийный контент (видео, изображения) через Интернет. Это один из самых дешевых способов общения в любое время и в любом месте при наличии Интернета. Основные преимущества IP-телефонии – низкая стоимость, мобильность, отсутствие дополнительных кабелей, гибкость, видеоконференцсвязь.

Для совершения IP-звонка необходимо устройство с подключением к Интернету. На рисунке 2.1 показано, как происходит IP-вызов.

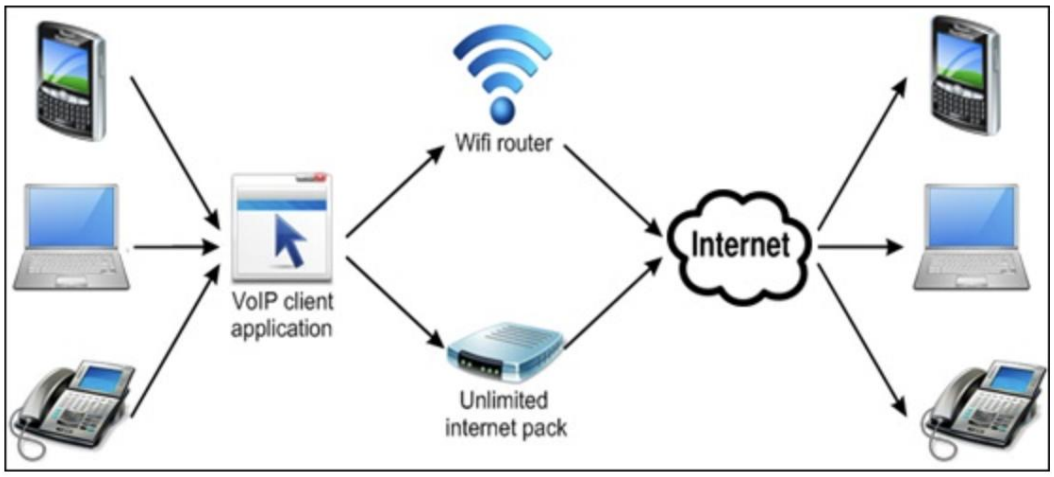


Рисунок 2.1. Схема работы IP-телефонии

2.2 Преимущества IP-телефонии

Перечислим основные преимущества IP-телефонии [74, 87, 100].

1) Сеть унифицированных коммуникаций (UC). IP-телефония является надежным решением голосовой связи по локальным сетям. Благодаря своей надежности она также рассматривается как модель унифицированных коммуникаций (UC) с различными ценными функциями, такими как поддержка присутствия, веб-, видео- и аудиоконференций, а также бесплатные звонки через сеть передачи данных.

2) Интеллектуальное решение для мобильности подключения. Несомненно, IP-телефония улучшает коммуникацию для всех, даже для удаленных работников. Сегодня нет необходимости носить с собой бизнес-телефон. IP-телефония позволяет удаленным сотрудникам получать доступ к своей сети с

помощью своих мобильных телефонов в любом месте, при условии, что там присутствует подключение к Интернету. Это фактически улучшает связь на станциях других предприятий, в городах или даже странах.

3) Простая в использовании технология WebRTC. Технология WebRTC является аналогом решения для удаленной работы. WebRTC – это программный сервис, который можно легко загрузить на свой ноутбук или настольный компьютер без необходимости использования какого-либо аппаратного устройства и который дает доступ ко всем службам UC (unified communication) [54].

4) Богатый функциональными возможностями коммуникационный аспект. IP-телефония революционизирует способ коммуникации благодаря своему богатому набору функций. Дополнительные функции IP-телефонии включают в себя телеконференции, программируемые кнопки, функции автосекретаря, голосовой почты для транскрипции электронной почты, подключения к нескольким сайтам через сеть передачи данных, окна единой системы обмена сообщениями, ожидания вызова и идентификатора вызывающего абонента и т. д. Такой набор функций позволяет использовать IP-телефоны в большей степени, чем TDM-системы.

5) Простота установки и настройки. Для установки и настройки IP-телефонов не требуется быть профессионалом и техническим специалистом. В нем нет сложности программирования, проприетарного программного обеспечения, графического пользовательского интерфейса и других подобных запутанных вещей.

6) Простота масштабируемости. IP-телефоны не ограничены количеством физических телефонных подключений. Это обеспечивает полную гибкость, когда возникает необходимость в добавлении нового IP-телефона. Предприятия могут легко добавлять или удалять новый или существующий IP-телефон из маршрутизатора.

7) Экономия затрат при повышении производительности. Работники могут общаться по одной или нескольким основным телефонным линиям как внутри организации, так и за ее пределами. Кроме того, IP-телефония поддерживает широкий спектр приложений, которые помогают работникам выполнять свои задачи быстрее и эффективнее.

2.3 Отличие IP-телефонии от IP-протокола

IP-телефония – это подмножество IP-протокола. Это подразумевает, что IP-телефония предназначена для голосового трафика по сети IP, в то время как IP-протокол в целом предназначен для обмена голосом, факсом и другими типами трафика данных [100]. В цифровом виде все элементы IP-телефонии используют оцифрованный голос, который передается в виде IP-пакетов через IP-сеть (в основном локальную сеть). Кроме того, IP-телефония фокусируется на оцифровке аналоговых голосовых сигналов (аналого-цифровое преобразование) и преобразуется в двоичные числа для передачи по IP-протоколу. Например, система IP-АТС (Private Branch Exchange) использует собственный IP-протокол и

стандарты (SIP, H.323) в сочетании с другими аспектами, такими как CRM и т. д. На рисунке 2.2 [87] представлена схема компонентов сети IP-телефонии.

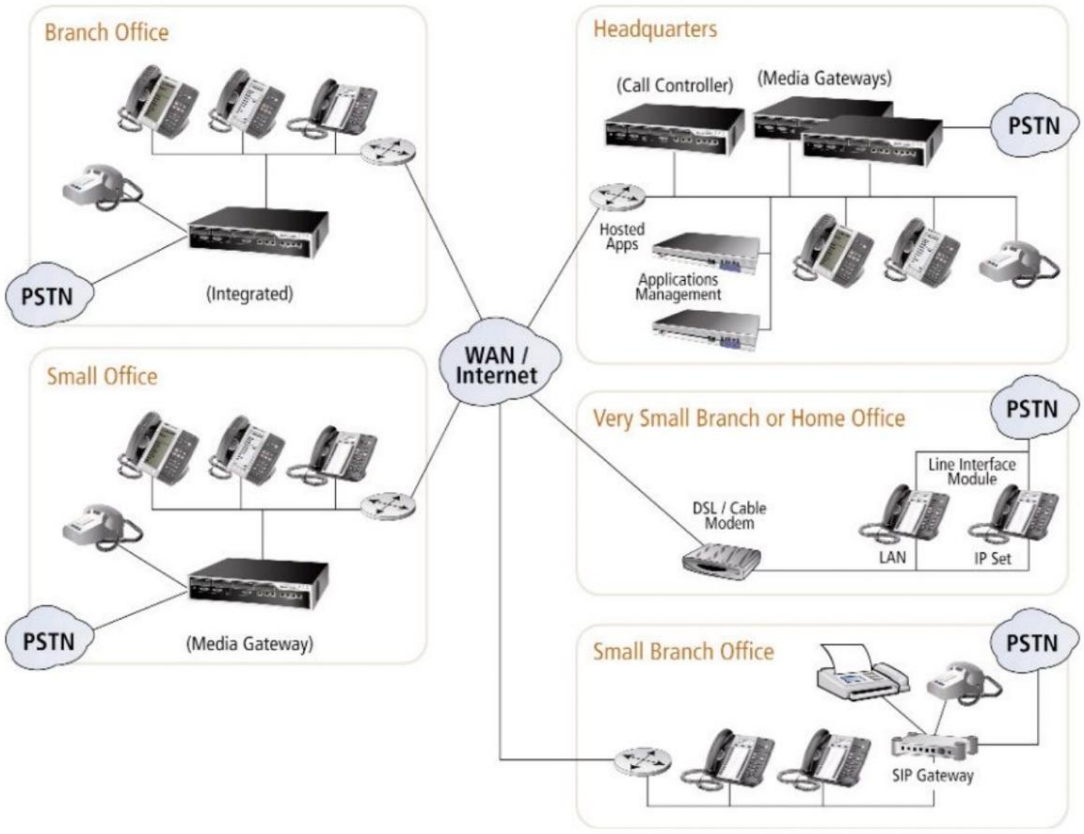


Рисунок 2.2. Схема компонентов IP-телефонии

2.4 Принцип работы IP-телефонов

IP-телефоны работают путем сканирования и обнаружения аналогового голосового сигнала человека и преобразования его в цифровые сигналы. Затем эти цифровые сигналы передаются по широкой линии в виде данных. IP-телефоны принимают телефонные разговоры и направляют их через систему IP-телефонов по сетевому кабелю в сеть, затем наружу, а затем в интернет-соединение. При этом вместо традиционной телефонной линии и телефонной сети используются интернет-протокол и локальная сеть офиса, которая для передачи вызовов и другой информации подключается к сети телефонного провайдера. И тот же протокол, и сеть также используются компьютерными системами, устройствами и принтерами. Таким образом, необходимо управлять и поддерживать только одну внутреннюю сеть для всех коммуникаций. Пример сети представлен на рисунке 2.3 [89].

Принцип пакетной передачи заключается в следующем. Для проведения сеанса связи необходимо набрать номер вызываемого абонента, после чего происходит соединение с сетевым шлюзом, как показано на рисунке 2.4 [89]. Голосовое сообщение абонента А с помощью микрофона преобразуется в аналоговый сигнал, который претерпевает ряд преобразований (кодируется). Внутри

шлюза происходит оцифровка голосового сигнала, как условно показано на рисунке 2.5 [89].

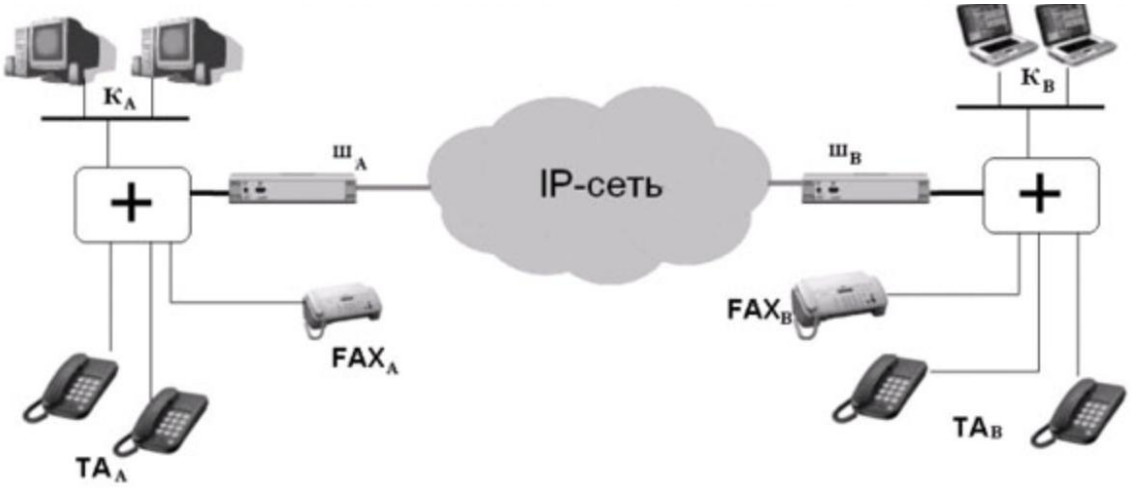


Рисунок 2.3. Сеть с IP-телефонией

Рисунок 2.4. Соединение с сетевым шлюзом

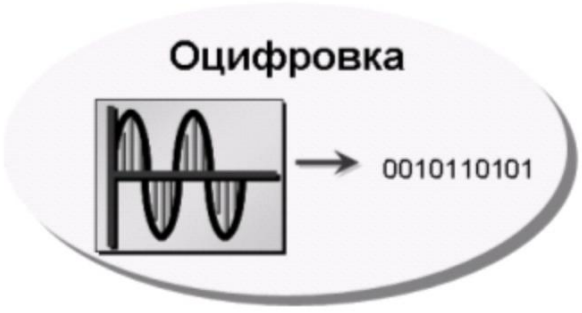


Рисунок 2.5. Оцифровка голосового сигнала

После оцифровки цифровой сигнал, занимающий изначально, как и речь, канал в 64 кбит/с, сжимается в соответствии с выбранным кодеком и разбивается на пакеты сигналов в соответствии с выбранным типом кодирующего устройства (кодеком) (рисунки 2.6 и 2.7 [89]). В преобразовании участвуют как аппаратные, так и программные средства со стороны абонента А.

Рисунок 2.6. Сжатие канала

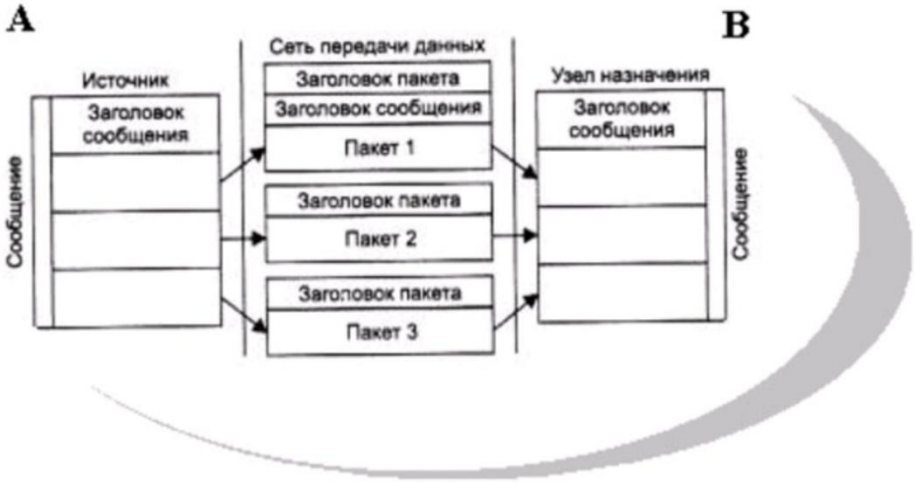


Рисунок 2.7. Разбиение на пакеты

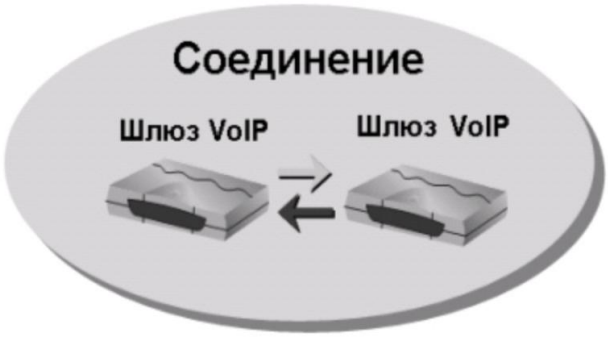


Рисунок 2.8. Соединение с приемной стороной

Далее сжатые данные отправляются в сеть. На приемной стороне имеется аналогичный набор устройств абонента B (рисунок 2.8 [89]), производящих преобразования в обратном порядке. Пакеты из сети поступают в телефонный шлюз, подключенный к телефонной линии. Все операции повторяются в обратном порядке, то есть осуществляется декодирование цифрового сигнала и преобразование его в аналоговую форму, которая приводит в действие звуковой динамик. Показанные этапы преобразования сигналов и передачи происходят в малые доли секунды, практически в реальном масштабе времени, что позволяет обеспечить дуплексный (двухсторонний) разговор.

В архитектуре технологии VoIP используется комбинация взаимосвязанных протоколов Интернета: это протокол RTP (Real Time Transport Protocol), который функционирует поверх протокола UDP (User Datagram Protocol), расположенного, в свою очередь, в стеке протоколов TCP/IP над протоколом IP. Таким образом, иерархия протоколов RTP/UDP/IP представляет собой своего рода транспортный механизм для речевого трафика.

В сетях с маршрутизацией пакетов IP для передачи данных всегда предусматриваются механизмы повторной передачи пакетов в случае их потери. При передаче голосовой информации в реальном масштабе времени этот прием неприменим, так как речевая информация очень чувствительна к задержкам, но менее чувствительна к потерям, поэтому для передачи речи (как и видеоинформации) используется механизм негарантированной доставки информации RTP/UDP/IP. Рекомендации ITU-T допускают задержки в одном направлении, не превышающие 150 мс.

2.5 Адресация в IP-сетях

Каждый терминал в сети TCP/IP имеет адреса трех уровней [92].

1. Физический уровень (MAC-адрес) – локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, куда входит данный узел.

2. Сетевой уровень (IP-адрес), состоящий из 4 байтов, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно или назначен по рекомендации специального подразделения Интернета (Network Information Center, NIC), если сеть должна работать как составная часть Интернета. Обычно провайдеры услуг Интернета получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла – гибкое, и граница между этими полями может устанавливаться весьма условно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

3. Символьный уровень (DNS) – идентификатор адреса, который назначается администратором и состоит из нескольких частей, например: имя машины, имя организации, имя домена.

Подавляющее большинство сетей сейчас использует протокол IPv4. Схема адресации протокола IPv4 предусматривает размер адресного поля 32 бита, что дает 2^{32} (или 4 294 967 296) потенциальных адреса.

IP-адрес любой рабочей станции состоит из адреса сети и адреса компьютера в этой сети. В архитектуре адресации предусмотрено пять форматов адреса,

каждый из которых начинается с одного, двух, трех или четырех битов, идентифицирующих класс сети (A, B, C, D или E – рисунок 2.9) [92].

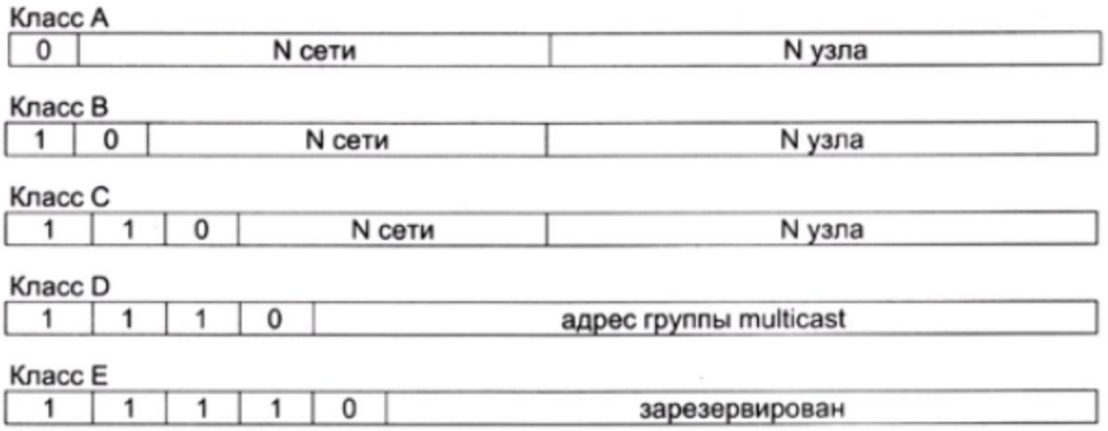


Рисунок 2.9. Структура IP-адреса

Область сетевого идентификатора (Network ID) определяет конкретную сеть в классе, а область Host ID идентифицирует конкретный компьютер в сети, а именно:

1. Адреса класса A идентифицируются начальным битом 0. Следующие семь битов определяют конкретную сеть (число возможных значений – 2^7 или 128). Остальные 24 бита определяют конкретный компьютер в сети, при возможном количестве компьютеров 16 777 216. Адреса класса A предназначены для очень крупных сетей с большим количеством рабочих станций;

2. Адреса класса B идентифицируются начальной двухбитовой двоичной последовательностью 10. Следующие 14 битов определяют сеть, при этом возможное количество сетей – 16 384. Остальные 16 битов определяют конкретный компьютер, с возможным количеством компьютеров 65 536;

3. Адреса класса C идентифицируются начальной трехбитовой последовательностью 110. Следующие 21 бит определяют сеть с возможным количеством сетей – 2 097 152. Остальные 8 битов определяют конкретный компьютер в сети, с возможным количеством компьютеров 256. Большинство организаций имеют адреса класса C;

4. Адреса класса D идентифицируются начальной четырехбитовой последовательностью 1110. Адреса этого класса предназначены для групповой передачи, и оставшиеся 28 битов определяют групповой адрес;

5. Адреса класса E идентифицируются начальной четырехбитовой двоичной последовательностью 1111. Адреса этого класса зарезервированы для будущего использования.

2.6 Особенности IP-телефонии

Приведем список основных особенностей IP-телефонии [72]:

1) Высокое качество голоса. Этот атрибут IP-телефонии обеспечивает бесперебойную связь, интеграцию звуковой маскировки для устранения ненужного

шума, а также доступ к истории групповых вызовов, фильтрации, экспорту и управлению записью.

2) Множество вариантов расширений. Встроенная функция автоматической маршрутизации вызовов позволяет пользователям автоматически направлять вызовы в один или несколько заранее запрограммированных пунктов назначения. Кроме того, звонки будут безопасно и автоматически перенаправляться на следующий доступный добавочный номер, при этом ящик голосовой почты связан с каждой строкой или добавочным номером.

3) Единый номер. Это одна из наиболее гибких характеристик, которая позволяет звонить с одного и того же номера с разных телефонов. Кроме того, номер мобильного телефона скрыт, поэтому звонящий не сможет определить ваше местоположение.

2.7 Модель OSI в сетях IP-телефонии

В сетях IP-телефонии реализуются четыре уровня модели OSI [121].

2.7.1 Физический уровень

На физическом уровне осуществляется передача потока битов по физической среде через соответствующий интерфейс. IP-телефония практически полностью опирается на существующую инфраструктуру сетей. В качестве среды передачи информации используются, как правило, витая пара категории 5 (UTP5), одномодовое или многомодовое оптическое волокно или коаксиальный кабель. Тем самым в полной мере реализуется принцип конвергенции телекоммуникационных сетей [113].

Часто используется технология PoE (Power Over Ethernet) – стандарты IEEE 802.3 af-2003 и IEEE 802.3at-2009. Ее суть заключается в возможности обеспечения питанием устройств посредством стандартной витой пары. Большинство современных IP-телефонов, в частности, модельный ряд Cisco Unified IP Phones 7900 Series, поставляются с поддержкой PoE. Согласно стандарту 2009 года, устройства могут получать ток мощностью до 25,5 Ватт.

При подаче питания используются лишь две витых пары кабеля 100BASE-TX, однако некоторые производители задействуют все четыре, достигая мощности до 51 Ватт. Необходимо заметить, что технология не требует модификации существующих кабельных систем, в том числе и кабелей Cat 5.

Для определения того, является ли подключаемое устройство питаемым (PD – powered device), на кабель подается напряжение 2,8–10 В. Тем самым вычисляется сопротивление подключаемого устройства. Если данное сопротивление находится в диапазоне 19–26,5 кОм, то процесс переходит на следующий этап. Если же нет – проверка повторяется с интервалом ≥ 2 мс.

Далее происходит поиск диапазона мощностей питаемого устройства путем подачи более высокого напряжения и измерения тока в линии. Вслед за этим на линию подается питающее напряжение 48 В. Также осуществляется постоянный контроль перегрузок.

2.7.2 Канальный уровень

Согласно спецификации IEEE 802 [72], канальный уровень разделяется на два подуровня:

– MAC (Media Access Control) – обеспечивает взаимодействие с физическим уровнем.

– LLC (Logical Link Control) – обслуживает сетевой уровень.

На канальном уровне работают коммутаторы – устройства, обеспечивающие соединение нескольких узлов компьютерной сети и распределение фреймов между хостами на основе физической (MAC) адресации.

Существует механизм виртуальных локальных сетей (Virtual Local Area Network). Данная технология позволяет создавать логическую топологию сети без оглядки на ее физические свойства. Достигается это тегированием трафика, что подробно описано в стандарте IEEE 802.1Q. На рисунке 2.10 [113] показан формат фрейма канального уровня.

Рисунок 2.10. Формат фрейма

В контексте IP-телефонии также существует Voice VLAN, широко применяющаяся для изоляции голосового трафика, генерируемого IP-телефонами, от других данных. Ее использование целесообразно по двум причинам:

– безопасность (создание отдельной голосовой VLAN уменьшает вероятность перехвата и анализа голосовых пакетов);

– повышение качества передачи (механизм VLAN позволяет задать повышенный приоритет голосовым пакетам, и, как следствие, улучшить качество связи).

2.7.3 Сетевой уровень

На сетевом уровне происходит маршрутизация, соответственно, основными устройствами сетевого уровня являются маршрутизаторы (Router). Именно здесь определяется, каким путем данные достигнут получателя с определенным IP-адресом [113].

Основной маршрутизируемый протокол – IP (Internet Protocol), на основе которого и построена IP-телефония, а также всемирная сеть Интернет. Также

существует множество динамических протоколов маршрутизации, самый популярным среди которых является OSPF (Open Shortest Path First) – внутренний протокол, основанный на текущем состоянии каналов связи.

На сегодняшний момент существуют специальные VoIP-шлюзы (Voice Over IP Gateway), обеспечивающие подключение обычных аналоговых телефонов к IP-сети. Как правило, они имеют и встроенный маршрутизатор, позволяющий вести учет трафика, авторизовать пользователей, автоматически раздавать IP-адреса, управлять полосой пропускания.

В состав стандартных функций VoIP-шлюзов входят:

– функции безопасности (создание списков доступа, авторизация);

– поддержка факсимильной связи;

– поддержка голосовой почты;

– поддержка протоколов H.323, SIP (Session Initiation Protocol) [12].

Для борьбы с возможными задержками передачи IP необходимо дополнять дополнительными средствами, например протоколами установления очередности (чтобы голосовые данные не конкурировали с обычными). Как правило, в этих целях на маршрутизаторах используется очередность с малой задержкой (LLQ – Low-Latency queuing), либо взвешенная организация очередей на основе классов (CBWFQ – Class-Based Weighted Fair Queuing). Кроме того, необходимы схемы маркировки с заданием приоритетов для рассмотрения голосовых данных как наиболее важных для передачи.

2.7.4 Транспортный уровень

Для транспортного уровня характерны [121] сегментация данных приложений верхнего уровня, обеспечение сквозного соединения, а также гарантия надежности данных.

Основные протоколы транспортного уровня – TCP (англ. Transmission Control Protocol, протокол управления передачей), UDP (англ. User Datagram Protocol, протокол пользовательских дейтаграмм), RTP (англ. Real-time Transport Protocol, транспортный протокол реального времени). Непосредственно в IP-телефонии используются протоколы UDP и RTP в связи с тем, что телефонная связь чрезвычайно зависима от задержек передачи, но менее чувствительна к потерям пакетов.

UDP базируется на сетевом протоколе IP и предоставляет транспортные услуги прикладным процессам, причем, в отличие от TCP, при отправке и получении данных никаких подтверждений не запрашивается. Также при отправке информации не обязательно установление логического соединения между модулями UDP (источником и приемником).

Несмотря на то, что RTP принято считать протоколом транспортного уровня, как правило, он работает поверх UDP. С помощью RTP реализуется распознавание типа трафика, работа с метками времени, контроль передачи и нумерация последовательности пакетов. Основное назначение RTP состоит в том, что он присваивает каждому исходящему пакету временные метки, обрабатываю-

щиеся на приемной стороне. Это позволяет принимать данные в надлежащем порядке, снижает влияние неравномерности времени прохождения пакетов по сети, восстанавливает синхронизацию между аудио и видео данными.

2.8 Основные протоколы уровня данных IP-телефонии

2.8.1 Протокол инициализации сеанса (SIP)

SIP (англ. Session Initiation Protocol, протокол установления сеанса) – это технология, позволяющая абонентам телефонной сети разговаривать друг с другом, обмениваться мультимедийной информацией, осуществлять видеозвонки, отправлять сообщения. Передача информации производится при помощи IP [98].

SIP – это протокол сигнализации, который используется для установления сеанса между двумя или более участниками, изменения этого сеанса и, наконец, завершения этого сеанса. Реальная передача данных осуществляется по протоколам TCP или UDP на пятом уровне модели OSI [74].

По принципу действия SIP похож на стандарт HTTP, используемый для передачи сообщений по электронной почте и интернет-приложений.

Поддержка протокола SIP позволяет выполнять следующие задачи:

– передача голосовой информации;

– отправка и прием мультимедийных данных;

– организация конференцсвязи;

– удержание вызова [95].

Благодаря гибкости протокола его возможности могут быть расширены в зависимости от требований к организации связи. Использование технологии SIP позволяет избежать ограничений, связанных с применением брандмауэров.

Структура SIP-сети проиллюстрирована на рисунке 2.11 [98].

В основу технологии положены следующие принципы [98]:

1) Мобильность пользователей. Каждый абонент сети может беспрепятственно перемещаться в зоне ее действия. Все пользователи имеют уникальный идентификационный номер, при помощи которого система определяет их местоположение.

2) Возможность масштабирования. АТС, использующие SIP-протокол, строятся по серверному принципу. Это позволяет увеличивать число элементов сети при ее увеличении.

3) Расширяемость. Стандарт можно дополнить новыми функциями при появлении дополнительных услуг. Кроме того, система может быть адаптирована к разным приложениям. Расширение можно выполнить путем введения новых заголовков для сообщений. Сервер обрабатывает только те сообщения, данные которых он может распознать. Другую информацию система игнорирует.

Все чаще телефонные системы на основе SIP-технологии используются вместо традиционной телефонии. Их преимущества [98]:

1) Стоимость установки и подключения оборудования ниже, чем для реализации аналоговой АТС.

2) Пользователи получают в распоряжение многоканальный телефонный номер, который никогда не бывает занят (при достаточной численности персонала).

3) Количество абонентов можно увеличить без существенных затрат.

4) Установка и настройка оборудования выполняется быстро и легко.

5) Тариф не зависит от локации абонентов, что делает выгодным использование телефонии в организациях, имеющих филиалы в разных регионах. Ограничения по географическому положению абонентов отсутствуют.

6) Имеется возможность отслеживания звонков и ведения соответствующей статистики, что позволяет оптимизировать работу персонала для повышения лояльности клиентов.

7) Широкий функционал системы позволяет ставить звонки в очередь, записывать разговоры, настраивать форму обратного звонка и так далее.

8) На основе SIP может быть создан удаленный колл-центр, что позволяет экономить на аренде помещения и нанимать на работу сотрудников из разных городов.

9) Виртуальная АТС настраивается в зависимости от графика работы организации.

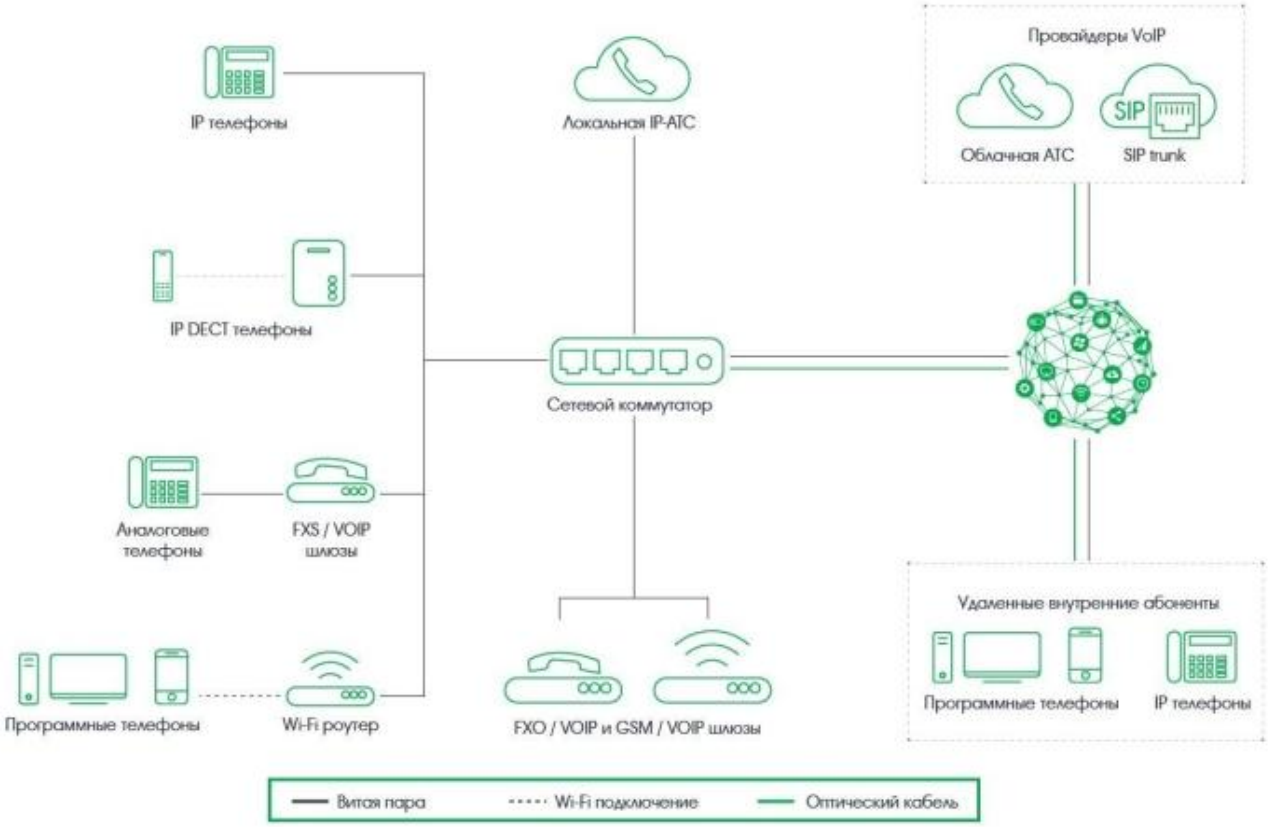


Рисунок 2.11. Структура SIP-сети

Принципы протокола SIP укладываются в одну общую модель «клиент-сервер», которая основана на постоянном чередовании запросов и ответов. SIP – это универсальный стандарт для передачи информации в Интернете. Он исполь-

зуется, например, в Skype. Стандарт может применяться в любых сетях со скоростью передачи информации не ниже 64 килобит в секунду [95].

Для пользователей системы доступны следующие способы совершения звонков [98]:

1) Посредством компьютера или ноутбука (для этого необходимо установить софт, подключить гарнитуру).

2) С помощью смартфона или планшета через 3G/LTE (для работы требуется установка приложения).

3) С использованием стационарного SIP-телефона (аппарат подключается к роутеру).

4) При помощи обычного телефонного аппарата, поддерживающего такую возможность (в этом случае требуется подключить телефон к VoIP-шлюзу, а шлюз – к роутеру).

Последовательность работы системы состоит в следующем:

1) При поступлении голосового звонка SIP-программа сжимает голос и преобразует в цифровой сигнал, что позволяет сохранить качество звука и уменьшить нагрузку на сеть.

2) Сигнал передается в принимающее устройство (ПК, смартфон, телефонный аппарат и т. д.).

3) Устройства коммутируются между собой при помощи IP-адресов для начала сеанса связи.

4) Цифровой сигнал преобразуется в аналоговый, благодаря чему пользователи могут слышать голоса друг друга.

Аналогичным образом осуществляется передача мультимедийной информации.

Протоколы связи SIP используются для работы элементов по модели «клиент–сервер»:

1) Терминал – конечный узел SIP-сессии для ее управления или передачи сообщения. Является одновременно и клиентом, и сервером.

2) Регистратор – узел SIP-сети. Находит и регистрирует терминалы, хранит о них данные.

3) Прокси-сервер – промежуточный элемент SIP-сети. Обеспечивает передачу сообщений между терминалами с помощью маршрутизации.

4) Шлюз – элемент для передачи сообщений между сетями.

5) Контроллер границы сеанса – выполняет сервисные функции между терминалами.

6) Сервер перенаправления – дополнительный элемент, который перенаправляет запросы между прокси-серверами и внешними доменами.

Использование стандарта SIP – это удобный и выгодный способ организации связи между абонентами во всем мире.

SIP является текстовым протоколом [74], и его синтаксис во многом схож с HTTP. Сообщения в SIP разделяются на запросы и ответы. Запрос генерирует терминал и направляет его серверу. Первая строка запроса содержит метод, оп-

ределяющий природу запроса, затем следует URI-адрес назначения запроса. Текстовые сообщения вместе с механизмом запроса-ответа упрощают устранение неполадок.

Вот список ключевых запросов:

– REGISTER – регистрация URI на сервере;

– INVITE – запуск протокола для связи;

– ACK – подтверждение запуска;

– BYE – завершение сеанса;

– CANCEL – отмена запроса;

– UPDATE – обновление состояния сеанса;

– REFER – запрос на переадресацию;

– PRACK – временное подтверждение;

– NOTIFY – уведомление о событии; сообщение подписчику о произошедшем событии;

– INFO – информация о сеансе.

Ответ от сервера поступает в виде цифрового кода. Такие коды объединяются в группы по первой цифре:

– 1XX – запрос попал на сервер и в данный момент обрабатывается;

– 2XX – запрос успешно завершен;

– 3XX – запрос необходимо перенаправить по новому адресу;

– 4XX – запрос отклонен или в нем содержится ошибка;

– 5XX – запрос не будет выполнен;

– 6XX – запрос отклонен, поскольку нет возможности для установки соединения.

Ниже приведены несколько моментов, на которые следует обратить внимание в отношении SIP.

SIP обеспечивает мультимедийный сеанс по Интернет-протоколу. Сеанс – это простой вызов между двумя конечными точками. Конечной точкой может быть смартфон, ноутбук или любое устройство, которое может получать и отправлять мультимедийный контент через Интернет.

SIP – это протокол, определенный стандартом IETF (Internet Engineering Task Force). Это определено в RFC 3261.

SIP воплощает архитектуру «клиент-сервер» и использует URL и URI из HTTP, а также схему кодирования текста и стиль заголовка из SMTP.

SIP может использоваться для двухсторонних (одноадресных) или многосторонних (многоадресных) сеансов. Другие приложения SIP включают передачу файлов, обмен мгновенными сообщениями, видеоконференции, онлайн-игры и распространение мультимедийных данных.

Протокол SIP разработан таким образом, чтобы быть независимым от базового транспортного протокола, поэтому приложения SIP могут работать по TCP, UDP или другим сетевым протоколам более низкого уровня.

На рисунке 2.12 представлено место SIP в общей сетевой структуре [98].

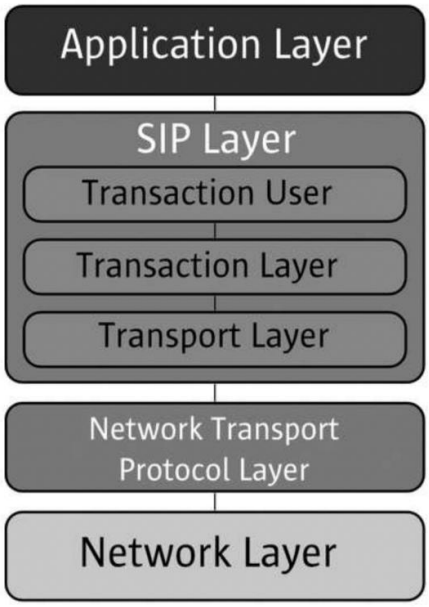


Рисунок 2.12. SIP-протокол в общей сетевой структуре

Как правило, протокол SIP используется для интернет-телефонии и распространения мультимедиа между двумя или более конечными точками. Например, один человек может инициировать телефонный звонок другому человеку с помощью SIP, или кто-то может создать конференцсвязь со многими участниками. Протокол SIP [98] был разработан таким образом, чтобы быть очень простым, с ограниченным набором команд.

2.8.2. Система протоколов H.323

H.323 [72] – это протокол, рекомендуемый Сектором стандартизации электросвязи МСЭ (ITU-T), который определяет протоколы для обеспечения сеансов аудиовизуальной связи в любой пакетной сети. Стандарт H.323 адресует сигнализацию и управление вызовами, передачу и управление мультимедиа, а также управление полосой пропускания для двухточечных и многоточечных конференций. Он широко внедряется производителями оборудования для голосовой и видеоконференцсвязи, используется в различных интернет-приложениях реального времени, таких как GNUGK и NetMeeting, и используется по всему миру поставщиками услуг и предприятиями как для голосовых, так и для видеосервисов по IP-сетям. Он является частью протоколов серии ITU-T H.32x, которые также обеспечивают мультимедийную связь по ISDN, ТСОП или SS7 и мобильным сетям 3G.

Сигнализация вызовов H.323 основана на протоколе рекомендации ITU-T Q.931 и подходит для передачи вызовов по сетям, использующим сочетание IP, ТСОП, ISDN и QSIG по ISDN. Модель вызовов, аналогичная модели вызовов ISDN, облегчает внедрение IP-телефонии в существующие сети АТС на основе ISDN, включая переход на АТС на основе IP.

В контексте H.323 АТС на основе IP может быть гейткипером (англ. gatekeeper – привратник) или другим элементом управления вызовами, который предоставляет услуги телефонам или видеофонам. Такое устройство может предоставлять или облегчать как базовые услуги, так и дополнительные услуги, такие как передача вызова, парковка, прием и удержание.

Как и протокол SIP, H.323 также учитывается в этом списке и обладает той же функциональностью, что и SIP. Этот протокол также отвечает за инициирование, изменение и завершение сеанса. Это один из набора стандартов ITU-T, который интерпретирует множество протоколов для обеспечения аудиовизуальной связи через компьютерную сеть. На самом деле это двоичный протокол, который передает голос или видео по сети.

H.323 – это системная спецификация, которая описывает использование нескольких протоколов ITU-T и IETF. Основу системы H.323 составляют следующие протоколы:

- Протокол регистрации, допуска и статуса (RAS) H.225.0, который используется между конечной точкой H.323 и гейткипером для предоставления услуг разрешения адресов и контроля доступа.
- Протокол управления H.245 для мультимедийной связи, который описывает сообщения и процедуры, используемые для обмена возможностями, открытия и закрытия логических каналов для аудио, видео и данных, управления и индикации.
- Транспортный протокол реального времени (RTP), который используется для отправки или получения мультимедийной информации (голоса, видео или текста) между любыми двумя объектами.

Многие системы H.323 также реализуют другие протоколы, которые определены в различных рекомендациях МСЭ-Т для обеспечения поддержки дополнительных служб или предоставления пользователю других функциональных возможностей.

Протокол H.323 имеет несколько подвидов [72]:

1) Серия H.235 описывает безопасность в рамках H.323, включая безопасность как для сигнализации, так и для носителей.

2) Серия H.239 описывает использование двух потоков в видеоконференциях, обычно один для видео в реальном времени, другой для неподвижных изображений.

3) Серия H.450 описывает различные дополнительные услуги.

4) Серия H.460 определяет дополнительные расширения, которые могут быть реализованы конечной точкой или гейткипером, включая рекомендации ITU-T H.460.17, H.460.18 и H.460.19 для преобразования сетевых адресов (NAT) и (или) обхода брандмауэра (FW).

В дополнение к этим рекомендациям ITU-T, H.323 реализует различные запросы IETF на комментарии (RFC) для передачи мультимедиа и пакетирования мультимедиа, включая транспортный протокол в реальном времени (RTP) [72].

Система H.323 определяет несколько сетевых элементов, которые работают вместе, чтобы обеспечить широкие возможности мультимедийной связи. Этими элементами являются терминалы, многоточечные блоки управления (MCU), шлюзы, гейткиперы и пограничные элементы. В совокупности терминалы, многоточечные блоки управления и шлюзы часто называются конечными точками. H.323 использует TCP-порт с номером 1720.

Для обеспечения связи между двумя людьми требуется по крайней мере два терминала. В большинстве развертываний H.323 используется гейткипер, чтобы, помимо прочего, облегчить разрешение адресов.

Терминалы являются наиболее фундаментальными элементами в системе H.323, поскольку это устройства, с которыми обычно сталкиваются пользователи. Они могут существовать в виде простого IP-телефона или мощной системы видеоконференцсвязи высокой четкости.

Внутри терминала H.323 находится стек протоколов, который реализует функциональность, определенную системой H.323. Стек протоколов включает реализацию базового протокола, определенного в рекомендациях ITU-T H.225.0 и H.245, а также RTP или других протоколов, описанных выше.

Большинство систем H.323 не реализуют такой широкий спектр возможностей, но логическое расположение полезно для понимания взаимосвязей.

Многоточечный блок управления (MCU) [72] отвечает за управление многоточечными конференциями и состоит из двух логических объектов – многоточечного контроллера (MC) и многоточечного процессора (MP). В более практическом плане MCU – это конференц-мост, мало чем отличающийся от конференц-мостов, используемых сегодня в ТСОП. Наиболее существенное отличие, однако, заключается в том, что микроконтроллеры для реализации H.323 могут микшировать или переключать видео в дополнение к обычному микшированию звука, выполняемому традиционным конференц-мостом. Некоторые микроконтроллеры также предоставляют возможности многоточечной совместной работы с данными. Для конечного пользователя это означает, что, разместив видеозвонок в микроконтроллере H.323, пользователь сможет видеть всех других участников конференции, а не только слышать их голоса.

Шлюзы – это устройства, которые обеспечивают связь между сетями H.323 и другими сетями, такими как сети ТСОП или ISDN. Если одна сторона в разговоре использует терминал, который не является терминалом H.323, то вызов должен проходить через шлюз, чтобы обе стороны могли обмениваться данными.

Шлюзы позволяют устаревшим телефонам ТСОП подключаться к крупным международным сетям H.323, которые в настоящее время развертываются поставщиками услуг. В частности, шлюзы используются внутри предприятия для того, чтобы корпоративные IP-телефоны могли через поставщика услуг обмениваться данными с пользователями в ТСОП.

Шлюзы также используются для того, чтобы устройства видеоконференцсвязи, основанные на H.320 и H.324, могли взаимодействовать с системами

H.323. Большинство мобильных сетей третьего поколения (3G), развернутых сегодня, используют протокол H.324 и способны взаимодействовать с терминалами на базе H.323 в корпоративных сетях через такие устройства шлюза.

Гейткипер [89] – это дополнительный компонент в сети H.323, который предоставляет ряд услуг терминалам, шлюзам и устройствам MCU. Эти услуги включают регистрацию конечных точек, разрешение адресов, контроль доступа, аутентификацию пользователей и так далее. Разрешение адресов является наиболее важной функцией гейткипера, поскольку оно позволяет двум конечным точкам связываться друг с другом без необходимости знать IP-адрес другой конечной точки.

Гейткиперы могут быть сконструированы для работы в одном из двух режимов сигнализации – прямой маршрутизации и маршрутизации гейткипера. Режим прямой маршрутизации является наиболее эффективным и наиболее широко используемым. В этом режиме конечные точки используют протокол RAS для получения IP-адреса удаленной конечной точки, и вызов устанавливается непосредственно с удаленным устройством. В режиме маршрутизации гейткипера сигнализация вызова всегда проходит через него. Хотя последнее требует от гейткипера большей вычислительной мощности, оно также дает гейткиперу полный контроль над вызовом и возможность предоставлять дополнительные услуги от имени конечных точек.

Конечные точки H.323 используют протокол RAS для связи с гейткипером. Аналогично, гейткиперы используют RAS для связи с другими гейткиперами [89].

Набор конечных точек, которые зарегистрированы для одного гейткипера в H.323, называется зоной. Эта коллекция устройств не обязательно должна иметь соответствующую физическую топологию. Скорее всего, зона может быть полностью логической и произвольно определяться администратором сети.

Гейткиперы имеют возможность соседствовать друг с другом, чтобы разрешение вызовов могло происходить между зонами. Это облегчает использование абонентских групп, таких как глобальная схема набора номера. Абонентские группы облегчают межзонный набор, так что две конечные точки в разных зонах все еще могут взаимодействовать друг с другом.

2.8.3. Транспортный протокол реального времени (RTP)

Определенный в RFC 1889, протокол RTP имеет стандартный формат пакетов для передачи аудио / видео через Интернет. Этот протокол широко используется в системах связи и развлечений, которые включают потоковые медиа, такие как телефония, телевизионные услуги, приложения для видеоконференций и веб-функции push-to-talk.

По сути, RTP работает рука об руку с RTCP (протоколом управления транспортом в реальном времени). RTP передает медиапотоки, в то время как RTCP отслеживает статистику передачи, QoS и помогает в установлении синхронизации различных потоков. Кроме того, RTP генерируется из портов с чет-

ным номером, а RTCP использует следующий более высокий порт с нечетным номером [89].

2.8.4. Протокол управления транспортом в реальном времени (RTCP)

Этот протокол определен в RFC 3550 и работает совместно с RTP. Протокол RTCP отвечает за отправку управляющих пакетов участникам конкретного вызова. Фактически его основная задача состоит в том, чтобы обеспечить обратную связь по QoS, предоставляемую RTP [87].

Как уже говорилось, RTP генерируется из портов с четным номером, в то время как RTCP работает на порту следующего более высокого нечетного номера. RTCP передает информацию и статистику, например дрожание, количество октетов и пакетов, а также время в оба конца. Конкретное приложение использует эти данные для управления параметрами QoS и выбора, например, для использования отдельного кодека.

2.8.5. Безопасный транспортный протокол реального времени (SRTP)

SRTP является одним из протоколов безопасности, используемых для технологии WebRTC [54], и был опубликован как RFC 3711 IETF (Internet Engineering Task Force) в 2004 году.

По сути, это расширенный компонент RTP (транспортный протокол реального времени), который добавляет элементы безопасности, аутентификацию в виде сообщений, защиту конфиденциальности и воспроизведения, в основном для IP-связи. Кроме того, он использует шифрование и аутентификацию для снижения рисков атак, таких как отказ в обслуживании [121].

2.8.6. Протокол описания сеанса (SDP)

Будучи опубликованным IETF как RFC 4566, SDP определяет конкретный стандарт для определения параметров, используемых при обмене мультимедиа (в основном потоковыми мультимедиа) между двумя конечными точками. Для этого SDP содержит следующие данные:

- какой IP-адрес будет принимать входящий медиапоток;
- какой номер порта используется для входящего медиапотока;
- какую категорию мультимедиа конечная точка ожидает получить (обычно аудио);
- по какому протоколу конечная точка ожидает обмена данными (обычно RTP);
- какую кодировку сжатия способна декодировать конечная точка (кодек).

В типичном процессе инициирования сеанса две конечные точки участвуют в сеансе. Каждая конечная точка передает SDP другой конечной точке, чтобы сообщить о своих спецификациях и возможностях. На самом деле SDP сам по себе не отправляет никаких носителей, а ограничивается согласованием подходящего набора параметров обмена мультимедиа. Даже медиапотоки также обрабатываются некоторыми различными протоколами и каналами.

2.8.7. Кодеки

Аудиокодеком называют программу или алгоритм, который сжимает либо разжимает цифровые звуковые данные, позволяя снизить требования к пропускной способности канала передачи данных. В IP-телефонии на сегодняшний день наиболее распространено преобразование посредством кодека G.729, а также сжатие G.711 по A-закону (a-law) и μ-закону (u-law) [53].

Кодек G.729 [53] сжимает исходный сигнал с потерей данных. Основная идея, заложенная в G.729 – передача не самого оцифрованного сигнала, а его параметров (спектральной характеристики, количества переходов через ноль), достаточных для последующего синтезирования на принимающей стороне. При этом все основные характеристики голоса, такие как амплитуда и тембр, сохраняются.

Данный кодек рассчитан на пропускную способность канала 8 кбит/с. Длина кадра, обрабатываемого G.729 – 10 мс, частота дискретизации – 8 кГц. Для каждого из таких кадров определяются параметры математической модели, которые в дальнейшем и передаются в канал в виде кодов.

При использовании кодирования G.729 задержка составляет 15 мс, из которых 5 мс тратится на заполнение предварительного буфера. Отметим также, что кодек G.729 предъявляет достаточно высокие требования к ресурсам процессора.

Кодек G.711 [53] – голосовой кодек, который не предполагает никакого сжатия, помимо компандирования – метода уменьшения эффектов каналов с ограниченным динамическим диапазоном. В основе данного метода лежит принцип уменьшения количества уровней квантования сигнала в области высокой громкости с сохранением качества звука. Сигнал в данном кодеке предоставлен потоком величиной 64 кбит/с. Частота дискретизации – 8000 кадров по 8 бит в секунду. Качество голоса субъективно лучше, нежели при применении кодека G.729.

Две широко использующиеся в телефонии схемы компаундирования – a-law и u-law. A-law или A-закон – алгоритм сжатия звуковых данных с потерей информации, который в основном используется на территории Европы и России. Для сигнала *x* преобразование по алгоритму a-law выглядит следующим образом (1):

$$F(x) = sgn(x) \begin{cases} \frac{A|x|}{1+\ln(A)}, |x| < \frac{1}{A} \\ \frac{1+\ln(A|x|)}{1+\ln(A)}, \frac{1}{A} \le |x| \le 1 \end{cases}, \quad (1)$$

где A – параметр сжатия (обычно принимается равным 87,7).

U-law или μ-закон – алгоритм сжатия звуковых данных с потерей информации, который в основном используется на территории Японии и Северной Америки. Для сигнала *x* преобразование по алгоритму U-law выглядит так (2):

$$F(x) = sgn(x)\frac{\ln(1+\mu|x|)}{\ln(1+\mu)}, -1 \le x \le 1, \quad (2)$$

где μ = 255 (8 бит) в стандартах Северной Америки и Японии.

Работа кодеков основана на импульсно-кодовой модуляции, то есть на передаче непрерывной функции в виде серии последовательных импульсов. Для получения на входе канала связи модулированного сигнала мгновенное значение несущего сигнала оцифровывается с помощью АЦП с определенным периодом. При этом количество оцифрованных значений в секунду (иначе, частота дискретизации) должно быть большим или равным двукратной максимальной частоте в спектре аналогового сигнала. Далее полученные значения округляются до одного из заранее принятых уровней. Заметим, что количество уровней необходимо принимать кратным степени двойки. В зависимости от того, сколько было определено уровней, сигнал кодируется определенным количеством бит (рисунок 2.13).

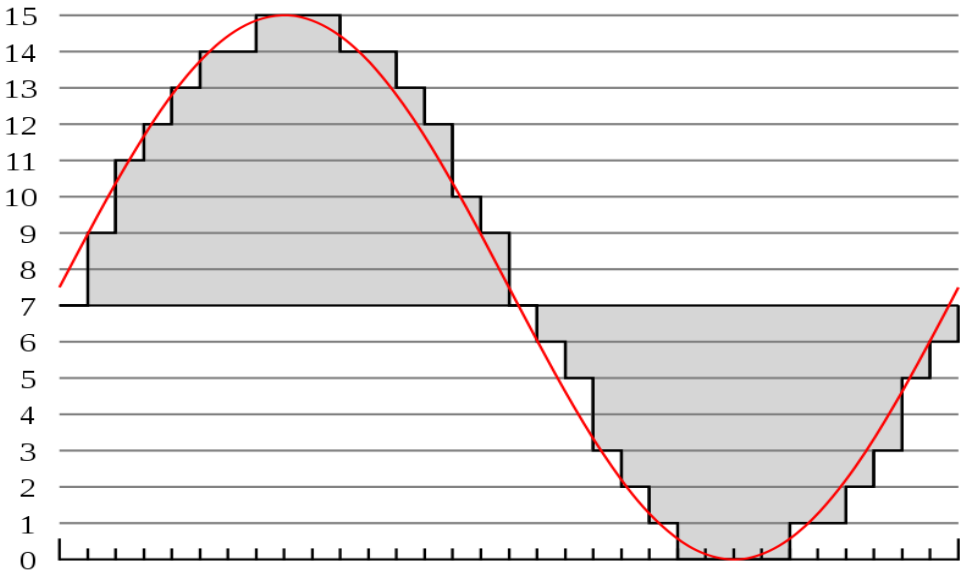


Рисунок 2.13. Квантование сигнала [53]

На рисунке 2.13 представлено кодирование с помощью четырех битов (то есть все промежуточные значения аналогового сигнала будут округляться до одного из заранее заданных 16 уровней). Для примера, в момент времени 0 сигнал будет представлен как 0111.

При демодуляции последовательность нулей и единиц преобразуется в импульсы демодулятором, уровень квантования которого равен уровню квантования модулятора. После этого ЦАП на основе данных импульсов восстанавливает сигнал, а сглаживающий фильтр окончательно убирает неточности.

В современной телефонии число уровней квантования должно быть большим или равным 100, то есть минимальное количество бит, которым может кодироваться сигнал – 7.

2.9 Вопросы качества обслуживания в IP-телефонии

2.9.1. Механизмы улучшения качества обслуживания

В сетях на основе стека TCP/IP высокое качество обслуживания трафика, чувствительного к задержкам передачи, не обеспечивается по умолчанию. При использовании протокола TCP имеется гарантия достоверной доставки информации, но ее перенос может осуществляться с непредсказуемыми задержками. Для UDP характерна минимизация задержек, но гарантия верной доставки пакета отсутствует [89]. В то же время добротность речевого трафика сильно зависит от качества передачи, и в сети, где не реализованы механизмы, гарантирующие соответственное качество, реализация IP-телефонии может не удовлетворять требованиям пользователей.

Основными показателями качества обслуживания являются пропускная способность сети и задержка передачи. Задержка при этом определяется как промежуток времени, прошедший с момента отправки пакета до момента его приема. Также существуют такие характеристики, как готовность сети и ее надежность (оцениваются по результатам контроля уровня обслуживания в течение длительного времени, либо по коэффициенту использования).

Для улучшения качества связи используются следующие механизмы:

1) Перемаршрутизация, что позволяет при перегрузке одного из каналов связи осуществить доставку при помощи резервных маршрутов.

2) Резервирование ресурсов канала связи на время соединения.

3) Приоретизация трафика, что дает возможность помечать пакеты в соответствии с уровнем их важности и производить обслуживание на основе меток.

Как было сказано ранее, голосовой трафик чрезвычайно чувствителен к задержкам передачи. Максимальное время задержки не должно превышать 400 мс (сюда включается и продолжительность обработки информации на конечных станциях). Различают два основных типа задержки:

- Задержка при кодировании информации в голосовых шлюзах или терминальном оборудовании. Уменьшается путем улучшения алгоритмов обработки и преобразования голоса.
- Задержка, вносимая сетью передачи. Уменьшается путем улучшения сетевой инфраструктуры, в частности, сокращением количества маршрутизаторов и использованием высокоскоростных каналов

На рисунке 2.14 [89] показаны источники задержек в IP-телефонии.

Еще одно явление, характерное для IP-телефонии – jitter, или, иначе, случайная задержка распространения пакета. Возникновение jitter обусловливается тремя фактами:

– ограниченная полоса пропускания или некорректная работа активных сетевых устройств;

– высокая задержка распространения сигнала;

– тепловой шум.

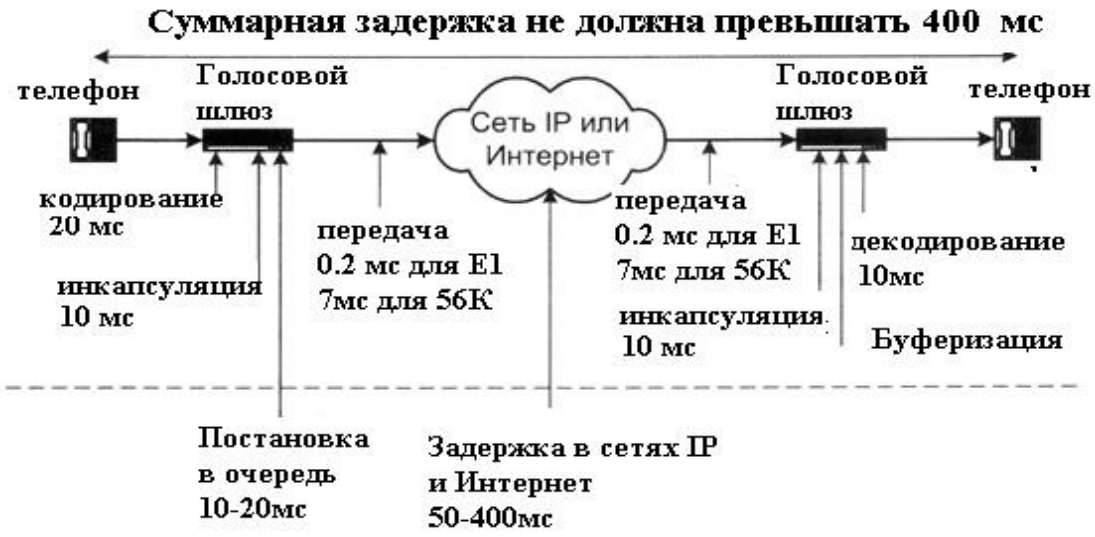


Рисунок 2.14. Источники задержки в IP-телефонии

2.9.2. Jitter

Обычно предусматривается динамическая подстройка длины буфера в течение всего времени существования соединения. Для выбора наилучшей длины используются эвристические алгоритмы [92].

Для компенсации неравномерной скорости поступления пакетов на приемной стороне создают временное хранилище пакетов, или так называемый jitter-буфер. Его задача – собрать поступающие пакеты в правильном порядке в соответствии с временными метками и выдать их кодеку с правильными интервалами и в правильном порядке. На рисунке 2.15 [92] продемонстрирован принцип работы jitter-буфера.

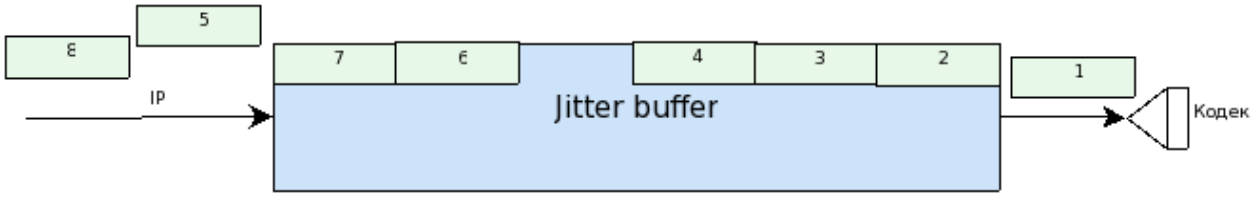


Рисунок 2.15. Jitter-буфер

Размер буфера приемного VOIP-устройства либо рассчитывается в процессе работы, либо принудительно задается в настройках. С одной стороны, размер буфера не может быть слишком большим, чтобы не увеличивать транспортную задержку. С другой стороны, маленький буфер вызывает потери пакетов при изменениях времени задержки в IP сети.

Отсюда и происходит одно из главных противоречий между интернет-провайдерами и пользователями IP-телефонии. С точки зрения провайдера все пакеты доставлены абоненту, т.е. потерь нет. А с точки зрения VoIP устройства разница во времени между приходом пакетов значительно превышает jitter-буфер, поэтому фактически потери есть. На практике потеря более 1% уже вы-

зывает определенные неприятные ощущения, при 2% разговор оказывается затруднен, а при значениях больше 4% разговор уже практически невозможен.

Рассмотрим расчет размера jitter-буфера [92].

Случайная задержка распространения J_i для i-го пакета может определяться по формуле (1):

$$J_i = J_{i-1} + \frac{|D_{i-1}| - J_{i-1}}{16}, \quad (1)$$

где D_i – отклонение от ожидаемого времени прибытия i-го пакета, которое определяется по формуле (2):

$$D_i = (R_i - R_{i-1}) - (S_i - S_{i-1}), \quad (2)$$

где R – время прибытия пакета в метках времени RTP, S – временная метка RTP, взятая из пакета.

Приведем пример расчета ожидаемого размера случайной задержки распространения 5-го пакета на основе формул (1) и (2).

Пусть $J_4 = 10$ мс, $R_4 = 10, R_3 = 11, S_4 = 6, S_3 = 5$, тогда $D_5 = -2$. В таком случае ожидаемый размер случайной задержки рассчитаем по формуле (3):

$$J_5 = 10 + \frac{|-2| - 10}{16} = 9{,}5 \text{ (мс)}. \quad (3)$$

Тогда для того, чтобы ни один пакет не был отброшен, размер-jitter буфера должен быть равным 9,5 мс. Для определения требуемого размера jitter-буфера в мегабайтах необходимо домножить полученное значение на 100 мбит/сек – среднюю пропускную способность сети, которая равна 128 кб.

Размер jitter-буфера должен быть больше, чем флуктуация транзитного времени в сети. Например, если время транзита пакетов колеблется от 5 до 10 мс, то буфер должен иметь размер 10 мс, чтобы ни один пакет не был потерян. При еще большем буфере (например, 12 мс) сможет работать механизм перезапроса потерянных пакетов.

2.10 Проблемы IP-телефонии

Наиболее распространенные проблемы IP-телефонии и способы их решения [121] охарактеризованы ниже.

Потребность в источнике питания. Устройства или трубки IP-телефонии работают от сети и получают это питание от настенной розетки. Таким образом, может быть больше шансов на его выход из строя во время локальных отключений электроэнергии, пока не будет доступно аварийное питание. В этом случае необходимо надежное резервное питание, чтобы избежать подобных проблем с Интернет-телефонией.

Сжатие голоса. Если качество вызова соответствует требованиям, но возникла проблема передачи голоса, то, скорее всего, имеет место неисправность настроек кодека. В этом случае единственный выход из ситуации – провести тестирование с различными кодеками, чтобы выяснить, какой из них будет лучшим. Если искажение звука происходит в самое загруженное время, тогда, вероятно, возникла какая-то проблема с пропускной способностью. В таком случае необходимо обновить интернет-сервис.

Проблемы выбора интернет-провайдера. При выборе интернет-провайдера необходимо принимать во внимание следующие факторы [93]:

– политика ценообразования (стоимость подключения номера, абонентская плата, исходящие вызовы);
– номера и дополнительный функционал (есть ли у оператора телефонии номера с нужными префиксами, т.е. с региональными номерами).
– прием и распределение входящих звонков; стратегия дозвона до сотрудника или отдела выбирается исходя из того, какие задачи нужно решить;
– автоматизация приема звонков, что обеспечивает моментальное соединение клиента с персональным менеджером или с сотрудником, с которым он общался в последний раз.

В случае постоянных проблем необходимо связаться с интернет-провайдером и немедленно проверить его услуги – возможно, у интернет-провайдера есть периоды высокой задержки в соединении, или данные отправляются по общедоступной сети вместо частной. В этом случае нужно узнать, можно ли решить проблему с помощью действующего интернет-провайдера или стоит переключиться на нового.

Так как системы IP-телефонии подключены к Интернету и прямо или косвенно зависят от пропускной способности сети, в них так или иначе будут возникать связанные с этим проблемы, однако они могут быть устранены довольно быстро.

2.11 Решения для развертывания телефонной сети

2.11.1 Asterisk

Asterisk [31, 33] – программная АТС, способная коммутировать как VoIP вызовы, так и вызовы, осуществляемые между IP-телефонами и традиционной телефонной сетью общего пользования. Поддерживаемые протоколы: IAX, SIP, H.323, Skinny, UNIStim. Поддерживаемые кодеки: G.711 (U-law и A-law), G.722, G.723, G.729, GSM, iLBC, LPC-10, Speex.

Asterisk – открытое программное обеспечение, которое может быть установлено без оглядки на лицензирование. Это делает данную программную АТС привлекательной для малого и среднего бизнеса. Количество абонентов в сети может достигать 2000 и ограничено только мощностью сервера.

Еще одно достоинство Asterisk – возможность гибкой настройки. Весь необходимый функционал либо уже реализован, либо может быть дописан самостоятельно без существенных временных и денежных затрат. Этому способствует принцип: одна задача – один программный модуль.

В сравнении с решениями от таких вендоров, как Cisco или Avaya, Asterisk привлекателен еще и стоимостью развертывания. Фактически все затраты сводятся только к покупке телефонных аппаратов и сервера, способного обеспечить требуемую нагрузку на сеть. Сама программа абсолютно бесплатна.

2.11.2 Cisco Unified Communication Manager (Call Manager)

Call Manager [60] предназначен скорее для крупных сетей, включающих до 30000 абонентов. Данный программно-аппаратный комплекс обеспечивает надежность работы и позволяет конфигурировать множество параметров, таких как переадресация звонков или голосовое меню. Существует и «облегченная» express-версия, предназначенная скорее для офисов.

Из преимуществ Cisco Call Manager следует отметить в первую очередь знаменитую техническую поддержку корпорации Cisco. При соответствующем уровне контракта на обслуживание любая проблема, начиная с вопросов по настройке и заканчивая вышедшим из строя оборудованием, будет решена практически мгновенно. Поэтому Cisco Call Manager подойдет компаниям, готовым платить немалые деньги, но и получать при этом высочайшее качество обслуживания.

2.11.3 Avaya IP Office

Система Avaya IP Office [100] может стать неплохим выбором для телефонной сети среднего размера. Количество абонентов здесь ограничено не только мощностью сервера, но и количеством приобретенных лицензий. Лицензировать необходимо практически все – платы расширения, используемые приложения и т.д., что может доставить определенные неудобства.

Конфигурирование может осуществляться через ряд программ, но наиболее популярная и простая в обращении – Avaya IP Office Manager. Также возможно управление через консоль с помощью Avaya Terminal Emulator.

В целом продукция корпорации Avaya не ограничивается одним IP Office. Avaya, в 2009 году слившаяся с еще одним известным производителем Nortel, является признанным лидером на рынке оборудования для IP-телефонии.

Резюме

IP-телефония – это вид связи, который использует Интернет для обмена голосовыми сообщениями и обладает рядом преимуществ, таких как низкая стоимость, мобильность, отсутствие дополнительных кабелей, гибкость, видеоконференцсвязь, сеть унифицированных коммуникаций (UC), интеллектуальное решение для мобильности подключения, простая в использовании технология WebRTC, богатый функциональными возможностями коммуникационный аспект, простота установки и настройки, простота масштабируемости, экономия затрат при повышении производительности.

Принцип работы IP-телефонии состоит в соединении с сетевым шлюзом, оцифровке голосового сигнала, сжатия канала, разбиения на пакеты, соединения с приемной стороной.

В IP-телефонии используются протоколы SIP, H.323, RTP, RTCP, SRTP, SDP и другие. Они имеют разный функционал, но самым популярным является протокол SIP [12]. Также используются кодеки G.729, G.711 и импульсно-кодовая модуляция.

Конечно, IP-телефония имеет ряд проблем: потребность в источнике питания, сжатие голоса, проблемы Интернет-провайдера, но в целом использование IP-телефонии является хорошим и эффективным решением.

Вопросы для самопроверки

1. В чем отличие IP-телефонии от IP-протокола?
2. Раскройте принцип работы IP-телефонов.
3. В чем заключаются сжатие каналов и разбиение сообщения на пакеты?
4. Дайте общепринятое определение термину «физический уровень (MAC-адрес)».
5. Дайте общепринятое определение термину «сетевой уровень (IP-адрес)».
6. Дайте общепринятое определение термину «символьный уровень (DNS)».
7. Кратко опишите физический уровень модели OSI в сетях IP-телефонии. Приведите примеры.
8. Кратко опишите канальный и сетевой уровни модели OSI в сетях IP-телефонии.
9. В чем заключается функционал основных протоколов уровня данных IP-телефонии?
10. Каков типовой состав структуры SIP-сети?
11. Для чего предназначена система протоколов H.323?
12. Для чего нужны шлюзы в системе протоколов H.323?
13. В чем заключается основной функционал гейткипера?
14. Существует ли в настоящее время необходимость применения протокола SRTP и почему?
15. Раскройте понятие кодеков в IP-телефонии.
16. Каковы проблемы качества обслуживания абонентов в IP-телефонии?
17. В чем заключается jitter как явление, характерное для IP-телефонии?
18. Перечислите основные проблемы выбора Интернет-провайдера?
19. Каково назначение Cisco Unified Communication Manager (Call Manager)?
20. Решает ли сегодня применение технологий IP-телефонии проблему обеспечения качества телефонной связи абонентам при развертывании вычислительных сетей?

Раздел 3. СОВРЕМЕННЫЕ ТЕХНОЛОГИИ IP-ТЕЛЕФОНИИ

3.1. Общие сведения

IP-телефония является неотъемлемой частью современной жизни многих людей и владельцев бизнеса по всему миру. За многие десятилетия технология претерпела значительные изменения. Сегодня IP-телефония – это больше, чем просто «голос» по интернет-протоколу (SIP), это возможность доступа к видео, контенту и другим формам важных данных в быстро меняющейся коммуникационной среде. Услуги IP-телефонии позволяют совершать и принимать звонки, проверять голосовую почту, проводить конференцсвязи и т. д. с помощью интеллектуальных устройств. IP-телефония стала технологией, которая изменила то, как мы сегодня общаемся друг с другом по всему миру, и эта технология готова к дальнейшему развитию.

Развитие технологий IP-телефонии происходило постепенно – от появления новых кодеков с улучшенным алгоритмом сжатия данных до выпуска современных приложений массового пользования. В данном разделе рассматриваются современные технологии IP-телефонии как на уровне сетевого устройства, так и на уровне программных решений, в том числе кодеки IP-телефонии и алгоритмы для улучшения качества связи, в частности, для повышения эффективности использования пропускной способности. Далее описан современный стандарт WebRTC, его применение, достоинства и недостатки.

Видеозвонки и WebRTC становятся популярными и занимают центральное место в нашей жизни. В разделе показано, как WebRTC заботится о безопасности и конфиденциальности и как новые технологии позволяют реализовывать сквозное шифрование в видеоконференциях, причем приводится не только теоретическая база стандарта WebRTC, но и практическое применение новой функции шифрования на примере использования приложения для видеосвязи Jitsi Meet.

Немаловажную роль в развитии технологий IP-телефонии сыграло появление ИИ. ИИ используется на различных коммуникационных платформах для повышения эффективности. Подобные приложения трансформируют и изменяют индустрию связи. В разделе рассмотрена такая популярная отрасль, как интерактивное голосовое меню, развитию которого способствует рост спроса на улучшение управления взаимоотношениями с клиентами [23, 75]. Растущее внедрение передовых технологий и рост числа облачных сервисов также стимулирует развитие технологии IVR. Все более широкое применение находят системы интерактивного голосового ответа в таких отраслях, как банковские и финансовые услуги, здравоохранение, путешествия, гостиничный бизнес и других приложениях для навигации или взаимодействия с вызывающими абонентами.

В разделе рассматриваются известные пользовательские приложения IP-телефонии, такие как Skype, Whatsapp, Telegram, а также бизнес-приложения Google Meet, Zoom, Jitsi Meet, Microsoft Teams, Webex Teams. Данные приложе-

ния проанализированы с точки зрения функциональности, используемых протоколов, передачи трафика, а также пользовательского рейтинга мобильных приложений, взятого из сервисов Google Play Store и App Store.

3.2. Кодеки в IP-телефонии

Кодек IP-телефонии – это технология, совмещающая в себе сжатие и обратный сжатию процесс (Compression and Decompression). Кодек преобразует аналоговые голосовые сигналы в цифровые пакеты или сжатую цифровую форму для передачи, а затем обратно в несжатый аудиосигнал. Кодек производит выборку формы сигнала через регулярные интервалы времени и генерирует значение для каждого образца. Как правило, выборки делаются 8 000 раз в секунду. Образцы накапливаются в течение определенного периода времени для создания кадра данных. Кодеки IP-телефонии определяют качество звука, пропускную способность и сжатие телефонных звонков по протоколу VoIP. Кодеки IP-телефонии используют либо собственные алгоритмы, либо алгоритмы с открытым исходным кодом. Алгоритмы кодеков стремятся минимизировать скорость передачи в цифровом представления сигнала без ощутимой потери качества сигнала.

Кодеки IP-телефонии отличаются способом сжатия звука. Сжатие необходимо для передачи звука, поскольку он требует большой пропускной способности, которая ограничена. Также важными характеристиками кодека являются количество битов, производимых в секунду, и период выборки – он определяет, как часто образцы передаются. Эти две характеристики определяют размер кадра.

Высокое качество достигается при низкой скорости передачи данных за счет использования избыточности сигнала, а также знания того, что определенные типы искажений при кодировании незаметны, поскольку они маскируются сигналом [15]. Модели избыточности сигнала и искажений маскировки становятся все более сложными, что приводит к постоянному улучшению качества сигналов с низкой скоростью передачи [26].

Рассмотрим самые популярные кодеки в IP-телефонии [55].

Кодек G.711. Международный союз электросвязи (ITU) представил кодек G.711 в 1972 году для использования в IP-телефонии. Этот кодек имеет два варианта: μ-закон и A-закон. В США и Японии используется μ-закон, в Европе – A- закон. Этот кодек может сжимать 16-битные образцы в 8 бит посредством логарифмического сжатия. В результате достигается коэффициент сжатия 1:2. Скорость передачи данных для обоих направлений достаточно велика и составляет 128 кбит/с (64 кбит/с для одного тракта).

Несмотря на высокое качество звука, требования к пропускной способности данного кодека также высоки. Кроме того, этот кодек не поддерживает несколько телефонных звонков так хорошо, как другие кодеки, например G.729. Кодек G.711 используется для всех видов приложений IP-телефонии, поскольку лицензионные сборы не взимаются. В нем также отсутствует цифровое сжатие,

поэтому он считается лучшим кодеком IP-телефонии для взаимодействия с телефонной сетью общего пользования.

Кодек G.723.1 – двухскоростной речевой кодер для мультимедийных коммуникаций, передаваемых со скоростью 5,3 (использует алгоритм MPC-MLQ с 24-байтовыми кадрами) и 6,3 кбит/с (использует алгоритм ACELP с 20-байтовыми кадрами). Кодек предназначен для голоса и сжимает голосовой звук в кадры длительностью 30 мс, также имеет низкие требования к пропускной способности. Не подходит для передачи музыки и невербальных звуков.

Кодек G.729 кодирует звук в виде кадров. Каждый кадр длится 10 миллисекунд и содержит 80 аудиочастей. Скорость передачи данных для одного направления этого не-HD кодека составляет 8 кбит/с. Поскольку сжатие выше, можно одновременно совершать больше звонков из своей сети. Данный кодек предполагает низкие требования к пропускной способности с приемлемым качеством звука. При этом некоторые провайдеры IP-телефонии могут не поддерживать кодек G.729. Музыка и другие невербальные звуки могут звучать нечетко.

В таблице 3.1 представлены основные кодеки и их характеристиками (данные взяты из исследования [21]), где MOS (Mean Opinion Score) – это усредненная оценка разборчивости речи.

Таблица 3.1 – Характеристики кодеков

Кодек	Скорость передачи данных (кБ/с)	Интервал выборки (мс)	MOS	Размер рабочей нагрузки (байт)	Пропускная способность с Ethernet (кБ/с)	Пропускная способность с RTP или FRF (кБ/с)
G.711	64	10	4.10	160	87.2	67.6
G.723	6.3	30	3.90	20	20.8	7.7
	5.3	30	3.80	20	31.2	11.6
G.729	8	10	3.92	24	21.9	8.8

Одной из основных проблем, стоящих перед развертыванием IP-телефонии, является достижение и поддержание приемлемого качества голоса. Качество голоса, воспринимаемое пользователем в сети IP-телефонии, должно соответствовать качеству голоса в обычных сетях. На воспринимаемое качество голоса влияет множество факторов, включая задержку, джиттер, потери пакетов и используемые системы голосовых кодеков. Большинство из этих факторов зависят от пропускной способности и других характеристик сетевых каналов. Все эти факторы необходимо учитывать для надлежащей обработки трафика IP-телефонии. Кроме того, так как нагрузка на вызовы значительно варьируется в зависимости от частоты дискретизации, обеспечиваемой различными системами кодеков, такими как G.711, G.729, то правильный выбор и использование системы кодеков IP-телефонии имеют решающее значение для качества голоса. Вы-

зывающий и вызываемый телефоны договариваются о выборе подходящего кодека при каждой попытке соединения. Как вызывающий, так и принимающий телефоны имеют список приоритетов для согласования правильного кодека.

Учитывая перечисленные параметры, можно подобрать необходимый кодек. Например, для достижения высокого качества связи больше подходит кодек G.711. При больших требованиях к пропускной способности подойдет кодек G.729. Кодек G.711 может быть выбран для IP-телефонии в сети WLAN. Для сети WiMAX наиболее эффективным является кодек G.729. Качество кодека G.723.1 является наиболее низким, следовательно, он может быть использован во всех сетях в зависимости от окружающей среды и плотности пользователей.

3.3. Алгоритмы повышения эффективности полосы пропускания

3.3.1. Пути уменьшения нагрузки на трафик

Одним из важных аспектов повышения производительности приложений IP-телефонии является уменьшение нагрузки на трафик сети. Для этого существует множество методов, из которых можно выделить три основных:

1. Мультиплексирование пакетов
2. Сжатие заголовков пакетов
3. Сжатие полезной нагрузки пакетов

При этом важно отметить, что сжатие полезной нагрузки пакетов включает комплексное применение первых двух способов в целях увеличения пропускной способности канала передачи данных. Соответственно, далее мы рассмотрим два основных способа – мультиплексирование и сжатие заголовков пакетов, понимая при этом, что применение сложных алгоритмов сжатия может привести из-за компрессии и декомпрессии к дополнительным задержкам передачи пакета по любому каналу связи.

Способы повышения эффективности использования полосы пропускания IP-телефонии основаны на том, что каждый пакет содержит достаточно большой заголовок. В таблице 3.2 представлены данные об использовании полосы пропускания заголовками пакетов в сравнении с полезной нагрузкой [20].

Таблица 3.2 – Использование заголовком пакета полосы пропускания в зависимости от размера пакета

Кодек	Размер пакета (байт)	Размер полезной нагрузки – данных пакета (байт)	Размер заголовка пакета (байт)	Использование заголовком полосы пропускания
G.729	80	20	60	75.0%
G.728	120	60	60	50.0%
G.723.1	80	20	60	75.0%
G.726	140	80	60	42.9%

Из таблицы 3.2 можно сделать вывод, что заголовки занимают в среднем около 60% полосы пропускания, что значительно расходует пропускную способность. Таким образом, большинство методов направлены на уменьшение размера заголовка пакетов, для чего могут использоваться методы мультиплексирования пакетов и методы сжатия заголовков.

3.3.2. Методы мультиплексирования пакетов

Методы мультиплексирования пакетов объединяют в один заголовок несколько пакетов IP-телефонии, которые имеют один и тот же маршрут к назначению. Соответственно, эти методы значительно уменьшают использование полосы пропускания заголовками пакетов. Количество пакетов ограничивается определенными параметрами, например, допустимой задержкой.

Есть несколько вариантов реализации мультиплексирования пакетов в зависимости от сети и параметров управления размерами пакетов. Один из примеров – метод [46] мультиплексирования для беспроводных сетей IEEE 802.11n, который работает на втором уровне модели OSI. Кадры IP-телефонии мультиплексируются в один Aggregation MAC Protocol Data Unit (A-MPDU). Схема объединения данных представлена на рисунке 3.1.

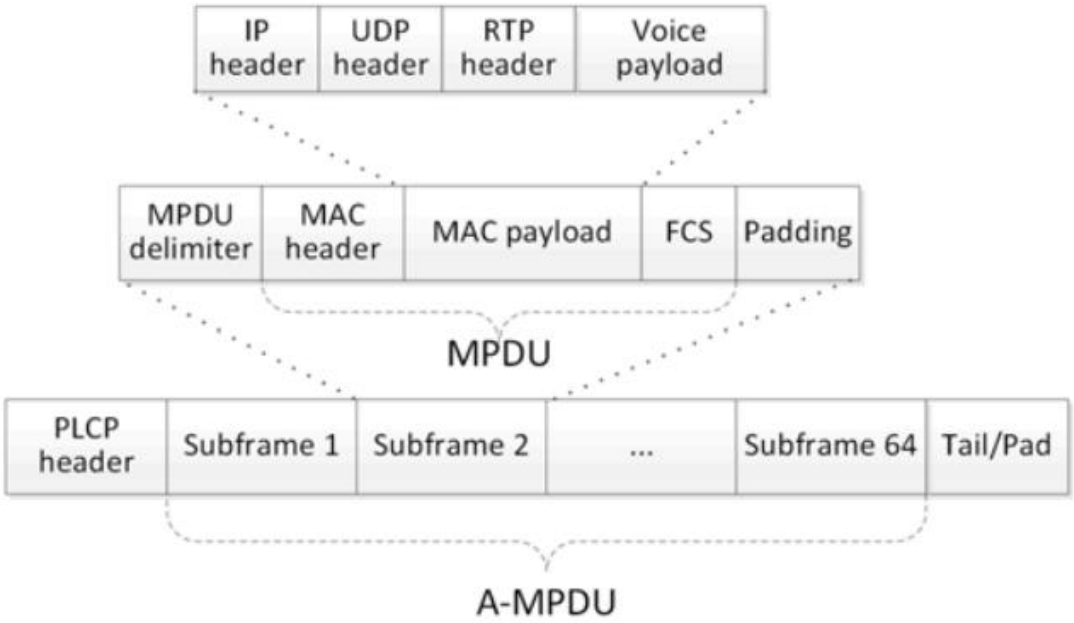


Рисунок 3.1. Aggregation MAC Protocol Data Unit

Если один из кадров внутри A-MPDU был поврежден, повторно отправляется только поврежденный кадр. Метод контролирует размер мультиплексированных кадров на основе загрузки канала, задержки от протоколов RTP/RTCP, буферной задержки, средней задержки доступа к среде. Уровень транспортного протокола реального времени (RTP/RTCP) измеряет сквозную задержку каждого полученного голосового RTP-пакета и периодически отправляет пакеты отчета приемника (RR) источнику. Пакет RR включает в себя максимальное значение сквозной задержки, наблюдаемое в течение последнего периода. После получе-

ния RR-пакета уровень RTP/RTCP источника передает полученную информацию о максимальной сквозной задержке предложенному планировщику агрегации на уровне MAC. Более того, планировщик агрегации отправителя непрерывно измеряет задержку доступа к среде для каждого успешно переданного голосового кадра.

Авторы [46] провели моделирование метода с 50 узлами, передающими со скоростью 600 Мбит/с, и показали улучшение производительности на 160% по сравнению с аналогичными методами в протестированных сценариях. Предложенная схема обеспечила пропускную способность до 275 Мбит/с против 0,13 Мбит/с у типичной схемы; при этом предложенная схема доставила все голосовые пакеты, и более 99,9% из них имели задержку менее 150 мс.

Еще одним примером использования данного метода является исследование [4]. Авторы предложили метод Payload Shrinking and Packets Coalesce (PS-PC), который уменьшает объем бесполезно расходуемой полосы пропускания путем мультиплексирования заголовков пакетов, а также сокращения полезной нагрузки пакета IP-телефонии до меньшего размера на основе предложенного алгоритма. PS-PC развертывается на шлюзе IP-телефонии, который представляет собой точку выхода для огромного числа одновременных вызовов IP-телефонии, которые направляются в один и тот же конечный шлюз IP-телефонии. На рисунке 3.2 показан участок сети, где работает метод PS-PC. PS-PC состоит из двух основных компонентов, а именно: PS-PC на стороне отправителя (S-PS-PC) и PS-PC на стороне получателя (R-PC).

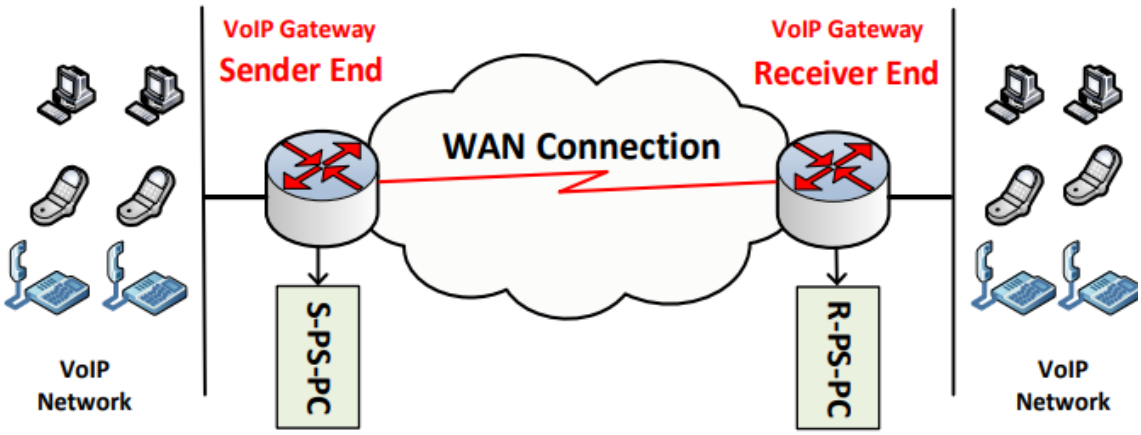


Рисунок 3.2. Участок сети с использованием PS-PC

В компоненте S-PS-PC выполняются 2 основные функции для улучшения использования полосы пропускания IP-телефонии: мультиплексирование пакетов и уплотнение полезной нагрузки пакетов. Процесс состоит из следующих шагов:

1. Группировка входящих пакетов IP-телефонии на основе шлюза IP-телефонии получателя;

2. Разделение заголовка и полезной нагрузки пакетов IP-телефонии;

3. Сокращение полезной нагрузки до меньшего размера на основе предложенного алгоритма;

4. Задание уникального идентификатора для каждого вызова. Этот идентификатор будет добавлен в заголовок каждого пакета, принадлежащего данному вызову;

5. Прикрепление оригинального заголовка ITTP вместе с новым заголовком к каждому пакету полезной нагрузки;

6. Соединение всех пакетов;

7. Добавление IP-заголовка.

Алгоритм уменьшения основан на том факте, что размер полезной нагрузки не изменяется в течение всего времени разговора. Таким образом, удаление некоторых битов из начала или конца полезной нагрузки может быть легко восстановлено, если разработать подходящий алгоритм.

В компоненте R-PS-PC создаются исходные пакеты IP-телефонии и отправляются по назначению. Процесс содержит следующие шаги:

1. Разделение пакета на IP-заголовок и полезную нагрузку;

2. Разделение заголовка и ITTP-заголовка каждого пакета, чтобы получить полезную нагрузку;

3. Восстановление исходного размера пакета на основе информации в заголовке. Восстановление исходного адреса IP-заголовка на основе таблицы состояний;

4. Присоединение ITTP-заголовка вместе с IP-заголовком к полезной нагрузке, полученной на предыдущем шаге, что восстанавливает исходный пакет, который прибыл на сторону отправителя;

5. Передача пакетов, сформированных на шаге 6, по назначению.

Авторы говорят о том, что предложенный метод PS-PC обеспечивает лучшее использование полосы пропускания, чем традиционный протокол ITTP. Помимо мультиплексирования пакетов, авторы также использовали метод уплотнения полезной нагрузки, которые описаны ниже.

Можно выделить следующие достоинства метода мультиплексирования пакетов:

1. Улучшение пропускной способности сети;

2. Непрерывность и последовательность передаваемых пакетов;

3. Гарантированная доставка данных.

Однако метод мультиплексирования имеет и недостатки:

1. Отсутствие приоритизации пакетов. Некоторые пакеты должны иметь более быстрое прохождение, чем другие. Однако в этом методе мультиплексированные пакеты будут иметь одинаковое обслуживание при прохождении по сети.

2. Отсутствие скрытия потерянных пакетов, следовательно, ухудшение четкости вызова. При потере пакета приложения IP-телефонии используют специальные механизмы для его сокрытия, чтобы улучшить четкость вызова. Механизмы сокрытия эффективны для типичных небольших пакетов IP-телефонии, но не в случае с объединенными пакетами. Таким образом, потерянный пакет не будет скрыт, и четкость вызова будет ухудшена.

3. Плохая работа в сети с маленьким количеством пакетов. Мультиплексирование большего количества пакетов в один обеспечит лучшую эффективность использования полосы пропускания. Но в случае небольшого количества сеансов пакеты должны ждать в буфере до тех пор, пока не поступит достаточное количество пакетов для мультиплексирования.

4. Увеличение задержки пакетов. Процесс мультиплексирования занимает время в зависимости от используемого метода. Поэтому время ожидания в буфере вместе со временем время мультиплексирования приведет к некоторой задержке и тем самым повлияет на четкость вызова.

5. Потребление ресурсов. Процесс мультиплексирования потребляет ресурсы устройства мультиплексирования.

Таким образом, методы мультиплексирования пакетов эффективны в сети с большим количеством пакетов, где имеется достаточно ресурсов для обеспечения алгоритма мультеплексирования, а также где важен порядок передачи пакетов и гарантированная доставка. Они не подходят для сетей с небольшим трафиком, где приоритизирована скорость передачи пакетов, а также четкость вызова.

3.3.3. Методы сжатия заголовков

Методы сжатия заголовков используют две особенности в пакетах IP-телефонии для уменьшения размера заголовка. Первая особенность основана на неизменяющихся полях в заголовке, а вторая – на постоянно увеличивающихся полях. Как пример использования данного метода можно привести исследование [4]. Авторы предлагают в качестве решения метод уменьшения или обнуления полосы пропускания или SmlZr (Smallerize/Zeroize). Метод SmlZr разработан специально для звонков P2P IP-телефонии в сетях IPv6. Суть предлагаемого метода заключается в сокращении размеров ненужных полей в заголовке для сохранения полезной части пакета. Авторы проводят анализ полей заголовков пакетов RTP/UDP/IPv6 IP-телефонии и выделяют поля, которые можно сократить:

1) Поля заголовка пакета IPv6, который используется во всех приложениями в сетях на базе IP.

1. Информация об адресе источника IPv6 (SIPv6) не нужна приложениям IP-телефонии, поскольку приложения IP-телефонии не являются приложениями «запрос/ответ». Абоненты знают IPv6-адреса друг друга во время установки вызова. Во время разговора пакет IP-телефонии передается на уже известный адрес получателя, а не в качестве ответа на полученные пакеты. Поэтому поле, содержащее адрес источника, является дополнительным для вызовов P2P IP-телефонии.

2. Информация в поле Next Header необходима для идентификации протокола верхнего уровня во всех приложениях, включая IP-телефонию. Однако в качестве протокола верхнего уровня в IP-телефонии всегда используется UDP со значением 17 в поле Next Header. Поэтому можно использовать уже известные значения этого поля.

2) Поля заголовка пакета UDP, который используется во многих приложениях на базе IP.

1. Информация об исходном порте не нужна приложениям IP-телефонии по тем же причинам, что и адрес источника.

2. Поле контрольной суммы также является необязательным, и оно может быть исключено.

3. Поле длины необходимо для определения длины сегмента уровня 4, включая заголовок UDP. Однако поле длины равно полю «Длина полезной нагрузки» в заголовке IPv6.

3) Заголовок пакета RT, который содержит информацию для различных типов мультимедийных приложений реального времени в сетях на базе IP.

1. Информация в поле «Источник синхронизации» помогает в устранении конфликта, когда начальное значение номера последовательности одинаково для двух источников. Но в случае P2P-вызовов существует один источник. Таким образом, поле SSRC является дополнительным и необязательным.

Соответственно, вышеперечисленные поля могут быть опущены. Суммарный размер этих полей составляет около 27 байт, они могут быть использованы для передачи голосовой информации. Авторы предлагают алгоритм для этого преобразования. Это приводит к уменьшению или обнулению полезной нагрузки пакета, тем самым повышается эффективность использования полосы пропускания. Авторы приводят анализ производительности данного методом: SmlZr сокращает полосу пропускания на 25% по сравнению с протоколом RTP. Экономия полосы пропускания полезна для звонков P2P IP-телефонии, так как снижает нагрузку на трафик. Таким образом, улучшение пропускной способности звонка повышает его четкость.

Также одним из способов улучшения пропускной способности сети является робастное сжатие заголовков пакетов (RoHC). RoHC сжимает 40–60 байт накладных расходов в 1–3 байта, размещая компрессор перед каналом с ограниченной пропускной способностью, а декомпрессор – после него. Компрессор преобразует большие накладные расходы всего в несколько байт, а декомпрессор делает обратное [40].

Протокол RoHC использует преимущества избыточности информации в заголовках одного сетевого пакета (например, длина полезной нагрузки в заголовках IP и UDP) и нескольких сетевых пакетов, принадлежащих одному потоку (например, IP-адреса). Избыточная информация передается только в первых пакетах. Следующие пакеты содержат переменную информацию, например идентификаторы или порядковые номера. Эти поля передаются в сжатом виде, чтобы сэкономить больше битов.

Для повышения производительности перед сжатием пакеты классифицируются на потоки. После того как поток пакетов классифицирован, он сжимается в соответствии с профилем сжатия, который подходит лучше всего. Профиль сжатия определяет способ сжатия различных полей в сетевых заголовках.

RoHC может работать в трех режимах:

1) Однонаправленный (U-режим). В режиме U пакеты отправляются только в одном направлении: от компрессора к декомпрессору. Поэтому этот режим делает RoHC пригодным для использования на линиях, где обратный путь от декомпрессора декомпрессора к компрессор недоступен или нежелателен;

2) Двунаправленный оптимистичный (O-режим). Режим O используется для передачи запросов на восстановление ошибок и подтверждения значимых обновления контекста от декомпрессора к компрессору. Режим O направлен на максимизацию эффективности сжатия и редкое использование канал обратной связи;

3) Двунаправленный надежный (R-режим). Для режима R характерны более интенсивное использование канала обратной связи и более строгая логика на компрессоре и декомпрессоре, которая предотвращает потерю контекстной синхронизации между компрессором и декомпрессором, за исключением очень высоких остаточных битовых ошибок.

В работе [16] предложена модель для исследования производительности робастного сжатия заголовка (RoHC) при работе IP-телефонии на каналах 802.11. В расчетной модели был выбран U-режим RoHC. Кроме того, был предложен новый элемент под названием RoHCGain для измерения дополнительной полосы пропускания, которую могут использовать другие потоки из-за использования RoHC с трафиком IP-телефонии. Результаты исследований авторов показали, что RoHC применим только в тех случаях, когда каналы 802.11 перегружены или передают жадные потоки.

Независимо от конкретной реализации, методы сжатия заголовков имеют определенные недостатки:

1. Методы сжатия заголовков плохо работают при высокой потере пакетов или длительном времени обхода;

2. Сжатие заголовков содержит множество сложных операций на устройствах сжатия и распаковки. Эти операции перегружают устройства сжатия/декомпрессии и расходуют их ресурсы;

3. Выполнение операций сжатия/декомпрессии в пакете создает новый источник задержки для приложений IP-телефонии.

Обобщая, можно констатировать, что подходы мультиплексирования пакетов и сжатия больших заголовков обеспечивают улучшенное использование полосы пропускания для решений IP-телефонии. Однако они создают множество проблем и не подходят для многих сценариев и окружения.

3.4. Сквозное шифрование в WebRTC

3.4.1. Протокол WebRTC

За последние несколько лет произошло резкое развитие технологии голосовой связи со значительным переходом к передаче голоса по Интернет-протоколу. Актуальность защищенной передачи информации в сетях IP-

телефонии возрастает по мере развития IP-телефонии. Для обеспечения безопасности IP-телефонии разработан ряд методов, усовершенствованы протоколы [23, 75]. Рассмотрим развитие протокола WebRTC.

Протокол WebRTC (от англ. Web Real-Time Communication) появился в 2011 году как альтернатива SIP. WebRTC – это стандарт, который описывает передачу потоковых аудиоданных, видеоданных и контента между браузерами или другими поддерживающими его приложениями в режиме реального времени (см. рисунок 3.3). Технология WebRTC делает возможной видеосвязь через окно браузера, так что для присоединения к звонку необходимо только перейти по ссылке на соответствующую веб-страницу. Раньше веб-сайты и приложения, которые использовали связь в реальном времени – аудио, видео и обмен данными – часто требовали подключаемых модулей. WebRTC положил этому конец, позволив приложениям запускать RTC с помощью JavaScript API. Сначала поддержка была смешанной, поскольку технологические гиганты представили конкурирующие решения, но в 2021 году WebRTC стал официальным стандартом и сегодня используется всеми основными браузерами и 95% веб-пользователей.

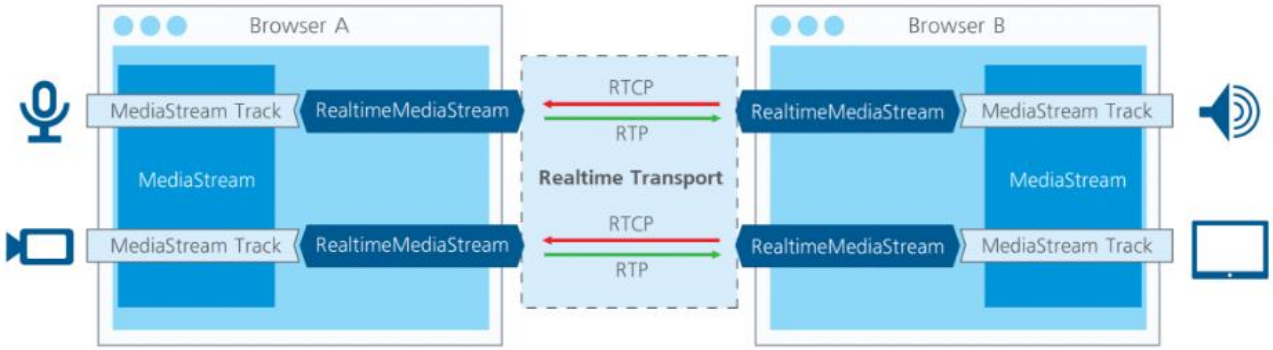


Рисунок 3.3. Архитектура WebRTC

В настоящее время WebRTC стремительно развивается. В последние годы бурное развитие и энтузиазм интернет-видеоприложений, таких как прямая трансляция, онлайн-классы и дистанционное управление, стимулировали развитие интернет-технологий аудио- и видеосвязи в реальном времени, требующих WebRTC. Разработаны и внедрены единые, открытые и прозрачные стандарты.

За последний год использование WebRTC в Chrome выросло в сотни раз в результате увеличения количества видеозвонков из браузера [107]. Во время пандемии видеозвонки стали неотъемлемой частью жизни многих людей, поэтому разработчики браузеров начали оптимизировать технологию. И это было особенно важно, потому что по мере перехода сотрудников и студентов на удаленную работу и учебу все чаще стали встречаться ресурсоемкие звонки с большим количеством участников и видеоэффекты в видеовстречах.

3.4.2. Проблема безопасности в WebRTC

По мере того, как виртуальные встречи становятся все более популярными, пользователи начали заботиться о безопасности используемых приложений.

WebRTC считается очень безопасным, но по мере развития функций важно, чтобы безопасность также усовершенствовала свое качество. Одним из последних достижений является поддержка E2EE на медиасерверах, которая обеспечивает сквозное шифрование (E2E) в групповом видеовызове. Это стало возможным благодаря внедрению так называемых вставляемых потоков (англ. Insertable Streams) в WebRTC [54].

Изначально система безопасности в WebRTC разрабатывалась для соединения точка–точка, одного транзитного участка, а не для нескольких «прыжков» между точками. В настоящее время большинство звонков работает через так называемый мост SFU [40], который позволяет совершать групповые звонки для 10–20 пользователей. Однако мост SFU – это такой же одноранговый узел, как и любой другой пользователь. Все участники конференции обмениваются медиаданными друг с другом через него и, соответственно, здесь уже нужны 2 «прыжка».

Преобладающей архитектурой для видеосвязи является так называемый Selective Forwarding Unit (SFU). SFU – это в основном маршрутизаторы пакетов, которые пересылают один или небольшой набор потоков от одного пользователя многим другим пользователям. В отличие от более традиционного блока управления многоточечной связью IP-телефонии (MCU), который декодирует и смешивает мультимедиа, SFU только маршрутизирует пакеты. Его мало заботит содержимое (кроме количества байтов в заголовке и того, является ли кадр ключевым кадром), так что теоретически SFU не нужно ничего декодировать и расшифровывать. Что касается шифрования, согласование DTLS-SRTP (протокол для шифрования RTP-нагрузки и проверки подлинности) происходит между каждой одноранговой конечной точкой и SFU. Это означает, что SFU имеет доступ к незашифрованной полезной нагрузке и может прослушивать ее. Это необходимо для таких функций, как запись на стороне сервера. С другой стороны, это означает, что нужно доверять объекту, выполняющему SFU, и/или клиентскому коду, чтобы сохранить этот поток закрытым. Модель безопасности с нулевым доверием (на англ. zero trust) всегда лучше для конфиденциальности.

3.4.3. Сквозное шифрование

Сквозное (E2E) шифрование в видеоконференциях – это способ защиты данных, который предотвращает доступ третьих лиц или серверов-посредников (SFU, TURN-серверы, шлюзы и т. д.) к ним или их изменение на каждом узле медиаконвейера. Один из простых способов представить истинное E2E-шифрование может быть реализован в том случае, если бы все видеоданные с момента их захвата камерой до момента их отображения на экране дважды зашифровывались. Контент сначала шифруется на уровне приложения, а второй раз – на сетевом уровне (см. рисунок 3.4). Поставщик видеоплатформы обычно заботится о сетевом уровне, но разработчик приложения отвечает за шифрование прикладного уровня.

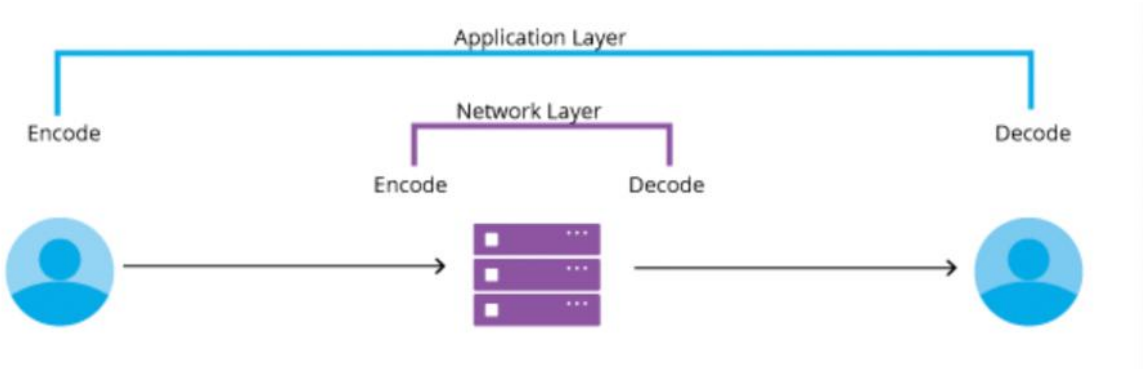


Рисунок 3.4. Шифрование и дешифрование

Для защиты данных между камерой и всеми промежуточными серверами разработчик приложения должен шифровать данные на прикладном уровне еще до того, как они будут отправлены на сервер, а также расшифровывать их в соответствующий момент перед отображением на экране зрителя. Это означает, что разработчики, использующие WebRTC SDK, должны принимать важные решения о том, как и где они будут защищать свои приложения.

Даже без защиты прикладного уровня шифрование WebRTC на сетевом уровне достаточно безопасно. Шифрование является обязательной частью архитектуры безопасности WebRTC и применяется ко всем аспектам установления и поддержания соединения.

Чтобы добиться сквозного шифрования, прикладной уровень также должен быть зашифрован. Это означает, что нужно сначала зашифровать сообщения, прежде чем отправлять их на сервер WebRTC. Это достигается разными способами в зависимости от типа отправляемого мультимедиа. Потоковое мультимедиа, такое как аудио, видео и трафик канала данных, необходимо шифровать перед его прохождением через медиасервер, а сообщения чата необходимо шифровать через шлюз.

Рассмотрим сквозное шифрование видео более подробно. Ключевой кадр в видеопотоке служит основой для последующих кадров. Ключевой кадр отправляется первым, а за ним следуют «дельта» кадры, которые содержат сжатую информацию об изменениях по сравнению с предыдущим кадром. Чтобы сделать это возможным, первые несколько байтов кадра должны оставаться незашифрованными. Точное количество байтов зависит от используемого кодека (VP8, VP9, H.264). Например, с VP8 нужно оставить 3–10 байт незашифрованными, потому что это байты, которые составляют заголовок кадра.

Способы шифрования сообщения до отправки на сервер WebRTC зависят не только от типа отправляемого мультимедиа, но и от того, используется ли собственный стек или веб-браузер. В то время как шифрование E2E в собственном стеке хорошо разработано и применялось в течение многих лет, шифрование E2E в браузере является совершенно новым и находится на ранних стадиях экспериментов.

Исторически сложилось так, что веб-браузеры не предоставляли разработчикам никаких средств для изменения аудио или видео перед их отправкой или воспроизведением, поэтому шифрование E2E в браузере было невозможно. За последние несколько лет было предложено несколько перспективных проектов, которые пытались создать стандарт для решения проблемы сквозного шифрования, в том числе конференцсвязь RTP с повышенной конфиденциальностью (PERC) [81], PERC Lite [37], маркировка кадров в Google Chrome. Однако ни один из предложенных методов не получил такой популярности или одобрения браузеров, которые необходимы для их использования в реальном мире. Поддержка этих проектов прекращена. Это оставило всех, кому нужно шифрование E2E в браузере, без вариантов. Но ситуацию меняет новая функция Chrome, называемая вставляемыми потоками (англ. Insertable Streams), которая была представлена 27 мая 2020 года.

3.4.4. Вставляемые потоки

Insertable Streams – функция, предоставляющая приложениям WebRTC доступ к аудио- и видеокадрам после того, как они были закодированы, но до того, как они были отправлены в сеть. WebRTC Insertable Streams позволяет делать E2EE в WebRTC через любое количество переходов [98].

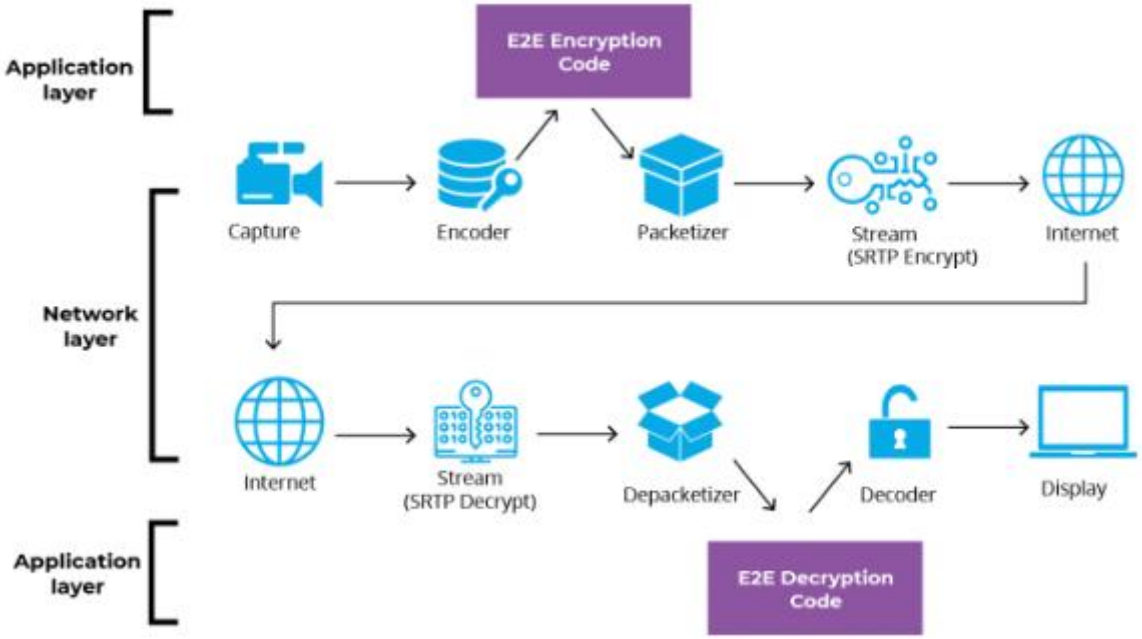


Рисунок 3.5. Уровни шифрования

По сути, сейчас это происходит аналогично E2EE в обмене сообщениями – расшифровать медиаданные можно только с помощью ключа, который обычно доступен только участникам звонка. Insertable Streams стремится решить проблему E2E-шифрования в браузере, позволяя пользователям предоставлять компоненты в RTCPeerConnection в виде набора потоков, а затем манипулировать и вводить новые компоненты, либо обертывать или заменять существующие ком-

поненты [14]. Это позволяет разработчику приложения перестраивать кадры, чтобы включить в заголовок небольшой фрагмент незашифрованной информации, необходимой для надежной отправки кадров по сети, обеспечивая при этом полное шифрование всех медиаданных. Это может быть сделано для каждого кодека и адаптировано для удовлетворения уникальных потребностей каждого медиа-сервера, а не жесткого отраслевого стандарта (см. рисунок 3.5).

Проект является экпериментальным, т.е. для его включения пользователям придется зайти в настройки Chrome и включить экспериментальные функции. Это может стать препятствием для входа на рынок для некоторых групп пользователей, но для компаний со строгими правилами и контролем в области ИТ сквозное шифрование в его нынешнем виде уже стало возможным.

3.4.5. Использование сквозного шифрования в Jitsi Meet

Многие приложения для видеоконференцсвязи уже поддерживают рассмотренное сквозное шифрование. Рассмотрим рекомендации по применению на примере Jitsi Meet – бесплатного программного обеспечения для проведения защищенных шифрованием видеоконференций [23, 35].

Чтобы сделать звонки со сквозным шифрованием в Jitsi Meet, нужно активировать опцию End-to-End Encryption в дополнительном меню (см. рисунок 3.6). Эта функция доступна для пользователей, чей браузер на базе Chromium 83 и выше (например, соответствующие версии Edge, Chrome, Opera и Brave).

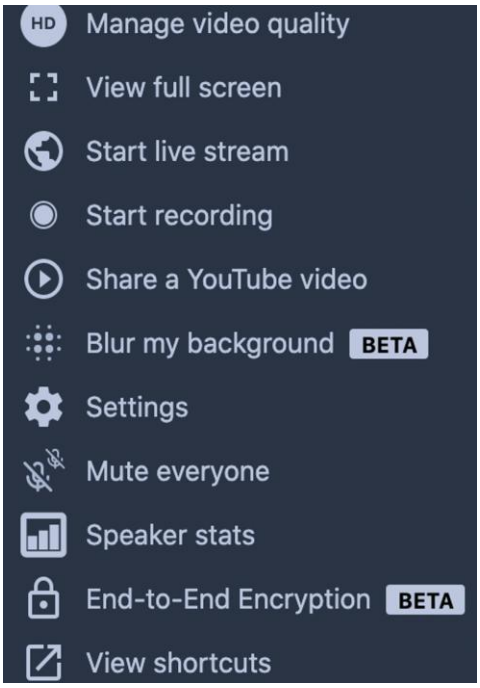


Рисунок 3.6. Дополнительное меню

Ввод ключа изображен на рисунке 3.7.

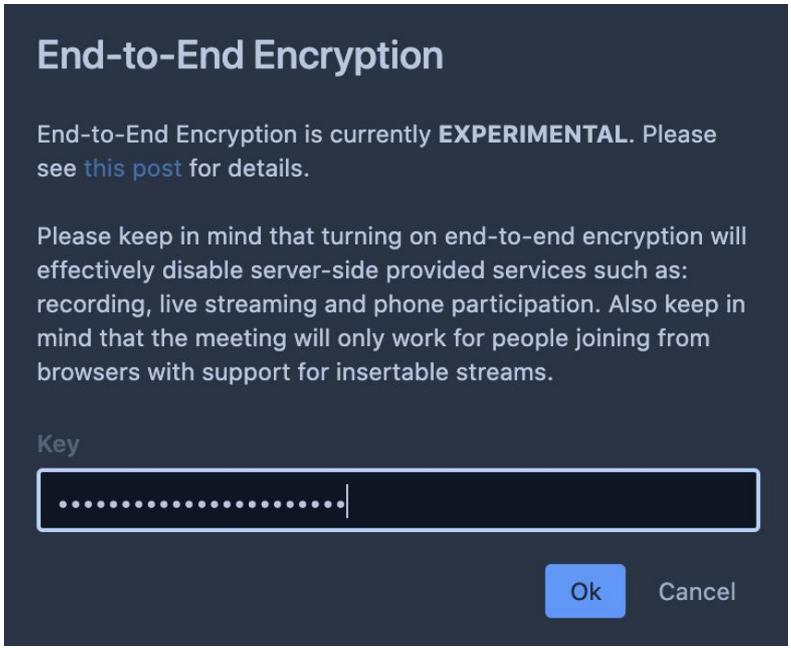


Рисунок 3.7. Ввод ключа

На видеовстрече Аня, Андрей и Михаил ведут сквозной зашифрованный разговор с использованием нового параметра e2eekey (см. рисунок 3.8). На первый взгляд, в видеозвонке нет ничего примечательного.

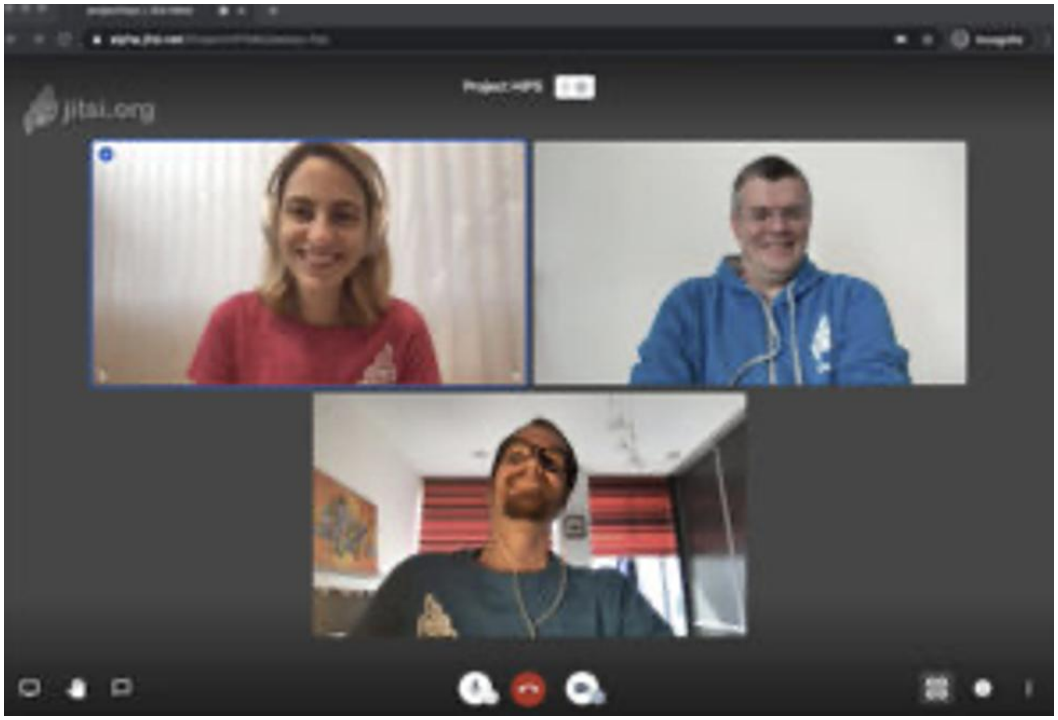


Рисунок 3.8. Видеочат с шифрованием

Все меняется, когда Денис решает присоединиться к звонку. Новый участник видит только нескончаемый поток шума (см. рисунок 3.9).

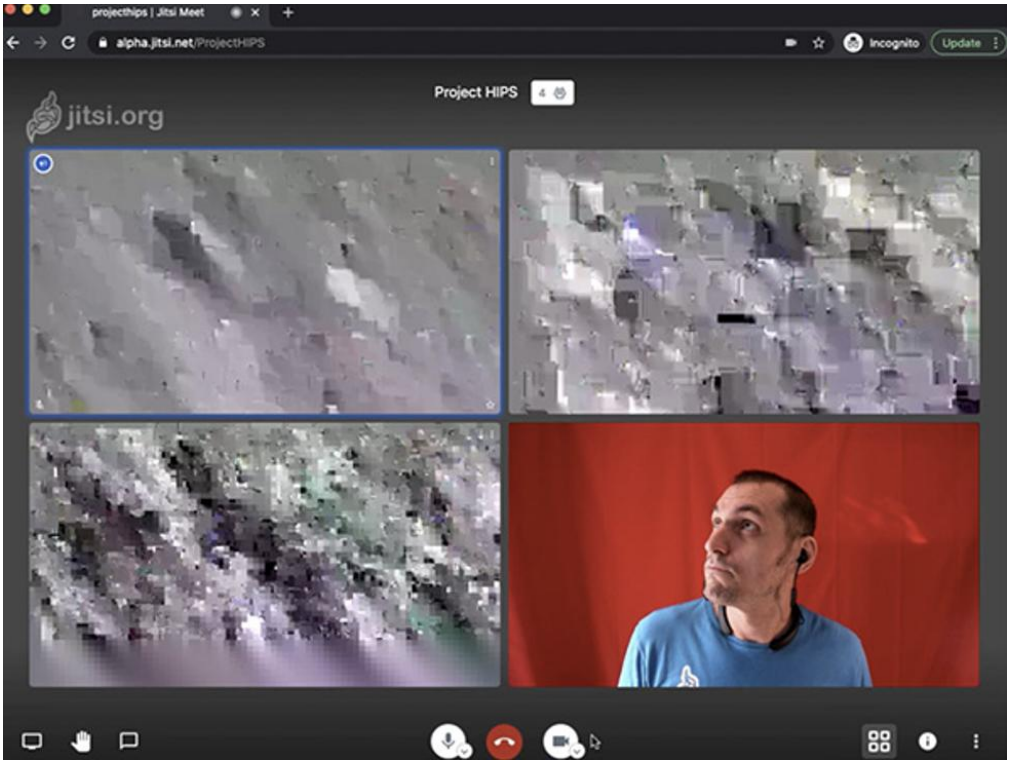


Рисунок 3.9. Шум в видеочате

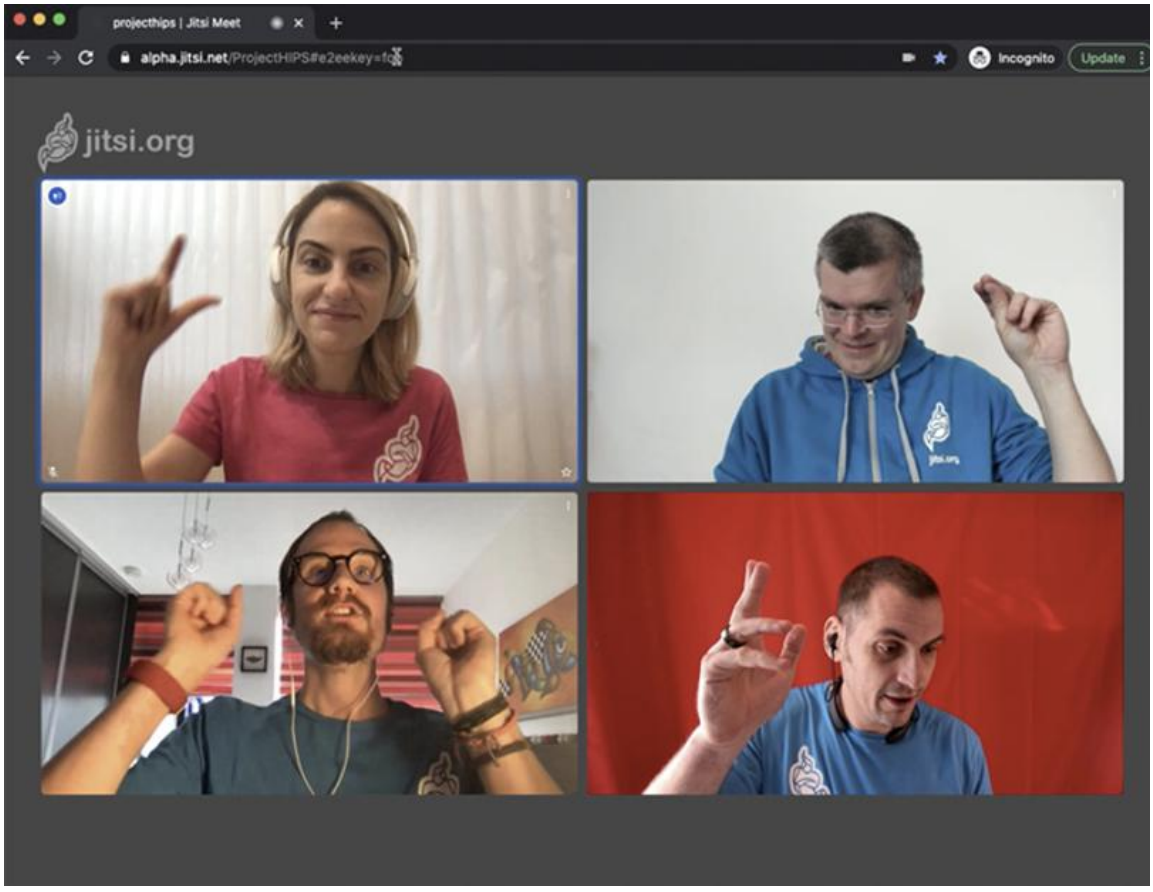


Рисунок 3.10. Использование ключа

Если бы Денис был мошенником, управляющим мостом для встречи, он больше не смог бы подслушивать ее, а попытка сделать это привела бы только к тому, что он наблюдал поток мусора. Единственный способ для Дениса принять участие в собрании – это получить доступ к ключу e2ee. В данном случае ключ был, и как только Денис использует его, он становится полноправным участником встречи (см. рисунок 3.10).

Jitsi Meet шифрует всю информацию, отправляемую по сети, с помощью DTLS-SRTP, чтобы никто не смог перехватить данные. Но DTLS-SRTP в WebRTC строго привязан к PeerConnection, что означает, что при использовании видеомаршрутизатора (например, Jitsi Videobridge) WebRTC и DTLS-SRTP могут предоставлять шифрование для соединения точка–точка, одного транзитного участка, а не для нескольких «прыжков» между точками.

В таких сценариях видеомаршрутизатор устанавливает столько зашифрованных каналов, сколько имеется участников. Это защищает все данные в сети. Однако для того, чтобы медиаданные от одного участника достигли другого, их необходимо извлечь из криптографического контекста отправителя и повторно зашифровать с помощью получателя [35].

Необходимость расшифровывать информацию во время ее передачи по Jitsi Videobridge технически предоставляет любому, кто управляет машиной JVB, возможность доступа к данным. Таким образом, они могут слышать и видеть всех присутствующих на собрании.

Благодаря технологии Insertable Streams в экосистеме Chromium, рассмотренной ранее, в Jitsi Meet очень просто можно добавить к видеоконференциям дополнительный уровень защиты e2e поверх существующего.

3.5. Системы с интерактивным голосовым меню (IVR-системы)

3.5.1. Основные сведения об IVR-системах

IP-телефония предлагает предприятиям новые способы использования широкого спектра коммуникационных функций, избегая при этом высокой стоимости стационарных телефонов. По мере того, как компании любого размера внедряют эту технологию, многие из них открывают для себя потенциал IP-телефонии в сочетании с искусственным интеллектом (ИИ). Фактически искусственный интеллект и IP-телефония оказываются ценными инструментами для оптимизации обслуживания клиентов [48].

Когда ИИ и IP-телефония объединяются для лучшего обслуживания клиентов и повышения эффективности, результатом становится повышение удовлетворенности клиентов, экономия средств и повышение вовлеченности сотрудников. ИИ позволяет телефонной системе IP-телефонии автоматически обрабатывать более рутинные вызовы, освобождая агентов для обработки более сложных случаев.

Даже когда для системы IP-телефонии с искусственным интеллектом становится очевидным, что вызов не может быть разрешен с помощью ее автомати-

зированных инструментов, система собирает важную информацию, которая лучше информирует агента о разговоре с клиентом.

В модели, сочетающей ИИ и IP-телефонию, проблемы решаются быстрее, а клиенты ценят возможность доступа к самостоятельным решениям. Это приводит к экономии средств, а также к повышению вовлеченности и лояльности клиентов.

Одним из ключевых преимуществ внедрения ИИ и IP-телефонии является повышение удовлетворенности сотрудников своей работой. Они удаляют более приземленные аспекты обслуживания клиентов, такие как ответы на рутинные вопросы и решение простых проблем, и вместо этого получают возможность решать более сложные ситуации. Эта более полезная позиция в сфере обслуживания клиентов может помочь предприятиям снизить текучесть кадров за счет повышения вовлеченности сотрудников.

ИИ уже позволил многим технологиям создавать более качественные продукты и с легкостью завоевывать больше клиентов. IP-телефония — это одна из технологий, на которую сильно повлияли технологии ИИ и интегрированные решения. Объединение ИИ и IP-телефонии может многое сделать. Одним из таких решений является IVR.

Интерактивное голосовое меню (англ. Interactive Voice Response, IVR) – это система телефонии, которая взаимодействует с вызывающими абонентами и выполняет функцию маршрутизации вызовов внутри колл-центра. IVR и ИИ объединяются новыми способами, которые позволяют компаниям получать лучшее из обоих миров: персонализированное самообслуживание для звонящих без огромных трудовых затрат, связанных с растущим штатом агентов-людей.

Система IVR используется для нескольких целей, таких как обработка телефонных звонков клиентов, предоставление сведений о транзакциях, прием запросов клиентов, предоставление информации о новых продуктах, перевод звонков агентам на основе запроса клиента и т. д.

Система IVR состоит из различных меню, подменю и опций в зависимости от приложения. Конечный пользователь выбирает подходящий вариант и проходит через систему IVR для завершения транзакции. Если конечный пользователь не может найти подходящий вариант или решение, тогда есть возможность перевести звонок на живого сотрудника, который действительно поможет клиенту, поговорив по телефону. Человек не взаимодействует с клиентом до тех пор, пока пользователь не переведет свой звонок на агента колл-центра (агента по работе с клиентами). Все меню, подменю, опции являются предварительно записанными сообщениями в системе IVR, и все эти сообщения воспроизводятся по запросу клиента. Эти предварительно записанные сообщения называются «подсказками» в системе IVR.

Например, для любого банковского приложения, если пользователь хочет узнать свой последний остаток на счете или последние 5 транзакций, IVR предоставляет эту информацию без разговора с клиентом. Клиенту нужно только

воспроизвести тональный набор с помощью клавиатуры, чтобы перейти к соответствующему пункту меню.

3.5.2. Технологии в IVR-системах

Рассмотрим базовые технологии, используемые в системе IVR [73].

1. Тональный набор или тональный сигнал (англ. Dual-Tone Multi-Frequency, DTMF) – это звуки или тональные сигналы, генерируемые телефоном при нажатии цифр. Эти тоны передаются по голосовому каналу. Технология DTMF работает за счет того, что трубка генерирует тоны на определенных частотах и воспроизводит их по телефонной линии при нажатии кнопки на клавиатуре. Оборудование на другом конце телефонной линии слушает определенные звуки и декодирует их в команды. Эти команды обычно используются для набора телефонного номера для вызова, но также могут использоваться для сигнализации команд управления телефоном или управления удаленным оборудованием, поскольку управляющие тоны воспроизводятся на том же канале, что и голосовой сигнал. Это внутриполосная сигнальная система.

DTMF определяет восемь различных тонов. Они делятся на высокую группу и низкую группу. Каждое нажатие клавиши соответствует двум тонам (отсюда и название двойного тона) – одному из высокой группы и одному из низкой группы. Это позволяет использовать 16 ключей. Эти клавиши обозначаются цифрами от 0 до 9, * (звездочка), # (решетка) и буквами от A до D. Буквенные клавиши обычно не используются и отсутствуют в подавляющем большинстве потребительских телефонов.

Для кодирования символа в DTMF сигнал необходимо сложить два синусоидальных сигнала. Частоты синусоид берутся по приведенной ниже таблице (см. рисунок 3.11) из столбца и строки, соответствующих передаваемому символу.

1	2	3	A	**697 Гц**
4	5	6	B	**770 Гц**
7	8	9	C	**852 Гц**
*	0	#	D	**941 Гц**
1209 Гц	**1336 Гц**	**1477 Гц**	**1633 Гц**	

Рисунок 3.11. Кодирование символов

2. Технология распознавания речи – еще один способ общения, при котором вызывающий абонент вводит данные в систему IVR, используя свой чистый голос, чтобы система могла правильно интерпретировать ввод и предоставлять точную информацию.

3. Блок аудиоответа (англ. Audio Response Unit, ARU) – это технология, которая позволяет компьютеру взаимодействовать с людьми с помощью голосовых и тональных сигналов DTMF, вводимых с клавиатуры. В телекоммуникациях ARU позволяет клиентам взаимодействовать с хост-системой компании через телефонную клавиатуру или с помощью распознавания речи, после чего они могут обслуживать свои собственные запросы, следуя диалогу ARU. Системы ARU могут отвечать предварительно записанным или динамически генерируемым звуком, чтобы дополнительно указать пользователям, как действовать дальше. Приложения ARU можно использовать для управления практически любой функцией, где интерфейс можно разбить на серию простых взаимодействий. Системы ARU, развернутые в сети, рассчитаны на обработку больших объемов вызовов.

4. Автоматический распределитель вызовов (англ. Automatic Call Distributor, ACD) – это технология, которая распределяет вызовы клиентов в порядке их поступления следующему доступному подходящему агенту. Эта телекоммуникационная технология запрограммирована на категоризацию вызовов на основе предварительно установленных параметров. Затем вызовы передаются соответствующему агенту для обработки запроса клиента. Он также может использовать DNIS (служба информации о набранных номерах) для предоставления агенту-клиенту информации при приеме вызова. Помимо основной функции маршрутизации вызовов, ACD может осуществлять мониторинг звонков с целью анализа удовлетворенности клиента и будущего обучения операторов; реализовывать обратные вызовы в случаях долгого ожидания вызывающего; отправлять клиентов на голосовую почту; интегрироваться с CRM, благодаря чему агенты получают всю необходимую им информацию о вызывающем абоненте.

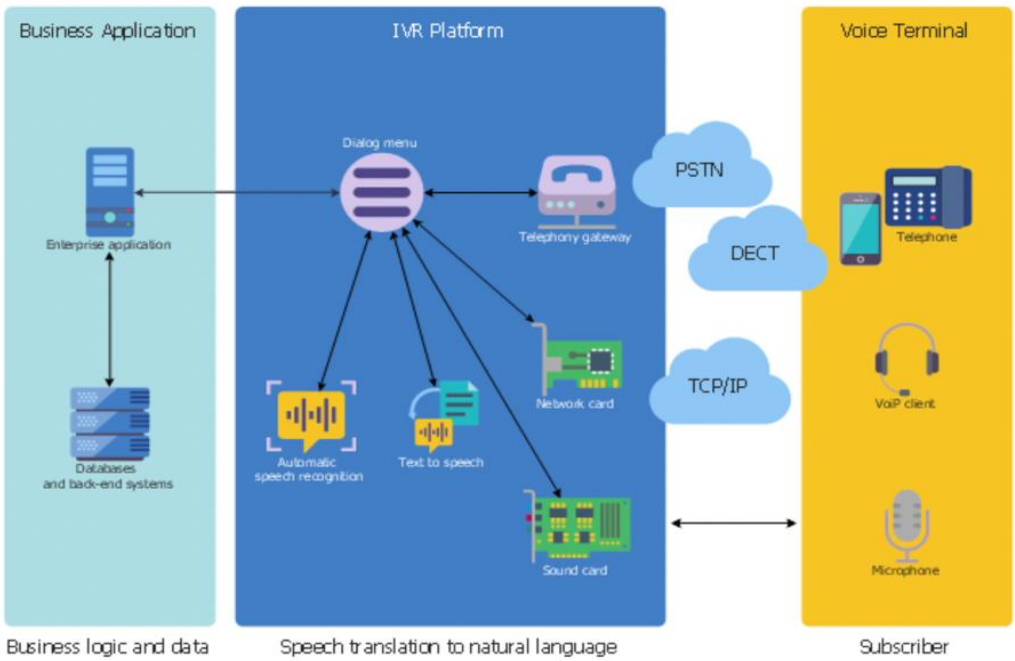


Рисунок 3.12. Архитектура IVR

5. Преобразование текста в речь (англ. Text To Speech, TTS) – возможность предоставления динамической информации клиентам путем автоматического преобразования текстовых данных в произнесенные слова. TTS – это компьютерный генератор речи, который произносит такую информацию, как новости, электронная почта и т.д.

Таким образом, архитектура IVR (рисунок 3.12) представляет собой комбинацию телефонного оборудования (например, телефонного кабеля, USB-телефонной платы и т.д.), программного приложения, базы данных, сети и вспомогательной инфраструктуры. Также иногда используется преобразователь текста в речь.

3.5.3. Развертывание IVR-систем

IVR можно развернуть несколькими способами [70]:

- Через оборудование, установленное на территории заказчика.
- Через оборудование, установленное в ТСОП (телефонная сеть общего пользования).
- Через поставщика услуг приложений (ASP)/размещенный IVR.

Компания или организация могут приобрести все аппаратное и программное обеспечение и использовать его самостоятельно или подписаться на услугу IVR-хостинга. Хостинг-сервис взимает ежемесячную плату за использование своих серверов и программного обеспечения IVR. Услуга хостинга помогает организации настроить систему IVR, которая наилучшим образом соответствует ее потребностям, и обеспечивает техническую поддержку, если что-то пойдет не так.

Традиционно приложения IVR создавались и развертывались на дорогих платформах, требующих сложной интеграции с серверной частью, больших капитальных затрат и высоких затрат на обслуживание. Благодаря надежному IP-соединению с Интернетом в настоящее время популярны хостинговые IVR за небольшую часть стоимости и обслуживания владения одним из них.

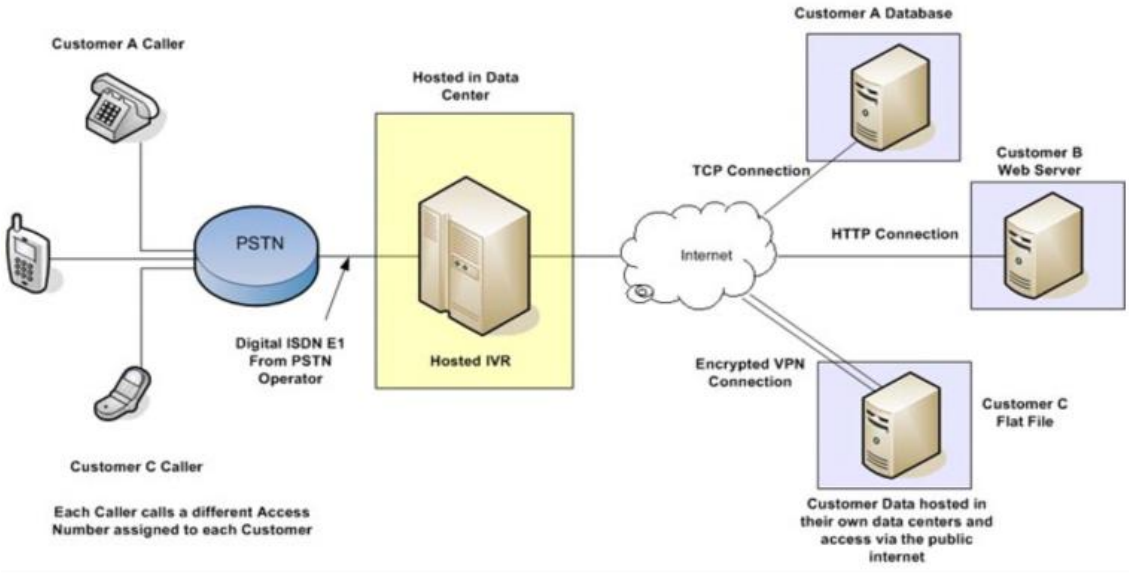


Рисунок 3.13. Получение данных

Вместо того, чтобы размещать IVR у заказчика, размещенный IVR располагается в надежном центре обработки данных с цифровыми телефонными линиями ISDN E1 (30 каналов) и выделенным доступом в Интернет. Линии ISDN позволяют клиентам совместно использовать телефонные каналы, чтобы пользоваться всеми функциями цифровых телефонных линий, не платя за это. Поскольку на каждой линии ISDN доступно до 1000 прямых номеров, на одной линии можно совместно использовать множество различных приложений для разных целей. С другой стороны, выделенный доступ в Интернет обеспечивает надежную связь с базами данных клиентов или веб-страницами, расположенными в любой точке мира.

Когда поступает звонок от клиента А (см. рисунок 3.13), IVR может получить запрос на получение данных из базы данных клиента А через Интернет. Как только необходимая информация извлечена, она воспроизводится вызывающему абоненту. Таким образом, информация может быть получена из любой базы данных или с любого веб-сервера через Интернет.

3.5.4. Компоненты системы IVR на основе VXML

Многие из современных наиболее совершенных систем IVR основаны на специальном языке программирования, называемом VoiceXML (Voice eXtensible Markup Language, VXML). Пример VoiceXML документа:

```
<vxml version="2.0" xmlns="http://www.w3.org/2001/vxml">
  <form>
    <block>
      <prompt>
        Привет, мир!
      </prompt>
    </block>
  </form>
</vxml>
```

VoiceXML интерпретатор преобразует текстовую фразу «Привет, мир!» в синтезированную речь.

Основные компоненты системы IVR на основе VXML:

1. Телефонная сеть. Входящие и исходящие телефонные звонки направляются через обычную телефонную сеть общего пользования (PSTN) или через сеть IP-телефонии.

2. Сеть TCP/IP. Стандартная интернет-сеть, подобная той, которая обеспечивает подключение к Интернету и внутренней сети в офисе.

3. Телефонный сервер VXML. Этот специальный сервер находится между телефонной сетью и сетью Интернет. Он служит интерпретатором или шлюзом, так что вызывающие абоненты могут взаимодействовать с программным обеспечением IVR и получать доступ к информации в базах данных. Сервер также содержит программное обеспечение, которое управляет такими функциями, как преобразование текста в речь, распознавание голоса и распознавание DTMF.

4. Веб-сервер/сервер приложений. Здесь располагаются программные приложения IVR. На одном сервере может быть несколько разных приложений: одно для обслуживания клиентов, одно для исходящих звонков по продажам, одно для преобразования голоса в текст. Все эти приложения написаны на VXML. Веб-сервер/сервер приложений подключен к серверу телефонии VXML по сети TCP/IP.

5. Базы данных. Базы данных содержат информацию в реальном времени, к которой могут обращаться приложения IVR. Если клиент позвонит в компанию, выпустившую его кредитную карту, и захочет узнать свой текущий баланс, приложение IVR извлечет общую сумму текущего баланса из базы данных. То же самое касается времени прибытия рейсов, времени просмотра фильмов и так далее. Одна или несколько баз данных могут быть связаны с веб-сервером/сервером приложений по сети TCP/IP.

3.5.5. Применение IVR-систем

В настоящее время системы IVR разработаны практически для всех отраслей и соответствующих приложений, таких как банковское дело, страхование, телекоммуникации, и их также можно использовать для информации о поездках, розничных заказах, коммунальных услугах и т. д. Система IVR предоставляет информацию всем пользователям или клиентам на основе их запросов. С помощью системы IVR можно снизить стоимость и улучшить качество обслуживания за счет удовлетворения запросов клиента без взаимодействия с реальным агентом. Если вызывающий абонент не может найти подходящее решение, то его вызов уже передается фактическому агенту.

В России обработку запросов с помощью роботов осуществляют аутсорсинговые контакт-центры операторов связи, банков и авиационных компаний. Реализация проекта по внедрению «виртуального сотрудника» в контакт-центр очень затратна, что делает это решение доступным только для крупных игроков рынка. Стоимость роботов по сравнению с оператором достигает соотношения 1/5. Однако в ряде запросов робот не сможет предоставить полную информацию, которую хочет получить клиент.

В США и Европе около 80% абонентов при подключении к колл-центру выбирают работу не с диспетчером, а с автоматическим IVR-сервисом, основная причина – сокращение времени обработки запросов за счет отсутствия ожидания ответа от живого оператора. В России ситуация в настоящее время развивается иначе, чем в Европе и США. Несмотря на то, что большинство звонков стандартные и решаются с помощью меню IVR, многие абоненты предпочитают услышать живого человека и решить свою проблему с помощью оператора.

В некоторых приложениях, таких как балансы банковских счетов, переводы и доступ к базам данных стратегических организаций и т.д., требуется высокий уровень безопасности. В таких приложениях предоставляемая информация защищена с помощью персонального идентификационного номера (ПИН). Однако этот подход не является безопасным и подвержен фальсификации и непра-

вильному использованию. Для преодоления этой проблемы предлагается подход к распознаванию образов, основанный на нейронной сети. Для аутентификации можно использовать определенные шаблоны пользователя, такие как отпечатки пальцев, сетчатка глаза, черты лица, идентификация последовательности ДНК, голос и т. д. Однако среди них голосовая аутентификация легкодоступна и наиболее подходит для системы интерактивного голосового меню. Верификации личности говорящего основывается на общем предположении, что на каком-то уровне изучения нет двух людей с абсолютно одинаковыми характеристиками голоса. К текущему моменту было совершенно немало попыток внедрения этой технологии, однако исследования в этой области все еще продолжаются.

3.5.6. Преимущества IVR-систем

Основными преимуществами использования IVR являются удобство удаленного доступа, высокий уровень доступности и экономичность [116]. Телефоны просты в использовании и знакомы представителям большинства демографических групп, что является преимуществом IVR по сравнению с некоторыми аналогичными интернет-подходами, которые также используются в настоящее время. Системы IVR доступны 24 часа в сутки, доступны нескольким людям одновременно, могут использовать разные языки для администрирования опросов и способны охватить широкие группы населения.

IVR легче получить, чем личные интервью, для групп населения с социально-экономическими проблемами, которые не имеют легкого доступа к компьютеру, испытывают трудности с незнакомыми компьютерными программами или живут слишком далеко.

Системы IVR также можно использовать для инициирования звонков, текстовых сообщений или даже электронных писем в качестве напоминаний для тех, кто не позвонил в определенное заранее установленное время.

IVR может направлять рутинные вызовы и общие вопросы, позволяя звонящим использовать самообслуживание IVR и освобождая агентов для обработки более сложных вызовов или вопросов по нескольким каналам. Это может значительно повысить эффективность и предоставить агентам более содержательную работу, а не повторяющиеся вопросы, такие как остатки на счетах, подтверждение времени встречи или сбор платежей. При использовании в исходящем режиме с преобразованием текста в речь (TTS) телефонный звонок IVR позволяет вам делать специальные предложения, отправлять напоминания и приветственные сообщения или совершать вызовы по сбору, не отвлекая агентов от других служб.

В отличие от традиционных телефонных интервью и письменных анкет, системы IVR способны собирать информацию и немедленно сохранять ее в компьютерной базе данных без необходимости привлечения сотрудника или исследователя даже для очень большого числа клиентов. Исследования показали, что IVR-интервью так же эффективны, как и личные письменные анкеты, живые телефонные интервью и интернет-подходы.

3.5.7. Недостатки IVR-систем

К недостаткам IVR относятся время для старта и финансовые обязательства, необходимые для написания сценариев, разработки записей и приобретения необходимого оборудования и программного обеспечения для запуска системы IVR, а также для обслуживания оборудования и резервного копирования данных с течением времени. Однако первоначальные затраты на программирование и приобретение оборудования являются фиксированными [10] и могут быть распределены между неограниченным числом участников. В качестве альтернативы можно заключить контракт на установку и обслуживание IVR с одной из нескольких компаний, предлагающих эту услугу, но этот вариант также требует значительных финансовых вложений. Хотя стоимость размещения IVR не является фиксированной, дополнительные затраты на добавление новых участников довольно малы. Какой бы вариант ни использовался, необходимо принять меры для предотвращения потери данных (например, из-за простоя компьютера, отключения электроэнергии, прерывания телефонной связи и т. д.). Также крайне важно, чтобы сохраненные данные IVR хранились так же надежно, как и любые другие записи клиентов.

Еще одним существенным недостатком IVR является то, что некоторые участники с низким социально-экономическим статусом или проживающие в отдаленных регионах могут не иметь постоянного доступа к телефонной связи. Имеются данные о том, что использование сотовых телефонов достаточно распространено даже в развивающихся странах, чтобы поддерживать вмешательства по телефону в качестве жизнеспособных моделей, но испытуемые, участвующие в исследованиях IVR с использованием сотовых телефонов, подвергаются риску плохого приема и сброшенных вызовов. В большинстве исследований эти проблемы решаются за счет использования бесплатных телефонных номеров, которые участники могут использовать для бесплатного доступа к системе IVR, и предоставления компьютерам IVR возможности приостанавливать сеанс при отключении вызова, продолжая сеанс в том же месте, когда участник снова подключается.

3.5.8. Рекомендации по применению IVR

Систематизируем рекомендации по эффективному применению IVR.

1. Необходимо сделать IVR интуитивно понятным. Решения интерактивного голосового меню должны предоставить клиентам более простой способ быстро получить то, что они хотят. Но этого можно достичь только в том случае, если будет разработан уникальный IVR с учетом потребностей клиентов. Для этого необходимо сделать меню телефона и логику маршрутизации более интуитивно понятными, сократив пункты меню до пяти или меньше. Кроме того, не думайте, что можно получить эффективный дизайн с первой попытки. Вместо этого лучше запланировать проведение A/B-тестов, чтобы скорректировать обмен сообщениями и подсказками и повысить удовлетворенность клиентов.

2. Системы IVR должны быть более персонализированными. Рекомендовано использовать IVR, чтобы укрепить связи с клиентами: если это известный звонящий, можно поприветствовать его по имени; если клиенты говорят на другом языке, можно ответить им соответствующим образом; если клиенты живут в определенном городе, можно дать им местный номер телефона. Нужно убедиться, что коммуникационное решение может взаимодействовать с программным обеспечением в режиме реального времени, чтобы можно было создать собственное меню для каждого пользователя и сделать его таким же естественным, как общение с человеком.

3. Клиентам должен всегда иметь возможность обратиться к реальному человеку. Некоторые абоненты могут предпочесть немедленно соединиться с человеком, поэтому обязательно нужно включить эту опцию. Хотя у автоматизации есть много преимуществ, для звонящего нет ничего более неприятного, чем желание связаться с реальным человеком и отсутствие подсказки для этого. Кроме того, нужно подключить данные звонящего к CRM-системе, чтобы агент мог получить к ним доступ в режиме реального времени. По исследованиям Accenture (консалтинговая компания, оказывающая услуги организациям по консультированию в сферах стратегического планирования, оптимизации и организации аутсорсинга бизнес-процессов, управления взаимоотношениями с клиентами, управления логистическими процессами, управления персоналом, внедрения информационных технологий), почти 90% клиентов разочаровываются, когда их переводят к живому агенту, потому что не смогли решить проблемы автоматизировано. Чтобы обеспечить положительный опыт работы с клиентами, программное обеспечение для распознавания речи должно быть достаточно умным, чтобы переадресовывать вызов, а агент должен иметь полную информацию о запросе клиента.

4. Использование преимуществ связи между брендом и клиентом. Использование решения Interactive Voice Response – это идеальная возможность добавить индивидуальность бренда в разговор. Системы IVR позволяют умным маркетологам представить свой бизнес и обеспечить обмен сообщениями и тоном, которые лучше всего представляют их бренд. Использование технологии IVR дает возможность произвести мгновенное и неизгладимое впечатление. Многие решения IVR позволяют создавать и настраивать сообщения так же часто, как рекламу, электронную почту и сообщения в социальных сетях. Необходимо создать все возможности, которые позволяют динамически отслеживать, измерять и улучшать качество обслуживания клиентов, как в любой маркетинговой программе.

5. Внедрение многоканальности. Независимо от того, разговаривает ли клиент с IVR, взаимодействует в веб-чате, публикует сообщения в социальных сетях или отправляет электронное письмо, коммуникационные платформы должны автоматически управлять многоканальным общением с клиентами, потому что клиенты ожидают, что компании будут знать все их сообщения. Необ-

ходимо, чтобы IVR было интегрировано во все каналы поддержки, такие как SMS, чат и видео, для действительно беспрепятственного общения.

6. Обеспечение легкой масштабируемости. Полная интеграция – это ключ к созданию отличного интерфейса IVR. Но, поскольку коммуникационные платформы часто бывают сложными, многие организации не могут внести необходимые изменения, используя собственные ресурсы. Обращаясь к коммуникационным API, корпоративные компании используют облачные технологии для быстрого вывода своих коммуникационных приложений на рынок без тяжелой работы в сфере телекоммуникаций, как это было раньше. Необходимо найти тот облачный сервис, у которого есть высоконадежное, высококачественное соединение, поддерживаемое глобальной сетью операторов связи. Нужен API, который легко развертывать, поддерживать и масштабировать – можно вовлечь разработчиков заранее и попросить их протестировать его в работе перед покупкой.

3.6. Анализ существующих приложений

3.6.1. Основные приложения для голосовой связи в реальном времени

В настоящее время приложений для связи в реальном времени с помощью голоса и видео являются основополагающими для досуга и бизнеса, помогая людям поддерживать связь с друзьями и родственниками и обеспечивать удаленную работу. Важность таких приложений стала особенно очевидной во время пандемии COVID-19, когда социальное дистанцирование и меры изоляции заставили миллиарды людей общаться исключительно с помощью онлайн приложений.

До сих пор не существует стандарта для взаимодействия между различными приложениями, и даже если они используют известные протоколы, то их сочетание в каждом приложении различно. Более того, подавляющее большинство приложений имеет закрытый исходный код и предоставляет очень мало документации. Это усложняет управление сетью для интернет-провайдеров (ISP) и администраторов корпоративных сетей.

Наиболее распространенными протоколами, которые используются в приложениях, являются:

- RTP для потоковой передачи мультимедиа;
- RTCP используется рядом с RTP для передачи потоковой статистикой, например, коэффициента потери пакетов;
- SRTP – вариант RTP, который обеспечивает конфиденциальность информации путем шифрования полезной нагрузки мультимедиа;
- UDP/TCP в качестве транспортных протоколов;
- STUN для обеспечения связи для обнаружения NAT;
- TURN для ретрансляции трафика через сервер, который находится в публичном Интернете;
- RFC для мультиплексирования пакетов RTP, STUN и др. в одном потоке UDP;

– SDP для согласования сетевых и мультимедийных характеристик сессии (например, аудио- и видеокодеки);
– TLS и DTLS для обеспечения конфиденциальности управляющих данных (логин, пароль, местоположение и др.).

Также стоит упомянуть WebRTC. Для создания рабочего приложения RTC необходимо согласовывать все вышеперечисленные протоколы. WebRTC [39] представляет собой набор высокоуровневых и стандартных API, которые могут быть использованы в браузерах и мобильных приложениях для видео- и аудиосвязи. В настоящее время большинство браузеров поддерживают WebRTC, и он является единственным способом для работы приложений RTC через Интернет, помимо специфических плагинов для приложений. WebRTC предоставляет программные интерфейсы для установления медиа-сессий, координируя использование SRTP, RTCP, STUN, TURN и DTLS.

В данном разделе будет рассмотрены потребительские приложения, такие как Skype, Whatsapp, Telegram, а также приложения, которые используются в основном для бизнеса – Google Meet, Zoom, Jitsi Meet, Microsoft Teams, Webex Teams. Некоторые из приложений, такие как Whatsapp и Skype, предлагают несколько версий, и будет рассмотрено только одно из них, самое популярное.

3.6.2. Анализ функциональности приложений

Большинство приложений имеют схожую функциональность, за несколькими исключениями. Итоги сравнения представлены в таблице 3.3.

Таблица 3.3 – Функциональность приложений

Приложение	Групповые звонки	Приложение для ПК	Мобильное приложение	Работа в браузере	Демонстрация экрана
Whatsapp	+	+	+	-	-
Telegram	-	+	+	-	-
Skype	+	+	+	+	+
Google Meet	+	-	+	+	+
Zoom	+	+	+	+	+
Jitsi Meet	+	+	+	+	+
Microsoft Teams	+	+	+	+	+
Webex Teams	+	+	+	+	+

Таблица 3.3. показывает, что все приложения, кроме Telegram, позволяют осуществлять групповые звонки. Большинство приложений имеют приложение для ПК. Google Meet на ПК можно использовать только через браузер. Все приложения имеют мобильную версию приложения, и все, за исключением Whatsapp и Telegram, могут использоваться непосредственно через браузеры, поддерживающие WebRTC. Демонстрация экрана доступна также во всех приложениях, кроме Whatsapp и Telegram.

3.6.3. Анализ используемых протоколов

Далее сравним протоколы, которые приложения используют. Для этого возьмем за основу работу [35], где авторы собрали трассировки для приложений IP-телефонии. Эксперименты проводились для приложений для ПК, установленные на тестовых машинах Windows, для мобильных приложений на iPhone и Android, а также для приложений в браузере Google Chrome, который поддерживает WebRTC. Эксперименты включали в себя аудио и видео, также функцию демонстрации экрана, когда эта функциональность доступна в приложении. Экспериментальный звонок длится не менее 5 минут, в общей сумме было сделано не менее 5 звонков. Используя собранные трассировки, авторы определили используемые протоколы, применяя Tstat, который предоставляет записи для всех наблюдаемых TCP и UDP потоков, а также показывает общую статистику для каждого потока RTP, такую как количество пакетов, битрейт и т.д. Результаты исследования в виде обнаруженных протоколов представлены в таблице 3.4.

Таблица 3.4 – Используемые приложениями протоколы

Приложение	Протоколы				
	UDP или TCP	RTP	STUN/ TURN	TLS/ DTLS	Другие
Whatsapp	UDP	+	+	-	-
Telegram	UDP	-	+	-	+
Skype	UDP	+	+	-	+
Google Meet	UDP	+	+	+	-
Zoom	UDP	+	+	-	-
Jitsi Meet	UDP	+	+	+	-
Microsoft Teams	UDP	+	+	-	+
Webex Teams	UDP	+	+	-	+

Как видно из таблицы 3.4, во всех случаях приложения используют UDP в качестве транспортного протокола. Также авторы [35] анализируют полезную нагрузку. В браузерной версии один медиапоток UDP может нести различные протоколы, мультиплексированные вместе. Это происходит с использованием WebRTC, где RTP, RTCP, STUN и DTLS передаются через один и тот же поток UDP.

Далее будут рассмотрены версии для ПК и мобильные версии приложений, поскольку браузерные версии используют только стандартные API WebRTC, о чем было сказано выше.

Протокол RTP используется во всех приложениях, кроме Telegram, приложения шифруют полезную нагрузку с помощью SRTP. Приложения, использующие STUN, используют TURN для связи в случае, если прямое соединение невозможно, STUN и TURN являются взаимодополняющими протоколами. Google Meet и Jitsi Meet используют DTLS, чередующиеся среди RTP-пакетов.

Рассмотрим особенности некоторых приложений, упомянутых в исследовании [35].

Skype использует модифицированную версию TURN под названием Multiplexed TURN, который представляет собой такой же простой механизм инкапсуляции, как и TURN, где обычный заголовок RTP следует после нескольких байтов. Его можно легко определить, посмотрев на первые два байта, всегда принимающие значение 0xFF10.

Telegram не использует ни одного известного протокола в рамках UDP потока передачи медиаданных, только STUN и TURN для установки сеанса. В официальной документации Telegram говорится о том, что данные шифруются и отправляются по сети через собственный протокол MTProto.

Zoom. В Zoom заголовок RTP в полезной нагрузке UDP отсутствует, а пользовательский механизм инкапсуляции занимает 4 байта. На основе размеров пакета и времени авторы [35] приходят к выводу, что в видеопотоках байты инкапсуляции принимают значение 0x05100100, а в аудиопотоках – 0x050f0100. Веб-клиент использует стандартные API WebRTC, хотя и очень своеобразно. Медиапоток WebRTC не открывается, а только создает канал данных (WebRTC Data Channel), через который передается медиа [54].

3.6.4. Анализ трафика приложений

Рассмотрим работу приложений с точки зрения потоковой передачи мультимедийного контента, а также особенности использования протоколов, прежде всего RTP.

1) Peer-to-peer. Когда звонок включает только двух участников, приложение пытается заставить их общаться напрямую, чтобы избежать передачи трафика через сервер. Это имеет следующие преимущества:

- Снижение задержки связи. Пакеты проходят меньшее расстояние, поэтому пакеты приходят с меньшей задержкой;
- Снижение нагрузки на сервер. Серверам приложений не нужно брать на себя работу по пересылке трафика.

Однако такое соединение не всегда возможно, поскольку NAT, брандмауэры и промежуточные серверы могут препятствовать внутренним клиентам получать входящий трафик. Более того, этот метод работает только при двусторонних вызовах, поскольку для групповых вызовов это привело бы к тому, что трафик должен передаваться между всеми парами участников.

2) Избыточные потоки. Чтобы справиться с ненадежностью сети, в некоторых приложениях оборудование участников отправляет избыточные данные, которые могут быть использованы приемником в случае потери пакетов или ошибок. Такой подход называется Forward Error Correction (FEC) и обычно достигается за счет использования простых математических алгоритмов – например, отправки битов четности для защищенных пакетов. Некоторые кодеки разработаны для поддержки FEC нативно, и текущий пакет встраивает избыточные данные предыдущего пакета. Этот механизм называется внутриполосным FEC и реализован, например, в аудиокодеке Opus [98]. В других случаях отправитель передает данные FEC по отдельному каналу, в результате чего получается дополнительный независимый поток RTP. Это называется внеполосным FEC, и он используется для достижения стабильной коррекции ошибок и гибкости. Второе использование избыточных потоков – это так называемая техника Simulcast. При использовании Simulcast клиент кодирует видео в различных разрешениях (и битрейтах) и посылает их в виде отдельных потоков на устройство селективной переадресации. который решает, кто и какие потоки получает. Это полезно в том случае, если некоторые участники имеют плохие сетевые условия и могут получать только видео с низкой пропускной способностью.

Основываясь на данных [35], сравним работу приложений с точки зрения потоков трафика. Результат представлен в Таблице 3.5.

Таблица 3.5. Категории графика приложений

Приложение	Peer-to-peer	FEC	Simulcast	Другие
Whatsapp	+	+	-	-
Telegram	+	-	-	-
Skype	+	+	+	-
Google Meet	-	-	+	+
Zoom	+	+	-	-
Jitsi Meet	+	-	-	-
Microsoft Teams	+	+	+	-
Webex Teams	-	+	+	+

Авторы работы проводят эксперименты с использованием одноранговой связи, осуществляя звонки с двумя участниками, использующими устройства в одной локальной сети, где всегда возможна прямая связь. Все приложения используют данный вид связи, за исключением Google Meet и Webex Teams.

Для получения избыточности потоков авторы [35] проводят эксперименты, где клиент отправляет большее количество RTP-потоков, чем ожидалось. Приложения Whatsapp, Skype, Zoom, Microsoft Teams и Webex Teams используют внеполосный FEC. Skype и Microsoft Teams используют видео FEC с кодеком H.264, отправляя данные с разными PT в одном и том же потоке RTP. Webex Teams отправляет аудио и видео FEC в отдельных потоках RTP, в которых поле RTP Timestamp всегда имеет значение 0. Это можно подтвердить данными из журналов приложений, хранящихся на пользовательском оборудовании для каждого звонка. Аналогично, WhatsApp отправляет два параллельных RTP потоков, содержащих видео, оба с низким битрейтом 20–40 кбит/с. Zoom посылает избыточные аудиоданные, используя механизм, определенный в RFC 2198 [9]. Видеопоток несет небольшую, но постоянную долю пакетов, что позволяет предположить использование аналогичного механизма.

Приложения Skype, Google Meet, Microsoft Teams и Webex Teams использует Simulcast, а при использовании мобильного приложения клиент отправляет видеотрафик на трех различных битрейтах, что приводит к трем отдельным потокам RTP, которые отправляются на сервер ретрансляции. Затем каждый участник получает только один уровень качества в соответствии с выбором сервера. Webex Teams также отправляет несколько потоков с разным качеством для учета свернутых видео участников, которые не говорят в данный момент. Microsoft Teams и Skype отправляют пользовательские видео с тремя качествами одновременно.

Авторы также отмечают, что приложения Webex Teams, Google Meet, Microsoft Teams и Skype используют дополнительный заголовок RTP – Contributing source (CSRC). В Webex Teams CSRC однозначно идентифицирует участника вызова и, как таковой, может быть использован для изоляции потоков определенного пользователя на сетевом уровне. Google Meet использует выделенные потоки RTP для повторной передачи потерянных данных.

3.6.5. Анализ рейтинга и системных требований приложений

Проанализируем пользовательский рейтинг приложений [10, 62, 63]. Данные взяты из сервисов приложений для Android (Google Play Store) и для iOS (App Store). Результаты приведены в таблицах 3.6 и 3.7, где буквой М обозначается миллион единиц, буквой К – тысяча единиц.

Приложения Whatsapp, Telegram и Skype имеет самое большое количество скачиваний и оценок среди пользователей, что можно объяснить тем, что это пользовательские приложения, у них более широкая аудитория. Среди бизнес-приложений наиболее популярными являются Microsoft Teams и Zoom, а также Webex Teams на платформе Android. Можно заметить, что чем раньше прило-

жение было выпущено и чем меньше требуемая версия устройства, тем больше оценок и скачиваний оно имеет [62, 63].

Таблица 3.6. Данные о приложениях из Google Play Store

Приложение	Количество скачиваний	Рейтинг	Количество оценок	Требования к минимальной версии Android OS	Год выпуска
Whatsapp	1000M	4.2	157M	4.1	2010
Telegram	1000M	4.4	10M	6.0	2013
Skype	1000M	4.1	11M	6.0	2010
Google Meet	100M	3.2	2M	6.0	2017
Zoom	500M	2.4	3M	5.0	2013
Jitsi Meet	10M	3.0	49K	6.0	2016
Microsoft Teams	100M	4.3	5M	5.0	2016
Webex Teams	50M	4.3	1.8M	6.0	2011

Таблица 3.7. Данные о приложениях из App Store

Приложение	Рейтинг	Количество оценок	Требования к минимальной версии iOS
Whatsapp	4.7	9.8M	10.0
Telegram	4.3	138.6K	9.0
Skype	4.5	61.1K	11.0
Google Meet	4.7	179.9K	12.0
Zoom	4.6	2.2M	12.0
Jitsi Meet	3.7	397	12.0
Microsoft Teams	4.8	2.1M	14.0
Webex Teams	3.8	970	14.8

Рисунок 3.14. Рейтинг приложений в Google Play Store

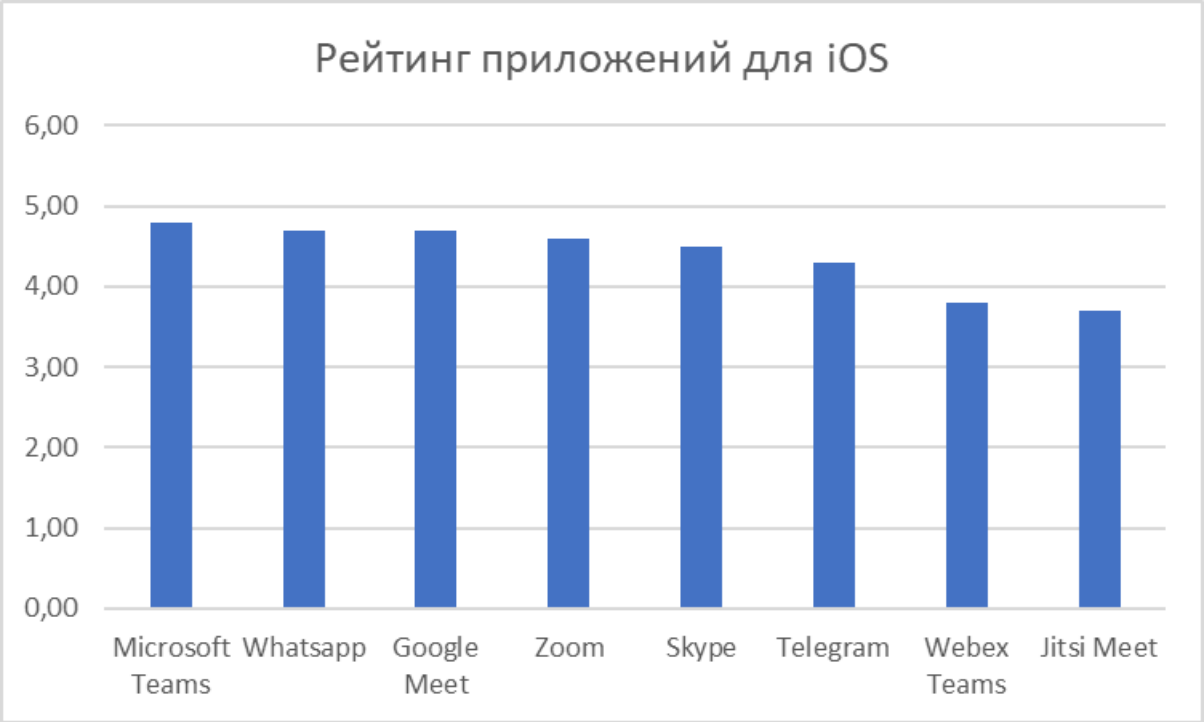


Рисунок 3.15. Рейтинг приложений в AppStore

Рейтинги приложений для Android OS и iOS представлены на рисунках 3.14–3.15. Видно, что Microsoft Teams и Whatsapp получают более высокую оценку от пользователей как Android, так и iOS. В конце рейтинга находятся приложение Jitsi Meet. Стоит отметить, что у этого приложения также меньше всего скачиваний и оценок пользователей. График общего рейтинга приложений на обеих платформах представлен на рисунке 3.16.

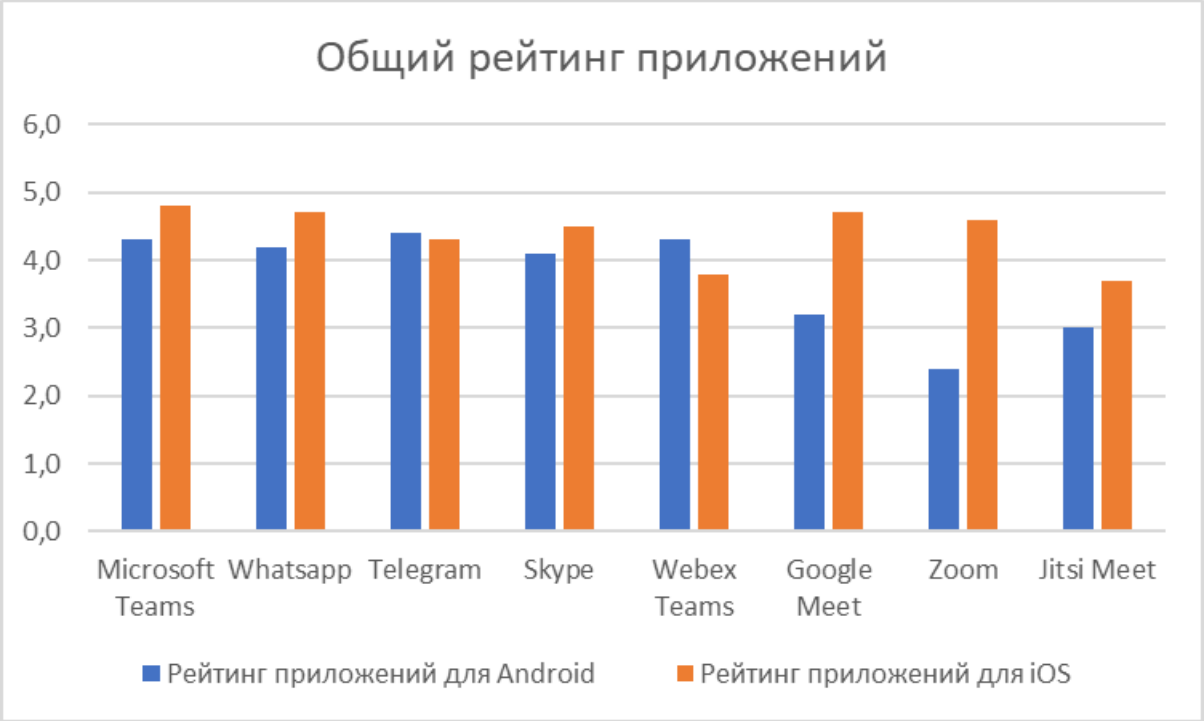


Рисунок 3.16. Общий рейтинг приложений

Резюме

Современные технологии должны гарантировать, что они делают достаточно, чтобы медиаданные шифровались для обеспечения конфиденциальности медиапотоков. Сейчас отрасль находится на пороге E2E-шифрования в браузере. Это захватывающее время, и компании стремятся добавить его в свои продуктовые линейки. Однако эта среда быстро меняется, и поставщики видеоплатформ должны уметь меняться вместе с ними. Продукты должны оставаться гибкими, поскольку API-интерфейсы и направления браузера могут измениться в любой момент.

IP-телефония и ИИ присоединились к технологическому тренду благодаря усовершенствованию своих услуг и продуктов для бизнес-операций. Применение технологий ИИ, например функций перевода в режиме реального времени, обработки естественного языка и многого другого, к каналам IP-телефонии может открыть новый мир для передовых моделей связи и делового сотрудничества в будущем.

Такие предприятия, как колл-центры, которые ежедневно принимают много звонков, могут извлечь выгоду из технологии IP-телефонии в сочетании с ИИ. ИИ в колл-центрах управляет трафиком вызовов, перенаправляя вызовы в другие сети с помощью методов машинного обучения. Это ценно для повышения эффективности бизнеса, поскольку обеспечивает общение без искажений как на стороне сотрудника, так и на стороне вызывающего абонента и повышает производительность групп обслуживания клиентов. ИИ помогает улучшить общее впечатление клиентов, предоставляя улучшенную интерпретацию запросов для

лучшего понимания требований клиентов. Поскольку все делается автоматически, это экономит время, легко решая сложные вопросы.

Вопросы для самопроверки

1. Каковы основные тренды развития современных технологий IP-телефонии?
2. Каковы пути уменьшения нагрузки на трафик в сетях передачи данных?
3. Опишите методы мультиплексирования пакетов.
4. В чем сущность методов сжатия заголовков пакетов?
5. Опишите режимы работы протокола RoHC.
6. Для чего применяется сквозное шифрование в протоколе WebRTC?
7. Есть ли проблемы безопасности в протоколе WebRTC? Какие и почему?
8. Какие перспективные проекты для решения проблемы сквозного шифрования Вы знаете?
9. В чем сущность функции Insertable Streams?
10. Каково назначение и применение Jitsi Meet?
11. Для достижения каких целей сегодня используются Interactive Voice Response?
12. Какие базовые технологии, используемые в системе IVR, Вы знаете?
13. Назовите основы развертывания IVR-систем.
14. Каковы преимущества применения IVR-систем в современном мире?
15. Назовите недостатки IVR-систем и их последствия?
16. Дайте обоснование рекомендаций по применению IVR-систем.
17. Перечислите основные приложения для голосовой связи в реальном времени.
18. Раскройте понятие и анализ функциональности приложений.
19. Перечислите протоколы, применяемые в основных приложениях для голосовой связи в реальном времени.
20. Раскройте понятие и анализ трафика приложений и избыточные потоки.

Раздел 4. ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕХНОЛОГИЙ IP-ТЕЛЕФОНИИ

Рост индустрии VoIP в ближайшие годы связан с условиями неопределенности, вызванной пандемией, ростом удаленной работы, увеличением количества мобильных устройств. Также неотъемлемыми факторами развития являются тенденции VoIP, направленные на внедрение 5G, рост UCaaS и более широкое использование ИИ. Согласно последним тенденциям рынка VoIP, к 2027 году мировой рынок мобильного VoIP достигнет 183,7 млрд долларов [53].

Компании испытывают растущую потребность в экономичных коммуникационных решениях, которые могут поддерживать корпоративную мобильность. Здесь на помощь приходят системы VoIP. Эта технология позволяет пользователям реализовывать гибкие системы связи, при этом используя все опции, необходимые бизнесу – звонки, SMS, электронную почту, видеоконференции и т.д. Более того, это поможет сократить эксплуатационные расходы.

Когда компании становятся глобальными, им нужны решения для улучшения связи и совместной работы с удаленными сотрудниками. Это увеличивает спрос на продукты VoIP, такие как IP-телефоны и дешевые тарифные планы [106]. Кроме того, государственные учреждения и частные компании по всему миру инвестируют огромные средства в технологии беспроводной связи, такие как 4G/LTE и сеть 5G. Эти разработки приводят к более высоким скоростям передачи для высококачественных услуг передачи голоса и данных для бизнеса [25].

4.1. Основные направления развития технологий IP телефонии

Сети 5G. Быстро меняющийся бизнес-ландшафт требует коммуникационного процесса, который может идти в ногу с ним. Вот почему внедрение сетей 5G является одной из самых обсуждаемых тенденций на рынке VoIP сегодня.

Сети 5G или глобальные беспроводные сети пятого поколения – это технология передачи данных, которая использует диапазон крайне высоких частот (30–300 ГГц). Это позволяет обеспечить более высокую скорость связи (до 20 Гбит/сек) и скорость отклика (до 1 мс), а также устранить дрожание (jitter) вызовов и потерю пакетов во время передачи данных [104]. Следовательно, это позволит интернет-пользователям иметь лучшее мобильное широкополосное соединение, молниеносную скорость просмотра, а также увеличить пропускную способность сети.

Исследование [74] показывает, что преимущества сети 5G включают в себя более высокую скорость передачи данных (72%), улучшенное подключение носимых устройств (50%) и снижение количества сброшенных вызовов (47%). Эти преимущества стимулируют все большее количество предприятий к внедрению VoIP, а те, кто внедряет VoIP, будут еще больше расширять свое использование. Только в 2019 году 25 операторов запустили услугу 5G. К концу 2020 года во всем мире насчитывалось около 218 миллионов пользователей 5G, что превысило прогнозируемые цифры.

Развитие сетевой инфраструктуры. Сетевые технологий стремительно развиваются, появляются новые концепции, которые позволяют упростить процесс построения сетей. Существуют два новых подхода к построению сетевой инфраструктуры: программно конфигурируемые сети (SDN) и виртуализация сетевых функций (NFV).

SDN (рисунок 4.1) предлагает выносить логику работы с устройств на отдельный контроллер, благодаря чему нет необходимости покупать дорогостоящие оборудование, дорогим будет только контроллер [47]. Так как на устройствах, поддерживающих SDN, нет никаких конфигураций, а за всю логику сети отвечает контроллер, то сеть становится вендор-независимой, что позволяет использовать оборудование от разных производителей.

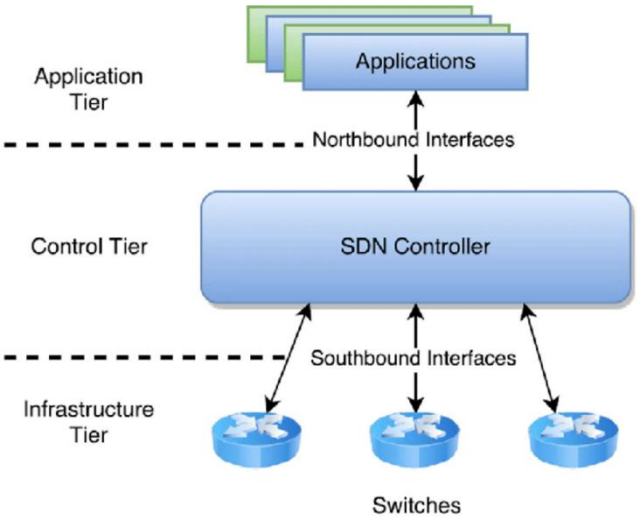


Рисунок 4.1. Архитектура SDN

Концепция NFV (рисунок 4.2) заключается в замене физических устройств их виртуальными аналогами. Это также позволяет сократить расходы на оборудование и добавляет масштабируемость, так как теперь для добавления нового элемента сети не нужно искать место для нового оборудования [24].

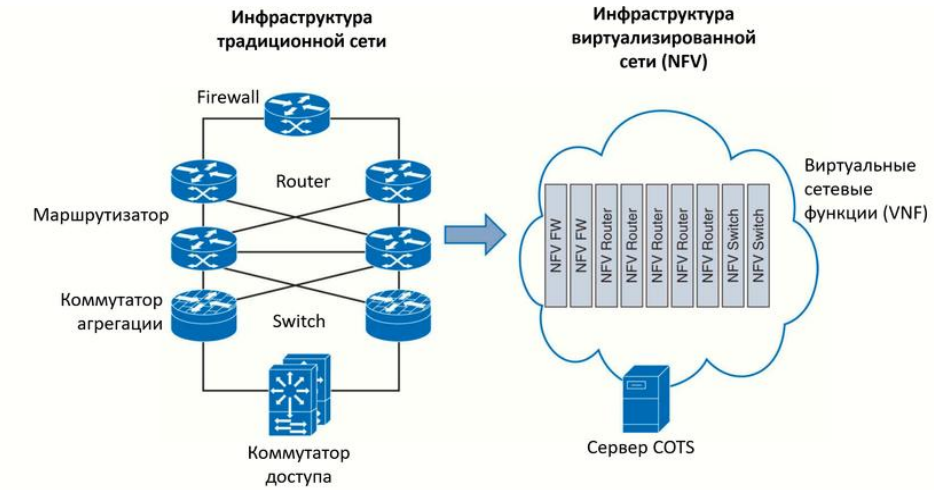


Рисунок 4.2. Архитектура NFV

Оба подхода упрощают управление сетью – не надо подключаться отдельно к каждому устройству для его настройки, что значительно сокращает и время работы сетевых инженеров, и шанс допустить ошибку.

Несмотря на очевидные преимущества данных подходов, такие как сокращение затрат, увеличение масштабируемости, упрощение развертывания и поддержки, на данный момент они не получили обширного применения. Связано это с тем, что технологии являются новыми и кардинально отличаются от привычного подхода. Со временем эти концепции станут применяться чаще, что, безусловно, повлияет на развитие VoIP технологий.

Искусственный интеллект. Перспективным направлением развития VoIP является совместное использование с ИИ, что позволит поставщикам услуг VoIP в автоматическом режиме классифицировать и распределять входящие сообщения на основе требуемой компетенции агента, срочности и набора навыков. ИИ способен обнаруживать недостоверность голоса человека и использовать биометрические маркеры для предотвращения мошенничества. Например, технологии Nuance обеспечивают 85% компаний из списка Fortune мерами по борьбе с мошенничеством в голосовой связи, используя набор данных известных мошеннических голосов как часть более широкой системы обнаружения мошенничества.

Технологии ИИ для борьбы с мошенничеством становятся все более доступными для малых предприятий, особенно по мере того, как популярные облачные инструменты VoIP подключаются к более крупным игрокам с ИИ [48].

VoIP и CRM. Интеграция данных VoIP с другими данными клиентов позволяет получить множество полезных сведений о частоте общения с клиентами, количество времени, потраченного на звонки, на основе которых можно определить наиболее нагруженные участки сети, где необходимо увеличить количество ресурсов колл-центра. Использование сервиса VoIP совместно с приложением управления взаимоотношениями с клиентами (CRM) гарантирует полностью обогащенные базы данных контактов, автоматическое обновление и работу в режиме реального времени [34].

Безопасность VoIP. Взломы безопасности VoIP в последние годы попали в заголовки первых полос газет. В мае 2019 года некоторые известные учетные записи WhatsApp стали жертвами взлома, который мог внедрить вредоносное ПО в их телефоны и украсть данные, просто позвонив им. Им даже не нужно было брать трубку, звонки не оставляли следов в журнале телефона. Бьорн Рупп, генеральный директор немецкой компании CryptoPhone, занимающейся безопасными коммуникациями, сказал в интервью Wired: «Безопасность никогда не была основной целью разработки WhatsApp, а это означает, что WhatsApp должен полагаться на сложные стеки VoIP, известные своими уязвимостями».

Можно ожидать, что важным направлением в развитии VoIP будет разработка более мощной многоуровневой защиты в целях избежания подобных взломов [77].

Умная маршрутизация по языку. Для компаний, обслуживающих своих клиентов на разных языках, не всегда легко персонализировать клиентский опыт. Однако все больше инструментов VoIP предлагают функции распознавания языка, которые направляют вызовы нужным представителям в соответствии с языком. Одним из поставщиков таких услуг является RingCentral, с помощью которого можно распознавать и маршрутизировать вызовы более чем на 70 языках [27].

Инновационные способы использования VoIP API. В будущем API будут творчески использоваться для интеграции с существующими системами и данными. Вариантом такого применения может быть подключение API RingCentral к сайту WordPress для отправления SMS-уведомлений о новых публикациях.

4.2. Перспективы повышения безопасности IP-телефонии

IP-телефония – это, прежде всего, сеть с коммутацией пакетов, которые передаются наряду с другими корпоративными сервисами, такими как Интернет, почта и др. Поэтому необходимо обеспечить системы корпоративной IP-телефонии многоуровневой защитой. Нужно учитывать, что риски включают не только перехват звонков и несанкционированное использование системы, но и использование систем VoIP для взлома других подразделений компании или для кражи данных и атак социальной инженерии.

Важно использовать четкий набор определенных мер, применяемых в комплексе, – межсетевое экранирование, антивирусная защита, регулярные обновления программного обеспечения, шифрование передаваемых данных, тестирование на проникновение, использование NAT адресации и другое.

Каждый крупный провайдер IP-телефонии имеет в своем наборе услуг облачную АТС, которая настраивается в считанные минуты и способна обеспечить телефонией компанию любого размера независимо от ее территориального расположения. Облачная или виртуальная АТС – это очень удобное решение, которое привлекает заказчиков тем, что не надо держать лишние сервера в здании и обслуживать их. Вместо этого можно просто арендовать необходимые серверные мощности или сервис телефонии. Однако с точки зрения информационной безопасности облачные АТС – это идеальная цель для хакерских атак, потому что, как правило, аккаунты для доступа к настройкам АТС находятся в открытом доступе. Если владелец аккаунта не озаботится созданием стойкого пароля, то он рискует оплатить немалый счет за телефонные разговоры злоумышленника или предоставить доступ к записям разговоров своих сотрудников. Таким образом, провайдер должен обеспечивать защиту целостности и конфиденциальности данных, используя шифрование [68].

Тенденции развития информационных технологий указывают на то, что в недалеком будущем голосовая информация также будет подвергаться шифрованию. Большинство VoIP-вендоров уже давно имплементируют в своих решениях поддержку таких протоколов, как SIP/TLS, SRTP, ZRTP и др., стимулируя поль-

зователей применять еще один уровень защиты. Например, большинство IP-телефонов и решений видеоконференцсвязи от компании Cisco, а также системы CUCM, CUBE, Cisco SBC, UCCS и др. поддерживают TLS 1.2 и SRTP. Самое распространенное Open Source решение IP-АТС Asterisk имеет поддержку защищенных протоколов передачи медиатрафика, начиная с версии 1.8. В программной Windows-based АТС 3CX версии V15 поддержка SRTP включена по умолчанию [102].

VoIP-решения зачастую очень тесно интегрируются с другими корпоративными системами, такими как CRM, ERP, CMS, не говоря уже о таких каналах бизнес–коммуникаций, как e-mail, обмен мгновенными сообщениями (чат) и социальные сети, формируя в совокупности концепцию UC (Unified Communications). Потенциальные преимущества, которые несет данная концепция, очень привлекательны, но вместе с тем создается множество точек, уязвимых к возможному взлому. Недостаточный уровень защиты одной из них может быть угрозой всей корпоративной сети. Поэтому разработчики, несомненно, будут усиливать безопасность каналов интеграции данных систем.

Можно также ожидать интеграцию систем корпоративной телефонии в такие средства защиты, как DLP (средства защиты от утечек), адаптации метрик VoIP в SIEM-системах (система управления информацией и событиями безопасности), а также появление унифицированных репутационных баз (Threat Intelligence) со списками потенциально опасных номеров или других индикаторов компрометации, относящихся к VoIP, которые будут автоматически блокироваться имеющимися средствами защиты [79, 80].

Помимо паролей, многоступенчатой аутентификации, шифрования и биометрии, будущие тенденции безопасности в отрасли VoIP могут опираться на технологии блокчейна для децентрализации контроля над системой. Отказ кибер-злоумышленникам в единой точке атаки означает, что им будет труднее взломать систему [29].

С развитием технологий передачи данных и появлением сетей поколения 5G были разработаны новые методы повышения безопасности подключения в сети, в перспективе применимые и в IP-телефонии.

Консорциум, разрабатывающий спецификации для мобильной телефонии (3GPP), в основу сети 5G заложил неавтономный режим (Non-Standalone, NSA), также известный как EN-DC (E-UTRA-NR Dual Connectivity). Ключевой особенностью неавтономного режима является возможность использовать уже существующую инфраструктуру LTE, что делает новую радиотехнологию доступной без замены сети. EN-DC использует LTE в качестве основной технологии радиодоступа, в то время как новая технология радиодоступа (New Radio, NR) служит вторичной технологией радиодоступа с пользовательским оборудованием (secondary radio access technology with User Equipments, UE), подключенным к обеим радиостанциям. Процедуры безопасности для EN-DC в основном соответствуют стандартам безопасности двойного подключения для 4G [91].

Главная базовая станция сети стандарта LTE eNB проверяет, имеет ли UE возможности 5G NR для доступа к вторичному gNB, то есть к базовой станции 5G, и права доступа к gNB.

eNB создает и отправляет ключ, который будет использоваться gNB для безопасной связи через NR; UE также получает тот же ключ. В отличие от двойного подключения в сетях 4G, сообщениями управления радиоресурсами (Radio Resource Control – RRC) можно обмениваться между UE и gNB, таким образом получаются ключи, используемые для защиты целостности и конфиденциальности сообщений RRC, а также данные плоскости пользователя (User Plane, UP). Хотя защита целостности для данных UP поддерживается в сети 5G, она не будет использоваться в случае EN-DC [61].

Модель доверия меняется при переходе от неавтономной к автономной системе 5G. Считается, что доверие в сети уменьшается по мере удаления от ядра. Это влияет на решения, принимаемые при разработке системы безопасности 5G.

В архитектуре роуминга домашняя и гостевая сети соединяются через прокси-сервер SEcurity Protection Proxy (SEPP) для уровня управления межсетевым соединением. Такая модель доверия изображена на рисунке 4.3. Это усовершенствование реализовано в 5G из-за недавно выявленного большого количества атак, таких как кража ключей и перенаправление атак в SS7, а также олицетворение сетевого узла и подмена исходного адреса в сигнальных сообщениях в DIAMETER, которые использовали доверенный характер межсетевого соединения [7].

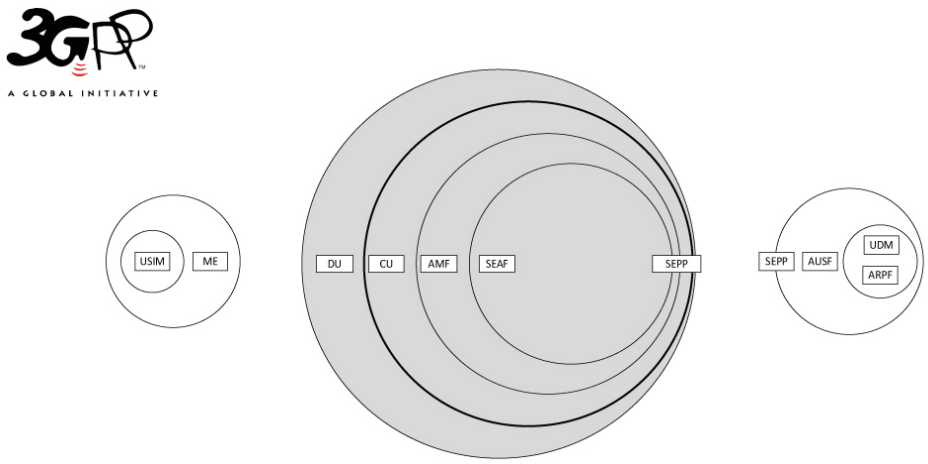


Рисунок 4.3. Модель доверия в сети 5G с роумингом

Функция сервера аутентификации (Authentication Server Function, AUSF) состоит в сохранении полученного после аутентификации ключа для повторного использования в случае одновременной регистрации UE в различных сетевых технологиях доступа, то есть сетях доступа 3GPP и сетях доступа Non-3GPP, таких как беспроводная локальная сеть IEEE 802.11 (WLAN). Функция хранилища и обработки учетных данных аутентификации (Authentication credential Repository and Processing Function, ARPF) – сохранять учетные данные аутенти-

фикации. Это выполняется с помощью USIM на стороне клиента, то есть на стороне UE. Информация о пользователе хранится в хранилище унифицированных данных (Unified Data Repository, UDR). Унифицированная база данных (Unified Data Management, UDM) использует данные, хранящиеся в UDR, и реализует логику приложения для выполнения различных функций, таких как создание учетных данных для аутентификации, идентификация пользователя, непрерывность сеанса и т.д. Активные и пассивные атаки через облачный сервис рассматриваются как на уровне управления, так и на уровне пользователя. В роуминговой архитектуре домашняя и гостевая сеть соединяются через пограничную сетевую функцию (Security Edge Protection Proxy, SEPP) для управления плоскостью межсетевого соединения. Это усовершенствование сделано в 5G из-за количества обнаруженных атак, таких как кража ключей и атаки с измененной маршрутизацией в SS7, а также имитация сетевого узла и подмена адреса источника в сигнальных сообщениях в DIAMETER, которые использовали доверительный характер межсетевого взаимодействия.

Аутентификация устройства в сети в 5G основана на первичной аутентификации. Это похоже на то, что было реализовано в 4G, но с некоторыми отличиями. Механизм аутентификации имеет встроенный домашний контроль, позволяющий домашнему оператору узнать, аутентифицировано ли устройство в данной сети, и принять окончательный вызов аутентификации. При первичной аутентификации 5G существует два обязательных варианта: аутентификация и согласование ключей 5G (5G-AKA) и протокол расширенной аутентификации EAP-AKA. По желанию, в 5G также разрешены другие механизмы аутентификации на основе EAP. Кроме того, первичная аутентификация не зависит от технологии радиодоступа, поэтому она может работать с технологиями, отличными от 3GPP, такими как WLAN IEEE 802.11.

Вторичная аутентификация в 5G предназначена для аутентификации в сетях передачи данных за пределами домена оператора мобильной связи. Для этой цели могут использоваться различные методы аутентификации на основе EAP и соответствующие учетные данные. Аналогичная услуга была возможна и в 4G, но теперь она интегрирована в архитектуру 5G.

В межоператорском интерфейсе существует несколько проблем безопасности, возникающих из протоколов SS7 или Diameter в более ранних поколениях систем мобильной связи. 5G с самого начала обеспечивает безопасность между операторами [18].

Связанные с идентификацией абонента проблемы известны со времен 4G и более ранних поколений мобильных систем. В 5G разработано решение для обеспечения конфиденциальности, которое защищает постоянный идентификатор пользователя от активных атак. Открытый ключ домашней сети используется для обеспечения конфиденциальности идентификации абонента.

Базовая сеть 5G основана на сервис-ориентированной архитектуре, которой не было в 4G и более ранних поколениях.

В 5G сеть радиодоступа логически разделена на распределенные блоки (distributed units, DU) и центральные блоки (central units, CU). DU и CU вместе образуют gNB – базовую станцию 5G. Безопасность обеспечивается для интерфейса CU-DU. Такое разделение также было возможно в 4G, но в 5G это часть архитектуры, которая может поддерживать различные варианты развертывания. DU, которые развернуты на самом краю сети, не имеют доступа к каким-либо пользовательским данным, когда включена защита конфиденциальности. Даже при разделении CU-DU точка безопасности радиоинтерфейса в 5G остается такой же, как в 4G, а именно в сети радиодоступа [7].

Иерархия 5G отражает изменения в общей архитектуре с использованием принципа безопасности разделения ключей. Одним из основных отличий 5G от 4G является возможность защиты целостности плоскости пользователя.

Мобильность в 5G похожа на мобильность в 4G с разницей в том, что в 5G привязка мобильности в базовой сети может быть отделена от привязки безопасности.

Основными областями использования 5G являются мобильная широкополосная связь и Интернет вещей (IoT).

4.3. Перспективы внедрения VoIP в IoT

Появление Интернета вещей (IoT) и рост количества подключенных к Интернету устройств уже много лет меняют мир бизнеса, и лучшее еще впереди. Радикальный сдвиг парадигмы изменит то, как предприятия и потребители используют телефонию VoIP . В то время как VoIP набирает обороты в качестве технологической основы для предложений телефонных систем, IoT предоставляет новые возможности платформы с дополнительными преимуществами для пользователей VoIP. Их синергия будет способствовать дальнейшему развитию умных домов, умных офисов и более умных телефонных решений.

IoT – это концепция, направленная на подключение каждого устройства с выходом в Интернет для передачи и обмена данными по сети без необходимости вмешательства человека. Все, от бытовой техники до промышленных гаджетов, таких как голосовые датчики, может быть частью сети IoT.

Интернет вещей стремится сделать нашу жизнь проще. Он заполняет пробел, в котором люди не умеют собирать данные об окружающем мире с круглосуточным вниманием и абсолютной точностью. Он создает структуру подключения, в которой данные с разных устройств автоматически обмениваются и анализируются, чтобы обеспечить интеллектуальную автоматизацию и управление устройствами.

Например, одним из распространенных приложений Интернета вещей в реальном мире является система «умный дом». Когда температура в помещении поднимается и превышает определенный порог, система охлаждения может автоматически включиться, чтобы понизить температуру, и отправлять владельцу оповещения в режиме реального времени через подключенное приложение на мобильных телефонах. В этом случае датчик температуры, система охлаждения

и мобильное устройство соединяются в сеть IoT, которая позволяет инновациям работать вместе, предлагая интеллектуальные, упреждающие и эффективные технологические решения.

Это всего лишь одно из многих приложений IoT в сфере бизнеса и клиентов, где услуги VoIP также должны найти свою нишу и в полной мере использоваться.

4.4. Возможности Интернета вещей и технологий IP-телефонии

Интернет вещей (IoT) соединяет множество бытовых приборов, чтобы сделать мир лучше и умнее. Большинство устройств IoT используют Интернет-протокол (IP) для предоставления функций и информации. И в этом вопросе VoIP пересекается с технологией IoT. Вот почему встраивание услуг VoIP в решения IoT не является чем-то вроде журавля в небе и уже происходит.

Благодаря Интернету вещей ценностное предложение услуг VoIP будет только расширяться. Это оказывает влияние на мир VoIP, предоставляя компаниям еще больше функциональных возможностей их телефонных сетей.

Например, когда вы находитесь рядом с домом, вы можете позвонить и дать указание включить гейзер, чтобы вы могли принять теплый душ по прибытии. Или, если у вас плотный график и вам нужно автоматическое напоминание о предстоящем событии, вы можете настроить календари на автоматическое уведомление по IP-телефону, чтобы не пропустить важную дату.

VoIP может служить частью механизма IoT для автоматизации и удаленного управления устройствами. Большая способность технологии передавать информацию из одной точки в другую надежным и безопасным способом только расширит поток данных системы IoT и принесет огромные преимущества пользователям VoIP, добавив существующим устройствам уровень цифрового интеллекта. Синергия между ними открыла огромный потенциал для бизнеса и изменит VoIP в последующие годы.

IoT считается ключом к технологиям будущего. Интернет вещей работает с миллиардами устройств, подключенных к Интернету. Вещь в IoT – это смарт-объект, которому можно назначить IP-адрес и предоставить возможность обмена данными по сети на основе интернет-протокола (IP). Смарт-объекты, как правило, имеют ограниченные возможности с точки зрения вычислений и памяти. IoT-устройства, которые не могут запускать стек IP, например лампочки, дверные замки и датчики, подключены к сети через шлюз IoT, который соединяет вещи с облаком. VoIP предполагает передачу голоса в IP-сети, при этом сам телефон может быть аналоговым, цифровым или программным (софтфон). Система VoIP подключена к шлюзу VoIP, а также к телефонной сети. Шлюз VoIP позволяет телефонным звонкам осуществляться через IP-сеть. Предприятие может использовать IP-сети, чтобы совершать все телефонные звонки между своими локальными и удаленными офисами или разделить голосовую связь между IP-сетью и телефонной.

Интеграция систем VoIP с IoT станет очень полезной во многих сценариях, таких как автоматический набор номера телефона для экстренного события,

управление IoT-устройствами через аналоговый телефон и интеллектуальный мониторинг объектов через VoIP-телефон. Далее будет рассмотрено решение для связи с IoT-устройствами через телефонные и мобильные сети.

IoT превратился в глобальную сетевую инфраструктуру объектов с идентификацией, зондированием и коммуникационными возможностями на основе информационных и коммуникационных технологий, такие как RFID, Bluetooth и Wi-Fi. Вещи в IoT включают в себя множество физических объектов, таких как датчики, исполнительные механизмы и другие устройства, которые могут быть подключены к проводной или беспроводной сети [18]. Эти вещи могут собирать и обрабатывать данные, реагировать на управляющие входы и передавать данные по сети. Интернет вещей превращает повседневные объекты в нашей среде в умные объекты, которые могут обмениваться данными с другими членами сети, часто использующими подключение по IP. Таким образом, умные объекты действуют и реагируют автономно в своем окружении и иметь возможность общаться друг с другом и обмениваются информацией с людьми.

Приложения IoT предоставляют доступ к информации через проводную и беспроводную сеть подключения, позволяя пользователям управлять смарт-объектами из любого места. В результате Интернет вещей будет использоваться для решения задач в разных областях, включая города, энергетику, транспорт, промышленность, здравоохранение и связь. Количество IoT-устройств быстро растет за счет интеллектуальных систем, которые устанавливаются как на потребительском, так и на корпоративном уровнях приложений [18].

VoIP. VoIP работает на базе IP или через Интернет. Голос оцифровывается и кодируется в пакетах поверх данных сети связи, а не через коммутируемую сеть общего пользования.

Имея общую базовую инфраструктуру, передача обычных и голосовых данных может быть объединена в одной сети. Телефонная система VoIP может принимать и маршрутизировать вызовы по IP-сети. Система VoIP подключена к шлюзу VoIP, а также к телефонной сети. Шлюз VoIP позволяет совершать телефонные звонки через IP-сеть. Как показано на рисунке 4.4, предприятие может использовать IP-сети, чтобы совершать все телефонные звонки между своим локальными и удаленными офисами или разделить голосовую связь между IP-сетью и телефонией.

Кроме того, системы VoIP предлагают множество функций бесплатно. Некоторыми из этих функций являются переадресация вызовов, конференц-связь, автосекретарь и голосовая почта. Самой привлекательной особенностью системы VoIP является экономия средств. Международные и местные телефонные звонки становятся дешевле, когда средой передачи является Интернет. Для предприятия VoIP снижает стоимость инфраструктуры и технического обслуживания, поскольку голосовой трафик и трафик данных объединяются в единую сеть.

Протоколы VoIP, такие как протокол инициации сеанса (SIP), могут интегрироваться с несколькими другими уровнями приложений, что обеспечивает

аудио- и визуальное общение через Интернет. SIP используется конечные точки для создания, изменения и завершения сеансов, состоящих из одного или нескольких мультимедийных потоков. Целью SIP является обеспечение сигнализации и установления соединения по IP-сети, которая присутствует в Телефонной сети общего пользования.

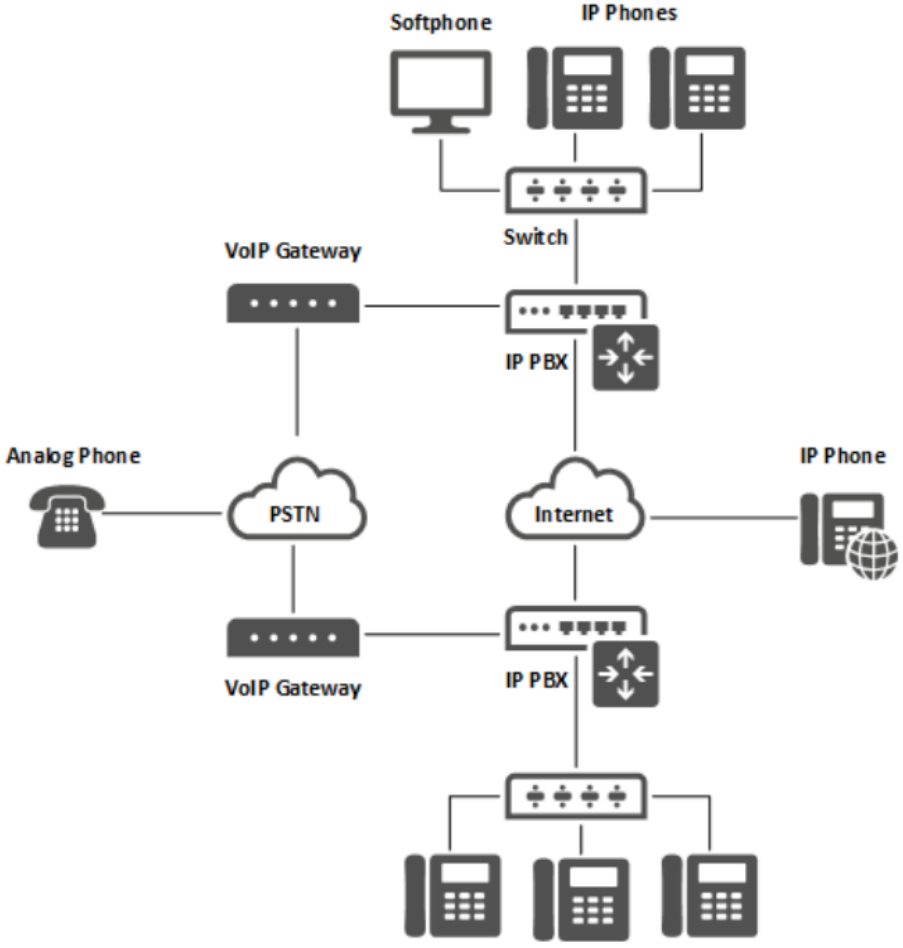


Рисунок 4.4. IP-телефония

Возможности «умной» VoIP системы. Поскольку IP является общим протоколом для Интернета вещей и VoIP, системы VoIP могут быть интегрированы в шлюз IoT для общения с вещами по телефонной сети и Интернет. Рассмотрим преимущества систем VoIP для Интернета вещей на примере интеллектуальной системы VoIP, которая позволяет пользователям общаться с вещами через любой телефон. Система через телефонные и мобильные сети позволяет пользователю получить доступ к IoT-шлюзу и дает ему возможность управлять IoT-устройствами удаленно. Основная идея этой системы заключается в том, чтобы использовать телефонные и мобильные сети для расширения возможностей подключения IoT-устройств. В последние годы было предложено несколько систем для увеличения возможностей подключения устройств дома и в офисе. Домашние устройства подключены к контроллеру с использованием различных коммуникационных технологий. Контроллер поддерживает сопряжение и уда-

ленный доступ к системе через коммуникационную сеть, обеспечивая, например, системы домашней автоматизации на основе Bluetooth и ZigBee. Однако существующие системы позволяют пользователям контролировать устройства через веб-браузер или приложение для смартфона.

Интеллектуальная система VoIP, как показано на рисунке 4.5, относится к системам домашней автоматизации, которые позволяют управлять освещением, дверьми, окнами и прочей бытовой техникой. Система имеет возможность маршрутизировать звонки, собирать информацию, взаимодействовать с абонентами и управлять устройствами через веб-браузер и телефоны любого типа, например, незрячие люди могут получить информацию о своем доме и управлять домашними устройствами, используя только клавиатуру телефона.

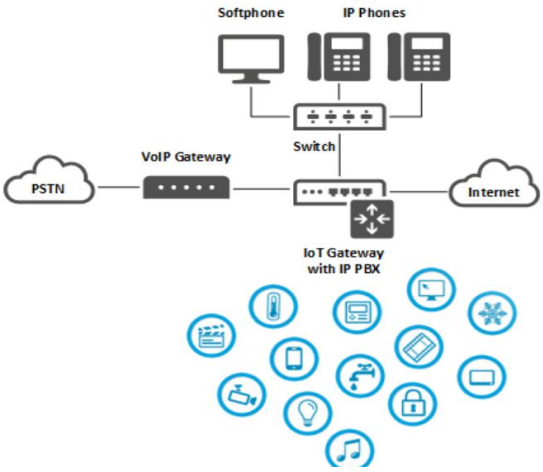


Рисунок 4.5. «Умная» VoIP система

Система также может быть настроена для домашней безопасности: в экстренном случае система автоматически способна набрать номер телефона и воспроизвести необходимое голосовое сообщение. Кроме того, телефоны VoIP можно настроить для приема SIP-уведомления от умной системы VoIP. Например, датчик движения может уведомлять пользователя через VoIP-телефон об активности на территории. Домашние устройства также могут управляться VoIP-телефоном с помощью функции XML, она позволяет VoIP-телефону служить пользовательским интерфейсом для системных служб, таких как включение света и показ температуры в помещении.

Пример реализации интеллектуальной VoIP системы. Умная система VoIP (рисунок 4.6) состоит из трех управляемых устройств – лампочки, дверного замка и открывателей окон, а также датчиков влажности, температуры, обнаружения газа и движения. Система позволяет выполнять следующие сценарии:

- принимать и совершать звонки по телефону сети с использованием шлюза VoIP;
- управлять лампочкой, дверным замком и открывателем окон через телефонная клавиатура;
- удаленно управлять домашними устройствами через аналоговый телефон с защитой паролем;

– отправлять уведомления о температуре, влажности и движении по территории через IP-телефон;
– автоматически звонить по номеру телефона с голосовым сообщением на случай аварийной ситуации с газом.

Система состоит из аппаратных и программных компонентов. Аппаратное обеспечение основано на Raspberry Pi – это недорогое решение для внедрения интеллектуальной системы VoIP. Raspberry Pi – это компьютер размером с кредитную карту, способный взаимодействовать с физическим миром, он использован в большом спектре приложений автоматизации. Существуют различные модели Raspberry Pi. Характеристики модели B, представленной на рисунке 4.7, а: 512 МБ RAM, два USB–порта, 26 контактов GPIO и порт Ethernet [38]. В феврале 2015 года его заменила RPi 2 B (рисунок 4.7, б), которая имеет много общих характеристик с RPi 1 модели B+, но использует четырехъядерный процессор ARM и имеет 1 ГБ RAM [116].

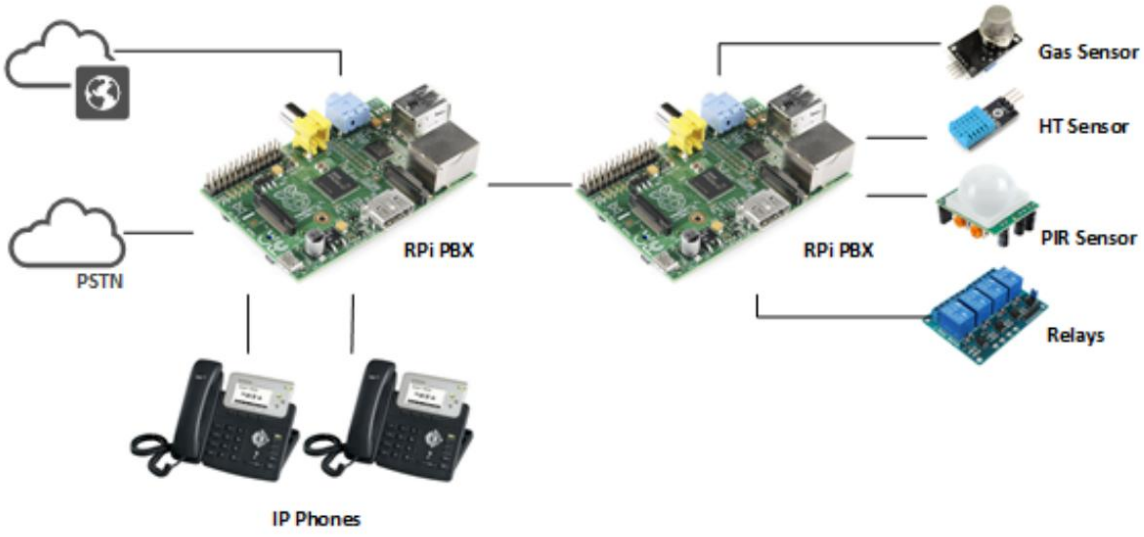
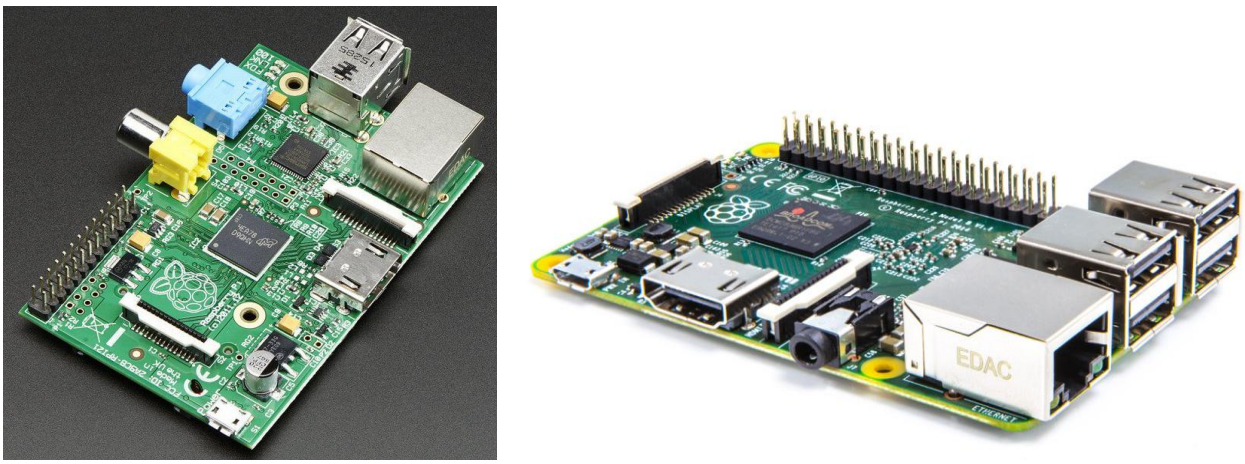


Рисунок 4.6. Схема системы



а б

Рисунок 4.7. а - Raspberry Pi 1 Model B; б - Raspberry Pi 2 Model B

Существует также несколько операционных систем, которые можно использовать с Raspberry Pi, однако есть бесплатная система Raspbian, разработанная специально для оборудования Raspberry Pi [38]. Данная операционная система основана на Debian Linux и оптимизирована для аппаратного обеспечения Raspberry Pi. Она поставляется с большим количеством программного обеспечения для программирования интерфейса физических устройств на основе Python.

В системе используются две платы RPi для IP-телефонии и домашней автоматизации и безопасности. Со второй платой используются различные датчики [50]. Язык программирования Python используется для чтения и записи контактов, а также для расширения функциональных возможностей системы по взаимодействию с физическим миром путем получения информации от датчиков и выполнения действий через реле. Шлюз VoIP настроен на первом RPi, что обеспечивает как входящие, так и исходящие вызовы через сеть PSTN или GSM [110].

Кроме того, на каждом RPi необходим SIP-транк для взаимодействия систем. Таким образом, вызывающие абоненты на первом RPi могут связаться с добавочными номерами на втором RPi, набрав добавочный номер напрямую. Добавочный номер на втором RPi предоставляется каждому устройству для включения и отключения – например, 101 для включения/выключения света и 102 для открытия/закрытия двери. Благодаря функции интерактивного голосового ответа (IVR) в системах VoIP вызывающие абоненты также могут взаимодействовать с устройствами через настраиваемое голосовое меню. Таким образом, вызывающим абонентам предоставляется возможность выбрать вариант, нажимая цифры на телефоне без помощи человека. Удаленный пользователь может получить доступ к системе через VoIP-шлюз или с помощью Интернета. Шлюз IoT интегрирован с IP-АТС для связи с домашними устройствами по аналоговому каналу или мобильному телефону. Для защиты домашних устройств от неавторизованных пользователей смарт-система VoIP настроена на ввод кода–пароля перед совершением каких-либо действий. При звонке на добавочный номер для включения или отключения устройства система проверит, введен ли правильный пароль, затем скрипт Python позволяет RPi включать или выключать это устройство [110].

4.5. Основные возможности и примеры интеграции VoIP и IoT

4.5.1. «Умный дом»

«Умный дом» – одна из первых технологических сфер, где сочетание VoIP и IoT может иметь значение. Всеохватывающая взаимосвязь VoI-устройств и другой бытовой техники облегчит управление домашней безопасностью, умным термостатом, освещением и т.д. [28].

Вот несколько примеров того, как IoT может работать в фоновом режиме, используя телефонную систему VoIP для автоматизации служб умного дома:

- Подключив мобильное устройство к термостату, можно регулировать температуру со своего телефона в любом месте, где есть подключение к Интернету, а также анализировать отчеты о погоде для установки температуры в здании.
- Холодильник проводит инвентаризацию всех своих текущих продуктов. Подключенное устройство затем отправляет список на VoIP-телефон покупателя, чтобы информировать его/ее о том, что требуется от продуктового магазина.
- Будучи подключенными к номерам и устройствам VoIP, автомобили могут оповещать об обслуживании механика, когда это необходимо.
- Периферийные устройства оборудования обмениваются диагностической информацией, при обнаружении проблем они отправляют пользователю предупреждение или даже вызывают службу поддержки.
- Подключив служба поддержки SMS для устройств IOT, можно отправить удаленную команду, и спринклерная система начнет поливать растения.

4.5.2. «Умный офис»

VoIP позволяет предприятиям работать в любом месте и с любого устройства. При подключении к IoT эта возможность будет максимальной. Подключая IoT и VoIP, предприятия могут создавать умные офисы, которые позволяют им значительно повысить свою эффективность и производительность.

Например, мобильные сотрудники могут подключить свой софтфон VoIP к офисному оборудованию, такому как принтер, факсимильный аппарат и настольный телефон, чтобы они могли использовать офисные ресурсы в любом месте, оставаясь продуктивными. Другим примером, который сегодня широко используется предприятиями, является интеграция системы VoIP с бизнес-платформами CRM. Благодаря интеграции продавцы могут получать данные о клиентах по звонку клиента, чтобы облегчить процесс продажи.

4.5.3. Преимущества интеграция VoIP с CRM

Лучшее взаимодействие с клиентами. Надлежащая интеграция системы VoIP и CRM позволяет компаниям обеспечить более плавное и беспроблемное взаимодействие с клиентами: надежная функция всплывающих звонков помогает сократить телефонные очереди клиентов и предлагает контекст для продаж или беседы со службой поддержки в кратчайшие сроки. Наличие всех форм данных в одном интерфейсе упрощает процесс обращения к клиентам для улучшения и укрепления отношений с ними, что, в свою очередь, помогает удерживать лояльных клиентов [2].

Данные о вызовах в реальном времени. Интеграция VoIP и CRM автоматически отслеживает и записывает журналы вызовов в реальном времени. Эти журналы могут включать телефонные номера, дату и время каждого звонка, продолжительность звонка, время ожидания, а иногда записи звонков также будут прикреплены к профилям клиентов, чтобы предоставить компаниям самую последнюю бизнес-аналитику.

Повышенная эффективность. Интеграция VoIP и CRM повышает эффективность работы: данные о вызове автоматически записываются системой в профиль клиента, помимо этих данных, настраиваемые заметки или последующие действия также могут быть добавлены сразу после вызова без дополнительных поисков, а некоторые CRM даже поддерживают автоматическое создание нового контакта при неизвестных входящих вызовах.

Лучшее управление. Эффективная интеграция VoIP с CRM позволяет собирать широкий спектр основных статистических данных, которые дают ценную информацию о производительности сотрудников. Эти данные предоставляют супервайзерам и менеджерам информацию об эффективности работы оператора, например, сколько вызовов оператор обрабатывает в день, количество разрывов связи и среднее время ожидания, а также помогают им определить, нуждается ли персонал в дальнейшем обучении продажам или поддержке.

Безопасность и доступ. Конечные точки VoIP могут играть активную роль в обеспечении безопасности и защиты любого местоположения, а также контролировать доступ к этому объекту. Устройства обработки изображений IoT, такие как IP-камеры безопасности и системы доступа к дверям, можно настроить как конечные точки VoIP и вызывать их с любого устройства, подключенного к Интернету, для просмотра прямых трансляций. Эти устройства безопасности также можно настроить на автоматический вызов и уведомление IP-телефонов при возникновении любых событий безопасности. Например, когда приходят посетители, система доступа к дверям, подключенная к сети VoIP, может инициировать вызов, чтобы уведомить пользователей о необходимости разрешить или ограничить доступ.

4.6. Проблемы развития технологии IP-телефонии

На данный момент существуют технологии, занявшие свою нишу и не дающие пространство для развития IP-телефонии. Транкинговая связь из-за своего удобства, а также максимальной эффективности в небольшом секторе будет востребована еще очень долго, что не дает место для развития IP-телефонии в качестве единственного, монопольного способа связи.

Кроме того, существуют значительные зоны, не покрываемые мобильной связью стандарта LTE (рисунок 4.8), следовательно, существование сотовой связи неминуемо как минимум еще некоторое время, за которое зона покрытия мобильной интернета не успеет увеличиться.

При уже появившемся стандарте мобильной связи 5G развитие технологии искусственно ограничивается властями некоторых стран. В Российской Федерации коммерческое использование технологии возможно только на базовых станциях, произведенных в Российской Федерации. Так как такие базовые станции только тестируются, массовое использование технологии можно ожидать через продолжительное время.

Развитие безопасности и конфиденциальности программных продуктов может ограничиваться для обеспечения общественного порядка. Таким образом,

обеспечивается безопасность большинства пользователей за счет снижения анонимности существующих программных продуктов.

Так как основная прибыль операторов сотовой связи поступает за счет предоставления звонков, из-за VoIP операторы начали терять прибыль, в связи с эти они ищут способы, препятствующие развитию IP-телефонии. Например, оператор Мегафон ввел ограничения на использование VoIP приложения Skype через мобильный Интернет за границей [11].

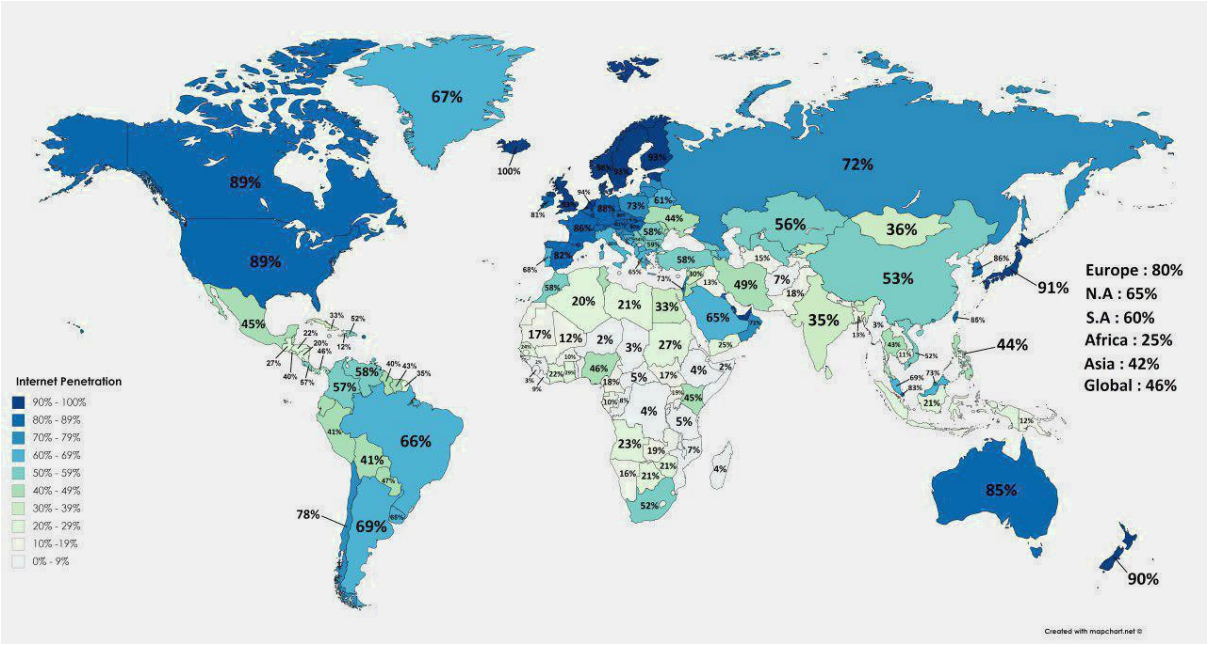


Рисунок 4.8. Зона покрытия мобильной связью

Резюме

Перспективы развития технологий IP-телефонии имеют множество направлений. Некоторые из них были рассмотрены в данном разделе. Развитие информационных технологий в целом напрямую влияет на развитие VoIP в частности. Основными тенденциями роста индустрии становятся интеграция искусственного интеллекта (ИИ), интернета вещей (IoT) и новых технологий обеспечения безопасности, пришедших с развитием мобильной связи.

Быстро меняющийся бизнес-ландшафт требует коммуникационного процесса, который может идти в ногу с ним. Внедрение сетей 5G является одной из самых обсуждаемых тенденций на рынке VoIP сегодня. Это положительно повлияет на скорость связи, скорость отклика, безопасность соединений.

Концепции «умного дома» и «умного офиса» активно развиваются в настоящее время, внедрение этих систем гарантирует повышение не только комфорта, но и эффективности, безопасности и лучшего управления. VoIP совершил революцию, предоставив значительную экономию средств, повышенную производительность и максимальный уровень мобильности и гибкости. Все эти преимущества могут быть дополнены возможностями, которые обеспечивают приложения IoT. На примере «умной» системы была рассмотрена успешная инте-

грации IP-телефонии и Интернета вещей, были определены возможности данной системы и оценена ее эффективность. В качестве развития интеллектуальной системы можно рассмотреть добавление функции распознавания голоса. Это открывает большие просторы для дальнейшего роста индустрии IP-телефонии.

Вопросы для самопроверки

1. Дайте обоснование перспектив развития технологий IP-телефонии.
2. Как связаны между собою сети 5G и технологии IP-телефонии?
3. Как связаны искусственный интеллект и технологии IP-телефонии?
4. Кратко опишите модель доверия в сети 5G с роумингом.
5. На чем основана базовая сеть 5G?
6. Какова сегодня основная сущность интернета вещей (IoT)?
7. В чем состоят перспективы внедрения VoIP в IoT?
8. Каковы основные совместные возможности и перпекктивы IoT и современных технологий IP-телефонии?
9. Назовите состав и возможности системы «Умный дом»?
10. Каковы состояние и перспективы интеграции системы VoIP с бизнес-платформами CRM?
11. Почему, по Вашему мнению, сегодня возникают проблемы развития и интеграции технологий IP-телефонии?

Раздел 5. ВИРТУАЛЬНЫЕ ОПЕРАТОРЫ СВЯЗИ

5.1. Общие сведения

Виртуальный оператор сотовой связи (Mobile Virtual Network Operator, MVNO) – компания, которая оказывает услуги сотовой связи под своим брендом, но не имеет собственной инфраструктуры и арендует ее у другого оператора.

Термин Mobile Virtual Network Operator был введен в обиход Национальным телекоммуникационным бюро, британским регулирующим органом в области телекоммуникаций (The Office of Telecommunications, OFTEL) в 1998 году.

Одним из первых примеров виртуального оператора является британская компания Virgin Mobile, которая существует с 1999 года. На протяжении следующих нескольких лет появились десятки виртуальных операторов, как независимых компаний, так и представителей известных торговых марок, некоторые из которых не были связаны с телекоммуникационной сферой.

В качестве виртуальных операторов также выступали представители MNO-компаний. Это было необходимо для расширения своей сети при отсутствии необходимой лицензии на предоставление услуг сотовой связи. Например, шведский телекоммуникационный холдинг TELE2 был создан в 1981 году и до 1993 года назывался Comviq. Сегодня холдинг работает в двух десятках стран Европы и СНГ, в том числе и в России, где на момент 2020 года насчитывалось до 46,6 млн клиентов [65].

5.2. Классификация виртуальных операторов сотовой связи

Среди MVNO существует достаточно определенная градация (рисунок 5.1) в зависимости от степени их вовлечения в процесс предоставления услуг мобильной связи. Традиционные операторы сотовой связи, MNO, могут предоставлять только радиочастотные ресурсы или собственные мощности (базовые станции, коммутаторы), а иногда сетевую инфраструктуру полностью (включая как аппаратное обеспечение, так и оборудование для ведения услуг, счетов, поддержки абонентов и др.).

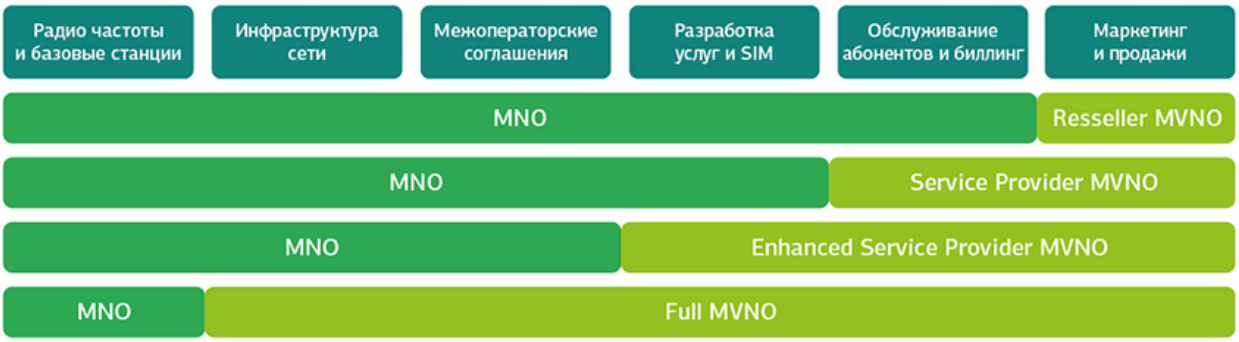


Рисунок 5.1. Диаграмма ресурсов разных типов MVNO

Reseller MVNO – самый простой вариант MVNO, специализирующийся только на продажах и маркетинге услуг базового оператора под собственным брендом [32, 33].

Service Provider MVNO (SP) – более продвинутый тип виртуальных операторов сотовой связи, где акцент делается на продаже контрактов, маркетинговой поддержке, развитием собственного бренда. Все технические вопросы выносятся во внешнюю среду, за которую ответственны реальные операторы, предоставляющие собственную инфраструктуру, либо на посредников. В качестве посредников выступают специализированные сервисные компании MVNE (Mobile Virtual Network Enables), занимающиеся поддержкой сетевой инфраструктуры и т.д. MVNE не обладают собственными лицензиями на предоставление услуг мобильной связи, это прерогатива традиционных операторов сотовой связи. Провайдер услуг MVNO работает под собственным брендом. MVNO может предлагать концепцию, бренд, каналы сбыта или большую существующую клиентскую базу, благодаря которым он может увеличить свои продажи или выделиться среди конкурентов.

Преимущества виртуальных операторов типа SP:

- собственные SIM-карты, возможность владения клиентской базой, а также возможность устанавливать тарифные пакеты и пакеты независимо от розничных цен, установленных оператором мобильной сети (MNO);
- использование MVNO для получения доли на рынке мобильной связи и доходов от телекоммуникаций или стимуляции роста основного бизнеса;
- концентрация на решениях для конкретной ниши или сегмента.

Недостатки виртуальных операторов типа SP:

- затраты на OPEX и CAPEX, связанные с ИТ-платформами;
- ограниченный доступ и контроль над возможностями сетевой маршрутизации;
- владение клиентами и SIM-картами, но не международным идентификатором мобильного абонента (IMSI).

Операционная модель / архитектура виртуальных операторов типа SP:

MVNO поставщика услуг обычно отвечает за процессы обслуживания клиентов, включая управление взаимоотношениями с клиентами (CRM), поддержку, процессы выставления счетов и платформу выставления счетов (BSS), тарифы, пакеты и рекламные пакеты, расходы на маркетинг, продажи и распространение, а также OPEX и CAPEX, связанные с ИТ-платформами [32, 33].

Enhanced Service Providers MVNO – это промежуточный тип виртуальных операторов. Такие компании могут предлагать абонентам собственные услуги, в том числе и дополнительные контент-услуги, поскольку обладают ресурсами для VAS, обеспечивают счета собственных абонентов и так далее. Обеспечением роуминга в сетях других операторов занимаются реальные операторы.

Преимущества виртуальных операторов типа Enhanced Service Providers:

– собственные SIM-карты, владение и отношения с клиентами, а также возможность устанавливать тарифные пакеты и пакеты независимо от розничных цен, установленных оператором мобильной сети (MNO);
– использование MVNO, чтобы заполнить долю на рынке мобильной связи и получать доходы от телекоммуникаций или стимулировать рост основного бизнеса (пакеты);
– концентрация на решениях для конкретной ниши или сегмента;
– MVNO может добавить свою собственную платформу услуг с добавленной стоимостью (VAS), чтобы повысить продажи или выделиться среди конкурентов в отношении приложений, данных и услуг контента [32, 33].

Недостатки виртуальных операторов типа Enhanced Service Providers:
– затраты на OPEX и CAPEX, связанные с ИТ-платформами;
– IMSI исходят от оператора мобильной сети (MNO) и контролируются им;
– MVNO не может заключать соглашения об оптовом присоединении трафика с другими операторами.

Операционная модель / архитектура MVNO Enhanced Service Providers:
– расширенный поставщик услуг отвечает за процессы обслуживания клиентов, включая управление взаимоотношениями с клиентами (CRM), поддержку, процессы выставления счетов и платформу выставления счетов (BSS), тарифы, пакеты и рекламные пакеты, расходы на маркетинг, продажи и распространение, а также OPEX и CAPEX, связанные с ИТ-платформами;
– некоторые виртуальные операторы типа Enhanced Service Providers могут владеть собственным реестром местонахождения (HLR), что позволяет управлять международным номером каталога абонентов мобильных станций (MSISDN), который представляет собой номер, используемый для международной идентификации номера мобильного телефона.

Full MVNO («полный» MVNO) – тип виртуальных операторов, которые предлагают своим абонентам весь спектр услуг, имеют собственные технические ресурсы, а также сами заключают соглашения на оказание услуг в роуминге, обеспечивают взаимодействие между операторами. Однако у них отсутствует лицензия на оказание услуг сотовой связи и есть необходимость использовать сети базовых станций реальных операторов [32, 33].

Преимущества виртуальных операторов типа Full MVNO:
– собственные SIM-карты;
– собственные диапазоны нумерации;
– регистр домашнего местонахождения (HLR);
– шлюзовый узел поддержки GPRS (GGSN);
– центр службы коротких сообщений (SMSC);
– служба мультимедийных сообщений (MMSC);
– шлюзовый центр мобильной коммутации (GMSC);
– собственные соглашения о роуминге;
– владение инфраструктурой сетевой коммутации;

– установка тарифных пакетов самостоятельно;
– полная собственность и отношения с клиентами;
– концентрация на решениях для конкретной ниши или сегмента;
– продажа собственных или партнерских услуг в качестве услуг с добавленной стоимостью (VAS);
– доступ к большим данным (данные об использовании пользователей) для улучшения качества обслуживания потребностей и желаний клиентов;
– использование MVNO, чтобы занять долю рынка мобильной связи и получать доходы от телекоммуникаций;
– расширение существующего основного бизнеса (пакеты) и получение большего контроля и независимости от операторов связи.

Недостатки виртуальных операторов типа Full MVNO:

– затраты на OPEX и CAPEX, связанные с необходимыми ИТ-платформами;
– необходимость определенного уровня понимания телекоммуникаций.

Операционная модель / архитектура «полного MVNO»:

отвечает за всю инфраструктуру и всю цепочку создания стоимости, кроме сетевой радиосвязи [32, 33].

5.3. Основы построения виртуальных операторов связи

Чтобы создать собственный виртуальный оператор, компаниям не нужно получать лицензии связи и строить базовые станции. Всю необходимую инфраструктуру они полностью или частично арендуют у родительского оператора – MNO (Mobile Network Operator), однако MVNO работает под собственным брендом (рисунок 5.2).

Совместная деятельность основного бизнеса с телеком-услугами открывает перед компаниями новые бизнес-возможности, позволяет сократить расходы на связь и обеспечивает лояльность клиентов [67, 69]. Для оператора создание MVNO позволяет увеличить клиентскую базу, получить источники дохода от аренды инфраструктуры, продвигать новые услуги и многое другое [94].

Рисунок 5.2. Схема связи MNO и MVNO

Под MVNO подразумеваются те компании, которые работают с конечным потребителем, занимаются маркетингом и продажами, а MNO (Mobile Network Operator) – это сам оператор, владеющий физической сетью.

Агрегаторы виртуальных операторов – MVNA (Mobile Virtual Network Aggregator). MVNA покупает оптовый доступ у оператора сети связи от имени нескольких MVNO, чтобы получить большую скидку, а затем перепродает доступ к сети каждому отдельному MVNO [83].

Платформа MVNE (Mobile Virtual Network Enabler) предоставляет MVNO технические решения, такие как поддержка клиентов, биллинговые системы, управление SIM-картами и так далее, что позволяет MVNO настраивать, эксплуатировать и взимать плату с абонентов [94] (рисунок 5.3).

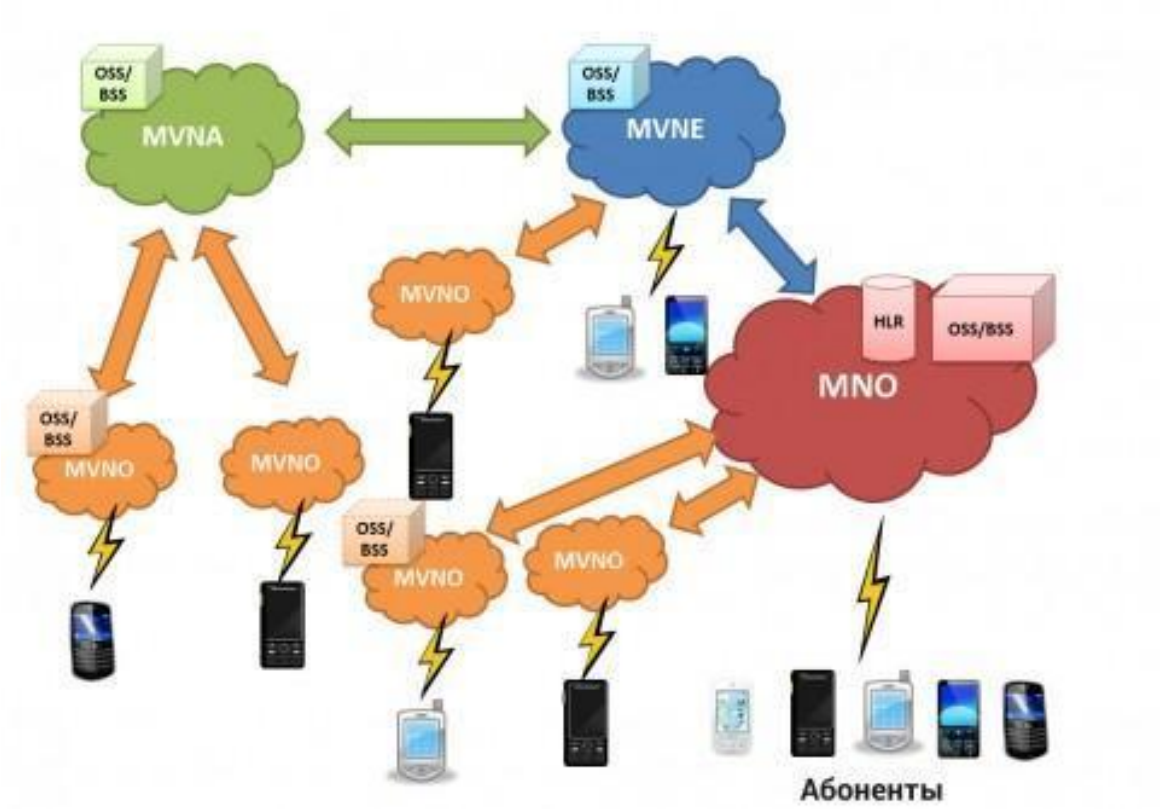


Рисунок 5.3. Схема взаимодействия между MNO, MVNE, MVNA и MVNO

На рынке существуют различные аппаратно-программные комплексы для реализации требований нормативного правового акта (НПА) для мобильных виртуальных операторов, работающих по схемам Light MVNO и Full MVNO [105]. На схеме (рисунок 5.4) представлены следующие элементы:

– MSC (Mobile Switching Center) – коммутатор сетей мобильной связи. Это АТС (автоматическая телефонная станция) с рядом функций, специфичных для сотовой связи функций. Поэтому многие MSC от известных производителей являются модификациями городских телефонных станций и изготавливаются на тех же платформах [111].
– G-MSC (Gateway MSC) – шлюзовой коммутатор мобильной сети для сетей GSM, UMTS, представляющий собой MSC с интерфейсами к другим теле-

фонным сетям. Почти все MSC операторов мобильной связи являются G-MSC, потому что MSC без доступа к внешним сетям смогут коммутировать только внутреннюю нагрузку данной мобильной сети. Такие сети редко используются на практике. Если объем трафика, исходящего во внешние сети связи, достаточно велик, то GMSC может быть реализован в виде отдельного коммутатора. Если в качестве GMSC используется автономное устройство, не предназначенное для коммутации внутренних нагрузок, то, по возможности, к нему подключают одновременно несколько MSC.

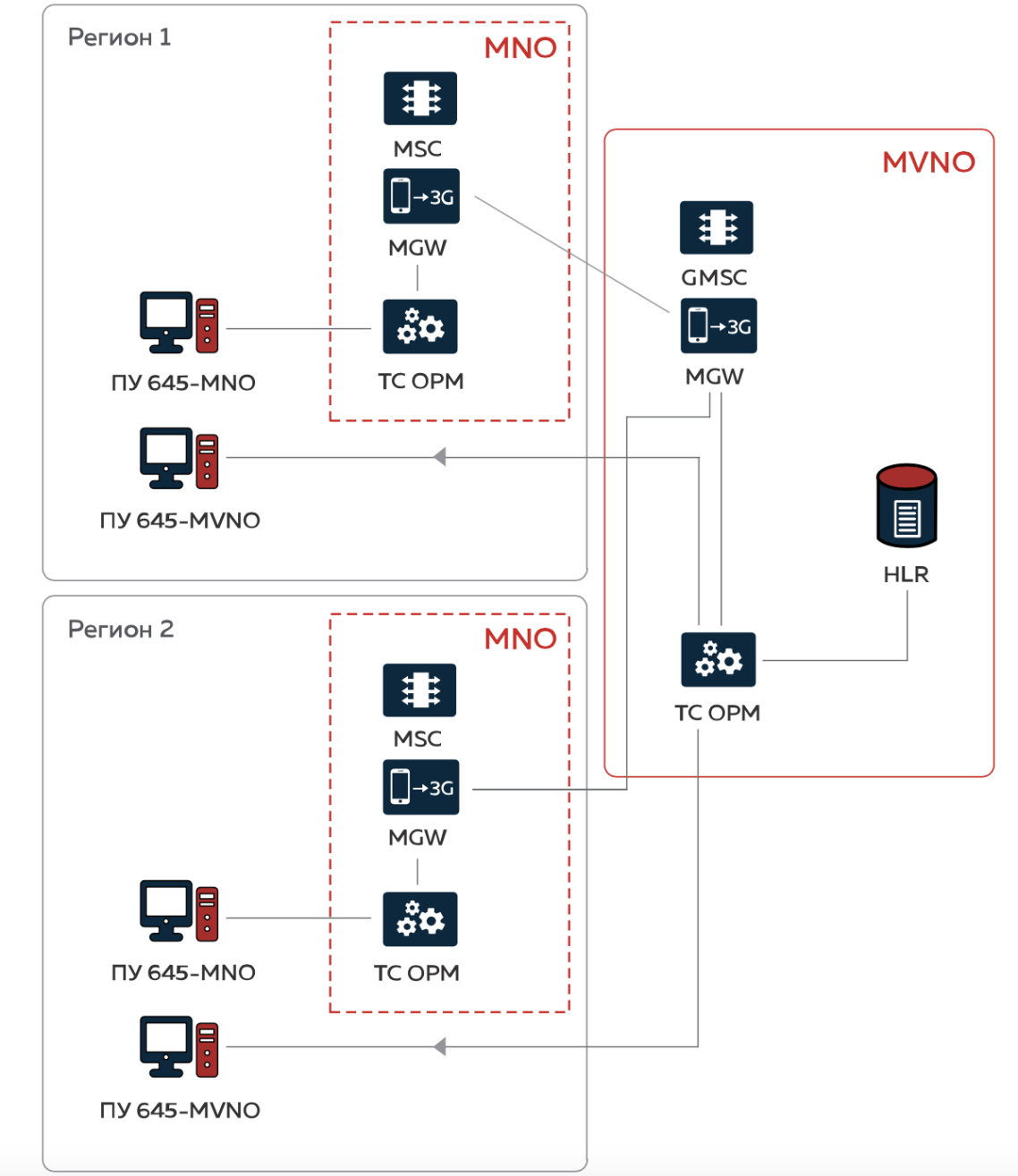


Рисунок 5.4. СпОС для MVNO

– MGW (Media gateway) – элемент сети сотовой связи стандарта UMTS, предназначенный для коммутации абонентских нагрузок. В сети UMTS

система коммутации (CN), в отличие от сети GSM, претерпела ряд изменений, одним из которых является разделение MSC на два элемента – MSC-S и MGW. MSC-S выполняет ряд функций обработки сигналов и управляет MGW. Весь абонентский голосовой трафик переключается на MGW под управлением MSC-S. Таким образом, к MGW подключаются интерфейсы к сети абонентского доступа и внешним голосовым сетям. Один MSC-S может одновременно управлять несколькими MGW [111].

– HLR (Home Location Register) – это централизованная база данных, содержащая подробную информацию о каждом абоненте данной сети GSM-оператора. С помощью HLR-запросов есть возможность проверять статусы мобильных номеров и удалять из базы устаревшие номера. Сервис проверки номера сохраняет конфиденциальность запроса и не затрагивает абонента.

5.4. Конвергентный MVNO

Конвергенция фиксированных и мобильных сетей FMC (Fixed Mobile Convergence) – это объединение различных типов сетей на единой технологической основе. Это расширяет возможности предоставляемых услуг MVNO, которые ранее создавались на раздельной основе (рисунок 5.5).

Рисунок 5.5. Конвергенция фиксированных и мобильных сетей и расширение возможностей услуг

Переход от аппаратного способа построения сетей, когда каждая функция создается при помощи выделенного аппаратного устройства, на программную реализацию, когда функции сети создаются при помощи программных модулей, работающих на стандартном вычислительном оборудовании в центрах обработки данных ЦОД (дата-центры), привел к расширению возможностей конвергентных сетей [120]. Если раньше виртуальным называли оператора, который не имеет собственной радиосети, то теперь подразумевается «виртуализация сете-

вых функций» NFV (Network Function Virtualization). Появился термин «виртуальный MVNO» (vMVNO), в котором элементы сетевой операторской инфраструктуры реализованы на стандартном IT-оборудовании дата-центров (серверы, системы хранения и локальные сети, их соединяющие) [83].

Благодаря переходу с традиционных аппаратных платформ на виртуальные ИТ-платформы (рисунок 5.6) удается достигнуть следующих преимуществ:

– снижение затрат на построение и техническую эксплуатацию сети;
– стандартизация и унификация сетевого оборудования;
– расширение спектра услуг сети;
– снижение времени разработки и вывода новых услуг на рынок.

Рисунок 5.6. Цифровая трансформация операторских сетей на основе технологии виртуализации сетевых функций в стандартном ИТ-оборудовании

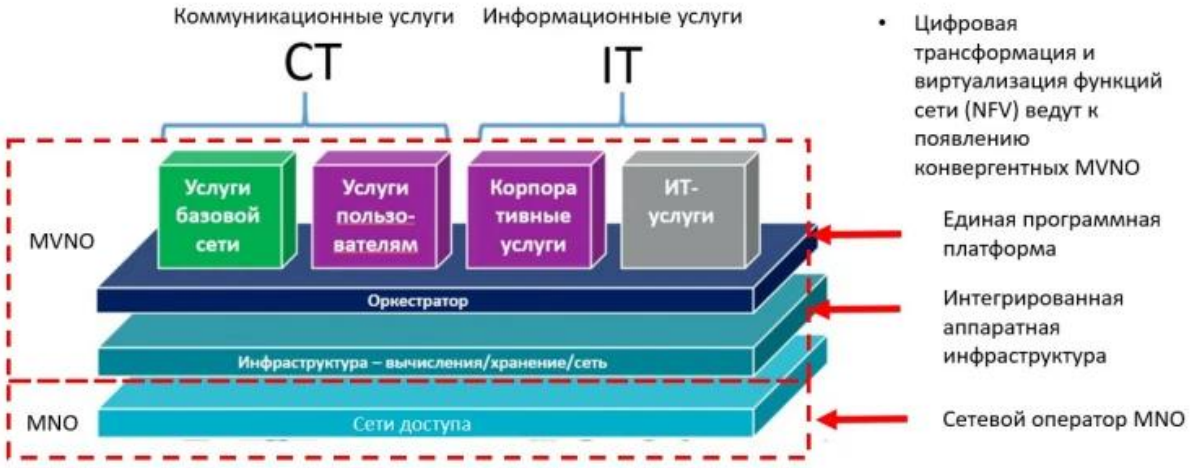


Рисунок 5.7. Архитектура конвергентного MVNO

Стандартное ИТ-оборудование называют COTS (Commercial Off The Shelf). Сети операторов могут строиться на общедоступном оборудовании, ко-

торое применяется во всех ИТ-системах, в том числе на корпоративных сетях предприятий.

Таким образом, за счет стандартизации и унификации сетевого оборудования появляется возможность построения как корпоративной сети (ИТ), так и сети связи общего пользования (СТ), на единой технологической основе [120]. За счет этого достигается снижение затрат на создание и техническую эксплуатацию сети, а также увеличения количества услуг сети. Более того, данный метод построения конвергентного MVNO обеспечивает снижение времени разработки и вывода новых услуг на рынок (рисунок 5.7).

5.5. HCI: Гипер-конвергентная инфраструктура

Три стандартных компонента инфраструктуры (как для обычных операторов, так и виртуальных) – вычисления (server), хранение данных (storage) и сеть (network). Эти элементы могут быть построены как в виде раздельного оборудования в дата-центре, так и виде гипер-конвергентной инфраструктуры (Hyper-Converged Infrastructure, HCI) [120]. В последнем случае конвергенции подвергается архитектура сети на основе технологии NFV, а также слой инфраструктуры (рисунок 5.5.1), и именно поэтому речь идет о гипер-конвергентности.

Рисунок 5.8. Гипер-конвергентная инфраструктура

Тип гипер-конвергентной инфраструктуры HCI преобладает при создании дата-центров и корпоративных сетей, а также при создании инфраструктуры операторов MNO/MVNO. Ее применение позволяет упростить строительство инфраструктуры, которая создается из «стандартных строительных блоков» и может увеличиваться в соответствии с потребностями [83].

Например, в случае классического MVNO «Газпром-Телеком» на начальном этапе SIM-карты были розданы лишь 5 тысячам абонентов из 450 тысяч планируемых. В то же время инфраструктура была предусмотрена сразу на большее количество абонентов, что привело к временному «замораживанию» инвестиций. В случае MVNO на базе HCI можно гибко увеличивать инфраструктуру согласно текущим потребностям и избежать нерациональных расходов [120].

5.6. Расширение услуг с помощью конвергентного MVNO

Конвергентный MVNO позволяет увеличить количество возможных услуг, предоставляемых операторам связи. Например, существуют конвергентные услуги унифицированной связи и коллективной работы UC&C (Unified Communication & Collaboration) [120]. Если широко известная услуга FMC представляет собой гибрид между фиксированной и мобильной связью (например, в зоне Wi-Fi сотовый телефон может выполнять роль фиксированного), то услуга UC&C может предоставить гораздо больший функционал (рисунок 5.9).

5.9. Рисунок 5.6.1. Спектр сервисов UC&C

Фактически UC&C предоставляет все услуги корпоративной сети для офисной работы на единой платформе. Рассмотрим некоторые из них.

Электронная почта с реализацией сервиса Click2Dial: если в письме есть номер телефона, есть возможность начать голосовой вызов с рабочего телефона. Если абонент отсутствует, вызов будет автоматически переадресован на его мобильный телефон. В противном случае можно оставить голосовое или текстовое сообщение, которое можно просмотреть на всех типах устройств: рабочем или мобильном телефоне, ноутбуке, планшете или компьютере [120].

Аудио-конференция, которая позволяет собрать телефонное совещание, выбрав участников из корпоративной базы данных.

Видеоконференция. Сотрудникам на рабочем месте доступны все инструменты для совещаний: доска, презентации, возможность коллективной работы над документами. Данная услуга помогает значительно сократить расходы компаний на организацию встреч, конференций и деловых поездок.

Сервис мобильности позволяет сотрудникам работать удаленно и предоставляет им доступ к корпоративным сетевым услугам через защищенный канал VPN, обеспечиваемый единой платформой безопасности.

Услуги видеонаблюдения – **VSaaS** (Video Surveillance as a Service). Традиционные способы построения систем видеонаблюдения предусматривают либо установку серверов хранения и анализа видеоизображений на предприятии – DVR/NVR, либо использование программного обеспечения для управления видео VMS (Video Management Software). Видео должно накапливаться и анализироваться на серверах, установленных на предприятии, с возможностью просмотра требуемых фрагментов через Интернет на устройствах уполномоченного персонала. Благодаря облачному видеонаблюдению VSaaS (рисунок 5.10) в компании устанавливаются только видеокамеры, которые подключаются к платформе конвергентного MVNO по каналам мобильной сети. Это значительно снижает расходы на развертывание системы видеонаблюдения.

Рисунок 5.10. Услуга облачного видеонаблюдения VSaaS в конвергентном MVNO

Система поддержки бизнеса как услуга – **BSSaaS** (Business Support System-as-a-Service) (рисунок 5.11).

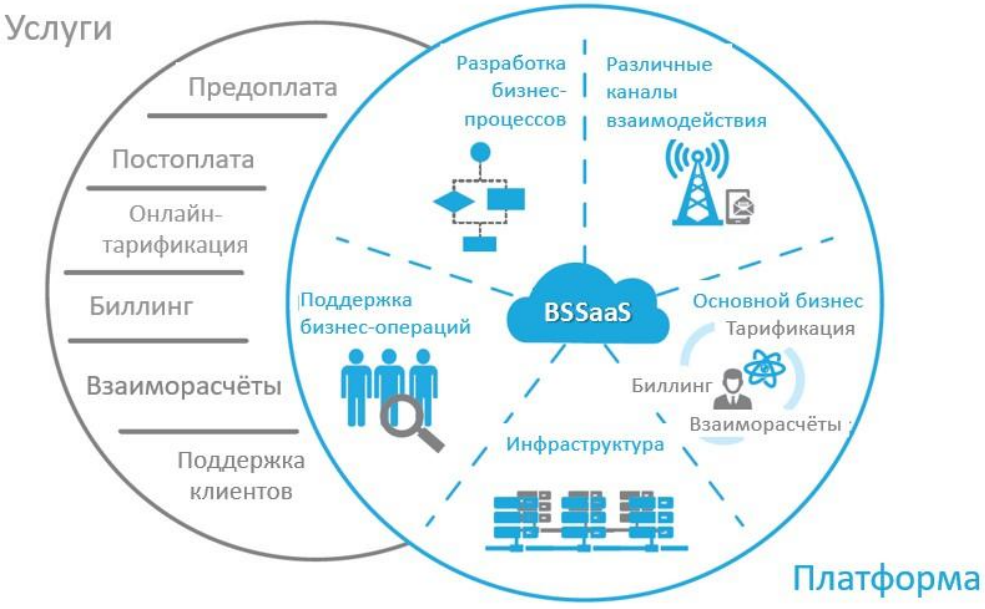


Рисунок 5.11. Услуги BSSaaS

Это важная часть организационной структуры операторов, как MNO, так и MVNO. В классическом MVNO «Газпром-телеком» система BSS арендуется у одного из базовых операторов (МТС, Вымпелком, МегаФон) [120]. Вывод собственной BSS в облако конвергентного MVNO дает возможность достичь существенной экономии операционных расходов бизнеса компании [101].

«Безопасность как услуга» – SECaaS (Security-as-a-Service). Информационная безопасность в конвергентном MVNO может быть обеспечена централизованно на единой платформе SECaaS (рисунок 5.12). Это повышает уровень защиты корпоративных пользователей, дочерних компаний и филиалов, а также внешних пользователей услуг связи и сети Интернет [120].

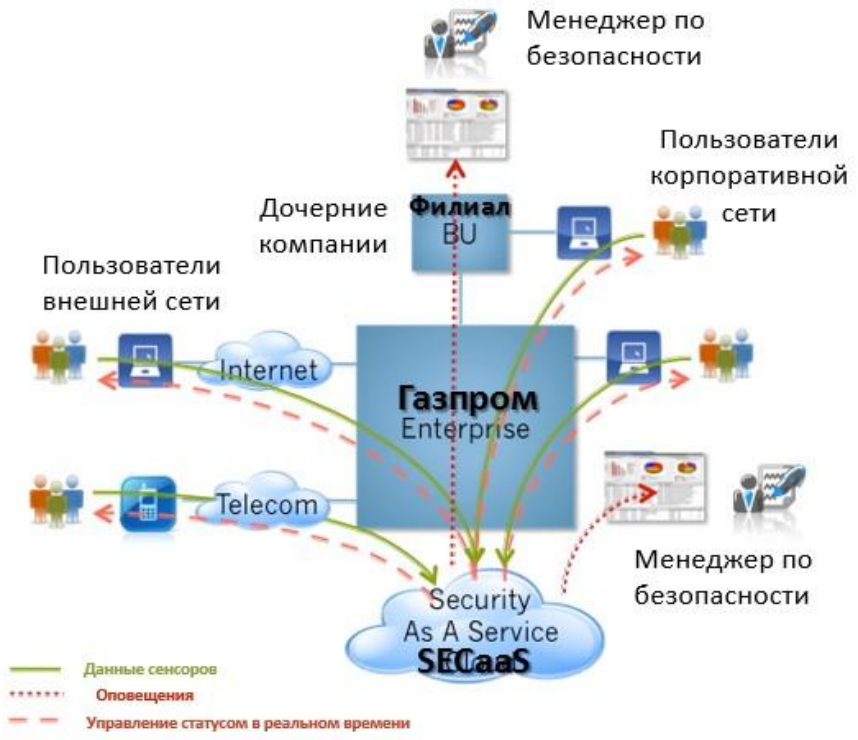


Рисунок 5.12. Услуга SECaaS в конвергентном MVNO

Программные клиент-сенсоры устанавливаются на всех устройствах пользователей MVNO, чтобы оповещать платформу SECaaS о любых подозрительных действиях пользователей или обнаружении внешних угроз безопасности и целостности данных. Сводные данные отображаются на объектах руководителей службы безопасности головного и дочерних предприятий [101]. Состоянием пользовательского устройства можно управлять в режиме реального времени, например, удаленно включать антивирусную проверку при появлении подозрительных данных на устройстве пользователя или блокировать доступ к опасным или нежелательным ресурсам, а также устанавливать права доступа к различным доменам корпоративной сети для пользователей с различным статусом.

Услуги профессиональной мобильной радиосвязи (ПМР) eLTE. Технология eLTE обеспечивает возможность беспроводной широкополосной передачи данных с пиковой скоростью 50 Мбит/с из сети и 20 Мбит/с в сеть при полосе 5, 10 и 15 МГц [120]. Система рассчитана для применения в вертикальных отраслях, таких как госорганы, транспорт, электроэнергетика, добыча и переработка полезных ископаемых, крупные предприятия и так далее. Кроме того, возможно применение eLTE в индустриальном Интернете вещей (IIoT).

Основные услуги, предоставляемые eLTE: видеонаблюдение, широкополосная передача данных, видеоконференцсвязь, геоинформационные системы, мобильные системы для экстренной связи в чрезвычайных ситуациях, широкополосный транкинг с возможностью видеосвязи [6, 120].

В диапазоне 400 МГц eLTE обеспечивает дальность связи почти до 20 км. В проекте для нефтедобывающих платформ норвежской нефтяной компании Tampnet в Северном море была обеспечена дальность связи до 40 км для голоса и передачи данных на скорости 1 Мбит/с (рисунок 5.13).

Рисунок 5.13. Применение ПМР eLTE в нефтедобывающей компании Tampnet

Для оперативного создания сети eLTE в местах проведения массовых мероприятий, в случаях стихийных бедствий и других экстренных ситуациях создана высокомобильная версия eLTE Rapid. Ее можно развернуть в течение нескольких часов или даже минут, а базовый комплект оборудования можно перевезти на легковом автомобиле или перенести в нескольких рюкзаках [120].

5.7. Базовая станция сотового оператора MVNO

Такие устройства, как смартфоны и планшеты, имеют постоянное подключение к радиовышке, которое происходит по определенному алгоритму – электронная система отправляет запрос на станцию о выделении своего мобильного/интернет-канала связи и ждет ответа коммутатора, который соединяет с нужным телефоном или обеспечивает доступ в Интернет [59].

Сама станция имеет конструкцию, которая включает вышки связи со сверхмощными антеннами. Типичная конструкция включает несколько антенн, каждая из которых осуществляет покрытие в 120С. Ее радиомодуль – еще одна

часть установки, которая связывает антенну с вышкой при помощи кабеля. Система осуществляет передачу информации при помощи двоичного кода, передавая ее в ядро, где она обрабатывается и отправляется на нужный сайт.

Существует несколько вариаций базовых станций, одна из которых – высокочастотная система MVNO. Как и любая сложная установка, MVNO имеет свои конфигурации, четыре из которых – это системы базовых станций, внедряющиеся преимущественно в зонах обслуживания базовых станций.

Фемтосота. Небольшая конструкция, имеющая габариты стандартного Wi-Fi приемника. Представляет собой точку доступа, которая рекомендована к приобретению частным лицам или индивидуальным предпринимателям, не имеющим отношение к операторам сотовой связи.

Пикосота. Установка, имеющая небольшую мощность. Ее можно интегрировать как универсальную систему под IP-телефонию, преимущественно на территории скопления пользователей.

Макросота. Стандартная система, которая вводится для создания цепочки мобильных сетей. Имеет достаточно большой радиус покрытия, отличается возможностью соединения с несколькими разновидностями базовых станций.

Микросота. Базовая станция, которая устанавливается для небольшого количества пользователей, так как она имеет минимальный радиус покрытия.

Таким образом, система MVNO является связующей частью цепочки «Абонент – оператор сотовой связи», благодаря которой реселлер MVNO получает необходимую среду для работы, а также оптимизацию расходов [59]. Имея подключение к базовой станции, пользователь получает следующие преимущества:

- минимальные финансовые затраты – используя базовую станцию, пользователь получает возможность сэкономить сумму, которую в перспективе можно потратить на другие отделы компании, например маркетинг;
- возможность использования в любых доступных регионах – хотя не все зоны в РФ и других странах имеют высокоскоростное покрытие, но при наличии станции оператора в регионе инженер может осуществлять свою работу по подписке;
- высокая безопасность и работоспособность – ответственность за работу возлагается на самого оператора, так как в его обязанности входит обеспечение бесперебойной работы и обслуживание базовых станций;
- легкость интеграции – установить модель можно без особых усилий, ведь заказчик при интеграции системы получает готовую к работе установку.

5.8. Перспективы развития виртуальных операторов связи в России

К концу 2020 года в России стало около 12 млн абонентов виртуальных мобильных операторов. Это примерно на 15% больше, чем годом ранее. Об этом свидетельствуют данные «ТМТ Консалтинг» [31] (рисунок 5.14).

На проекты MVNO в 2020 году пришлось не менее 5% всей базы абонентов мобильной связи в России против 4% в 2019 году. Если число клиентов виртуальных операторов ощутимо выросло, то объем всего рынка (с точки зрения количества абонентов) опустился на 4%.

Рост в сегменте MVNO эксперты связывают с банковскими проектами, доля которых за год выросла с 15% до 20%. Крупнейшим среди них остается «Тинькофф Мобайл», а также «СберМобайл».

Рисунок 5.14. Динамика абонентской базы MVNO и структура рынка MVNO, 2020 год

Также продолжили свое развитие более опытные операторские проекты, на которые по итогам года по-прежнему приходится три четверти рынка. Лидером остается Yota, которая контролирует более половины рынка MVNO. После нее идет «Ростелеком» с долей в размере 16%, а лидирующую тройку замкнул «Тинькофф Мобайл» (7%). В топ-5 также вошли «Сбермобайл» и МГТС [31].

По словам аналитиков, структура российских виртуальных мобильных операторов по типам клиентов в целом отражает структуру всего рынка мобильной связи. Основу его составляют частные пользователи, на них приходится 92% всех абонентов виртуальных операторов. Как и на рынке в целом, лидером здесь является Yota. В сегменте бизнес-клиентов крупнейший MVNO – «Ростелеком», на компанию приходится половина всех корпоративных абонентов виртуальных операторов.

5.9. Перспективы MVNO в зарубежных странах

В Европе и США количество виртуальных операторов связи исчисляется десятками, число их абонентов – миллионами человек, бюджет – миллиардами долларов. В одной только Великобритании услуги оказывают 87 виртуальных операторов, в Штатах – 73. По данным GSMA Intelligence, количество действующих MVNO по всему миру превышает 1,2 тыс [76].

Только за последние пару лет появились десятки MVNO-проектов – от виртуальных операторов футбольных клубов в Бразилии и Испании, кофейного сообщества Tchibo до MVNO с криптокошельком внутри экосистемы и другими финансовыми сервисами.

MVNO появились на Западе задолго до того, как это произошло в России. Регуляторы подготовили нормативную базу для успешного развития сектора MVNO намного раньше, чем это было сделано в России. На Западе много компаний-агрегаторов: для них создание MVNO – отдельный бизнес, который они поставили на поток.

Западные MVNO создали достаточно востребованные продукты для различных целевых аудиторий.

К примеру, американский Tracfone начинал как оператор для мексиканских мигрантов – компания соединила мексиканцев, которые жили в Штатах, с их друзьями, оставшимися на родине. С тех пор Tracfone привлек 26 млн абонентов и стал виртуальным оператором, который сам запускает новые MVNO-проекты для других сегментов. В ноябре 2020 года за $6,9 млрд компанию Tracfone приобрел Verizon, крупнейший оператор мобильной связи США.

Британский MVNO-проект GiffGaff ориентируется на молодежь. Пользователям из поколения Z он предлагает недорогую связь и мобильный интернет. После запуска в 2009 году GiffGaff ввел пакетные тарифы, которые состояли из набора минут, SMS, дата-трафика и назывались «коробками с подарками» (от англ. goody bags). Идея таких пакетов возникла на форумах сообщества проекта. Позже появились «коробки», включающие в себя только мобильный интернет.

Tesco Mobile – еще один успешный британский виртуальный оператор. Его запустила популярная торговая сеть Tesco. MVNO-проект работает в четырех странах, количество его клиентов только в Великобритании превышает 4 млн [76].

В 2022 году мировой рынок мобильных виртуальных сетей (MVNO) оценивается в 54,1 млрд долларов США. Ожидается, что в течение прогнозируемого периода среднегодовой темп роста рынка составит 8,8% [19]. В мире насчитывается около 1000 MVNO, которые в совокупности составляют около 10% от общего числа мобильных пользователей. Крупные операторы мобильной связи, такие как T-Mobile и Verizon, выбирают MVNO для оптовой продажи дополнительных мощностей по оптовым ценам, которые вместо этого остаются неиспользованными и помогают покрыть риск убытков. Потребность в более дешевых тарифах на услуги усиливает конкуренцию среди поставщиков услуг, которые вынуждены рассматривать MVNO как один из вариантов привлечения виртуальных клиентов. Ожидается, что появление M2M, облачных и мобильных денег в сочетании с ростом скорости использования данных увеличит спрос на MVNO.

Увеличение числа абонентов мобильной сети и растущее проникновение мобильных устройств мотивирует рынок. Количество абонентов мобильной связи по всему миру значительно выросло. Это связано с тем, что все больше потребителей выбирают устройства с выходом в интернет [67, 69]. Одним из са-

мых востребованных устройств связи является смартфон. Смартфоны очень важны из-за возможностей подключения, которые они обеспечивают. Количество смартфонов, используемых на международном уровне, относительно велико по сравнению с другими устройствами для подключения. Количество продаваемых смартфонов/мобильных устройств увеличивается, что приводит к увеличению количества подписок на мобильные сети, поскольку устройства для подключения не могут работать без подписок. Согласно прогнозу Zenith по мобильной рекламе, число владельцев смартфонов увеличится на 7% в 2022 году [19]. Ожидается, что растущее внедрение устройств подключения и растущее проникновение мобильных устройств приведут к значительному увеличению числа абонентов мобильной сети, что, в свою очередь, стимулирует рост мирового рынка MVNO.

Также ожидается, что тип реселлера будет доминировать на рынке. MVNO предлагает собственные услуги с добавленной стоимостью или не имеет активов в партнерстве с оператором мобильной связи в сегменте посредников. Помимо этого, реселлеры не получают никаких прав собственности на клиента, инфраструктуру или SIM-карты. Реселлеры не дают MVNO возможности фиксировать стоимость. Они позволяют MVNO получать прибыль от работы под собственным брендом. Торговый посредник несет ответственность за расходы на брендинг, продажи, распространение и распределение доходов с партнерским оператором мобильной связи. Однако операторы услуг могут фиксировать затраты независимо от затрат, устанавливаемых операторами мобильной связи [67, 69].

Полноценные MVNO получают прибыль, связанную с владением инфраструктурой сетевой коммутации. Общая прибыль, полученная торговыми посредниками, оценивается менее чем в 10%, а прибыль, полученная поставщиками услуг, оценивается примерно в 10–15%. В этой конкурентной среде поставщики услуг уделяют больше внимания торговым посредникам, чтобы привлечь больше виртуальных клиентов, тем самым поддерживая значительный рост реселлеров.

На мировом рынке MVNO предполагается рост MVNO в Европе, за ней в 2022 году последует Азиатско-Тихоокеанский регион и Северная Америка [19]. В Европе было несколько запусков продуктов, слияний и поглощений, чтобы воспользоваться этой возможностью. Основной движущей силой инвестиций стало постоянное развитие и применение передовых технологий для освоения огромных объемов, ранее считавшихся некоммерческими. Благодаря этой серии инвестиций в сегменты розничной торговли, скидкам и приложениям для мигрантов в Европе рынок в регионе готов к значительному росту в течение прогнозируемого периода.

5.10. Будущее IoT-MVNO

На фоне общего снижения темпов роста доходов от традиционных услуг мобильной связи, таких как телефония и Интернет, операторам приходится осваивать новые ниши. Одним из таких перспективных рынков является Интернет

вещей (IoT). Потенциал глобального рынка Интернетавещей составляет около 2 млрд долларов [117].

В результате опроса, проведенного TMForum – международной организацией, которая занимается вопросами развития и оптимизации бизнеса операторов связи, эксперты отрасли пришли к единому мнению: сейчас MVNO стоит задуматься о реализации IoT. Вовлечение MVNE позволяет виртуальным мобильным операторам освоить перспективные ниши, к которым относится IoT, гораздо быстрее и эффективнее.

Например, компания Plintron, являющаяся крупнейшим международным провайдером и агрегатором мобильной виртуальной сети (MVNE/MVNA), запустила IoT проект еще в 2016 году [117] и наблюдает повышенный интерес к этой технологии среди MVNO во всем мире.

Эксперты из TMForum считают, что IoT сначала будет успешен на опытных рынках США, Европы, Юго-Восточной Азии и Китая. При этом стратегия продвижения IoT будет в каждой стране отличаться. Более того, традиционное ценообразование как совокупность различных опций в IoT работать не будет.

IoT – совершенно другой рынок, значительно сложнее и фрагментированнее, чем голосовые услуги и передача данных. Большинство финансовых возможностей будет лежать в плоскости B2B, а не B2C [66].

Планируется, что к 2025 году количество IoT/M2M-устройств в России вырастет до 40,8 млн [66]. При этом наиболее емкими по-прежнему останутся такие сегменты, как транспорт, ЖКХ и энергетика. Согласно прогнозам аналитиков, отечественный рынок мониторинга и управления коммерческим автопарком вырастет в ближайшие пять лет более чем в два раза: с 8 млн устройств в 2019 до 18,5 млн – в 2025 г. Потенциал рынка IoT-устройств для ЖКХ и энергетики оценивается в 7,5 млн единиц, что стало возможным благодаря обязательному внедрению технологии smart metering (интеллектуальный учет электроэнергии) и технологии SmartGrid («умные» сети).

Резюме

В данном разделе был проведен обзор понятия виртуальных операторов связи, приведена их классификация, разобраны основы их построения, функционирования, а также рассмотрены перспективы развития виртуальных операторов связи в России и за рубежом.

Можно сделать вывод, что виртуальные операторы связи – это подающая большие надежды область телекоммуникационных технологий. Активно растущий темп внедрения виртуальных операторов связи показывает их популярность как среди абонентов, так и среди компаний, предоставляющих телекоммуникационные услуги. Различная вариация типов виртуальных операторов связи предоставляет компаниям выбор условий сотрудничества с реальными операторами связи. Выгода от отсутствия необходимости разворачивать сетевую инфраструктуру дает возможность виртуальным операторам обеспечивать абонентов услу-

гами связи по хорошей цене и сфокусироваться на улучшении предоставляемых функций своим клиентам.

Также большое развитие получило направление конвергенции различных типов сетей на единой технологической основе, что значительно расширило возможности предоставляемых услуг виртуальных операторов связи, которые ранее создавались на раздельной основе. Это повысило интерес к виртуальным операторам и дало большую площадку для их роста и развития.

Важно подчеркнуть, что с ежегодным увеличением количества устройств, использующих Интернет-соединение, необходимость в виртуальных операторах связи будет только расти.

Вопросы для самопроверки

1. Как Вы понимаете термин «Mobile Virtual Network Operator (MVNO)»?
2. На чем основана классификация виртуальных операторов сотовой связи?
3. В чем состоит архитектура «полного MVNO»?
4. Каково содержание типовой схемы связи MNO и MVNO?
5. Корректен ли сегодня термин «Конвергентный MVNO»? Как Вы его понимаете?
6. Из чего состоит и для чего применяется Commercial Off The Shelf?
7. Корректен ли термин «Hyper-Converged Infrastructure (HCI)»? Как Вы его понимаете?
8. В чем заключается спектр сервисов UC&C?
9. Из чего состоят услуги BSSaaS?
10. Можете ли Вы определить и обосновать перспективы развития виртуальных операторов связи?
11. Можете ли Вы определить и обосновать перспективы развития технологий IoT-MVNO?

Раздел 6. ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ВИРТУАЛЬНЫМ ОПЕРАТОРОМ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ IP-ТЕЛЕФОНИИ

6.1. Основные виды угроз

С развитием интернет-связи, в частность стека TCP-IP, появились и возможности развертывания голосовой связи поверх IP, для которой вопрос безопасности и конфиденциальности встает все более и более остро. Сегодня обеспечение безопасности является наиболее важным аспектом при создании качественного VOIP сервиса [77, 90].

Основной задачей обеспечения безопасности является защита информации от различного вида угроз с целью сохранности передаваемой информации. В процессе обмена информацией угрозы могут появиться на различных этапах [36].

Самый уязвимый из них – момент первичного обмена ключами. В процессе передачи обмена ключами на систему могут быть совершены различного рода атаки. Злоумышленник может тайно изменять информацию между двумя сторонами, подменять ее или прослушивать [52].

Поэтому протокол, обеспечивающий безопасность, должен предоставлять различные методы и средства защиты от такого рода атак [36]. Для рассматриваемых протоколов предполагается использование алгоритма Диффи-Хеллмана для передачи и обмена ключами с методами двусторонней аутентификации [49]. В этом случае протокол сможет противостоять вышеперечисленным угрозам, а значит, обеспечить конфиденциальную связь. В рассматриваемых протоколах для передачи предполагается только частичная информация, которая служит для получения генератора сеансового ключа. Это позволяет избежать излишней нагрузки на устройства и сеть. К тому же передаются и другие данные, такие как временные метки, случайные или псевдослучайные значения, идентификационная информация или различные политики безопасности, а прослушивание таких данных не несет существенные риски для безопасности.

6.1.1. Атака «человек посередине»

Основополагающей для всех атак является вид атаки, предполагающий существование возможности нахождения вредоносного узла между участникаи информационного обмена. Наиболее известным и общим является атака, называемая «man in the middle» («человек посередине»). «Человек посередине» (рисунок 6.1) – наиболее часто встречаемая уязвимость телефонных сетей, особенно опасная для IP-телефонии. В случае применения IP-телефонии злоумышленнику не нужен физический доступ к линии передачи данных. Находящееся внутри корпоративной сети устройство перехвата, скорее всего, может быть обнаружено, но внешнее прослушивание отследить практически невозможно. Кроме того, перехваченные данные или голос могут быть переданы далее с из-

менениями. В таких условиях весь незашифрованный голосовой поток необходимо считать небезопасным [17].

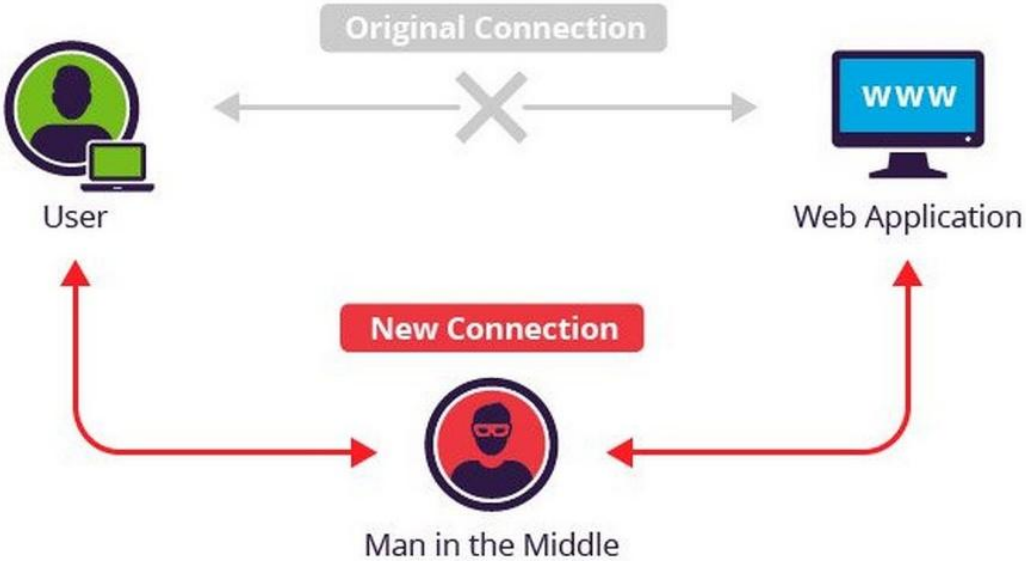


Рисунок 6.1. Иллюстрация концепции атаки “человек посередине”

6.1.2. Подмена и взлом пользовательских данных

Подмена и взлом данных – еще одна разновидность атак. Она наиболее опасна для систем, однако и требует некоторой подготовки. В частности, для получения ключей может быть использована ранее рассмотренная атака «человек посередине».

Отказ от использования или упрощение механизмов аутентификации и авторизации в IP-телефонии открывает для злоумышленника возможность несанкционированно получить доступ к системе, подменив данные о пользователе своими [17]. Возможен также взлом учетных данных пользователей посредством перебора или прослушивания незащищенных каналов связи. Подобная уязвимость может быть использована для совершения дорогостоящих звонков за счет жертвы, сводя на нет всю возможную выгоду от использования IP-телефонии. Также эта брешь в безопасности может применяться для записи перехваченных звонков на носители злоумышленника с целью применения данной информации в корыстных целях [49].

6.2. Основные технологии и протоколы

Для обеспечения безопасности и конфиденциальности связи, а также противодействию злоумышленников разработаны различные системы и протоколы, которые, по отдельности и в комбинации, решают следующие задачи: непосредственное шифрование данных, обмен первичной информацией и аутентификация, а также защита канала связи [77, 90]. Защита канала связи является общей задачей для любых IP-сетей, включая и VOIP, и типовым решением здесь служит создание VPN-сети поверх общей IP-сети [51]. В данном разделе рассматриваются специфичные для VOIP решения для обеспечения безопасности и конфиденциальности связи – как стандартные, так и новаторские и перспективные.

6.2.1. Протокол шифрования данных SRTP

Протокол SRTP применяется для обеспечения шифрования данных, начиная с 2004 года и до сегодняшнего дня.

SRTP (Secure Real-time Transport Protocol, безопасный протокол передачи данных в реальном времени) определяет профиль RTP (Real-time Transport Protocol, транспортный протокол в реальном времени) и предназначен для шифрования, установления подлинности сообщения, целостности, защиты от замены данных RTP в однонаправленных и multicast передачах медиа и приложениях [52]. Данный протокол был разработан командой экспертов по безопасности IP протоколов компаний Cisco и Ericsson и других компаний и был впервые опубликован в IETF в марте 2004 как RFC 3711 [21]. Так как RTP тесно связан с RTCP, то RTCP может использоваться, чтобы управлять сессией RTP. У SRTP также есть родственный протокол, названный Secure RTCP, или SRTCP. SRTCP обеспечивает функции, связанные с безопасностью в RTCP, для той же функциональности SRTP в RTP. Использование SRTP или SRTCP не является обязательным при использовании RTP или RTCP. Поэтому при использовании SRTP/SRTCP все дополнительные возможности, такие как шифрование и установление подлинности, являются опциональными и могут быть включены или выключены. Единственное исключение – функция аутентификации сообщений, которая обязательна при использовании SRTP [21].

Для шифрования медиапотока (в целях конфиденциальности голосового соединения) SRTP (вместе с SRTCP) стандартизирует использование только единственного шифра. Далее кратко описывается основной протокол шифрования – AES. Данный протокол может использоваться в двух режимах, превращающих изначально блочный шифр AES в потоковый шифр. Принцип работы SRTP и встроенного AES проиллюстрирован на рисунке 6.2, а устройство пакета SRTP – на рисунке 6.3.

Сегментированный целочисленный счетчик – типичный режим, который осуществляет произвольный доступ к любым блокам. Это существенно для трафика RTP, передающегося в публичных сетях с непредсказуемым уровнем надежности и возможной потерей пакетов. В общем случае почти любая функция может использоваться в роли «счетчика», предполагая, что эта функция не повторяется для большого числа итераций. Но стандарт для шифрования данных RTP – только обычное целочисленное значение счетчика. AES, работающий в этом режиме, является алгоритмом шифрования по умолчанию, с длиной шифровального ключа по умолчанию в 128 бит и ключом сессии длиной в 112 бит [52].

f8-режим – вариант режима способа обратной связи, расширенного для доступа с измененной функцией инициализации. Значения по умолчанию для шифровального ключа и ключа сессии – то же, что и в AES в режиме, описаном выше. (AES, работающий в этом режиме, был выбран для использования в мобильных сетях 3G UMTS.)

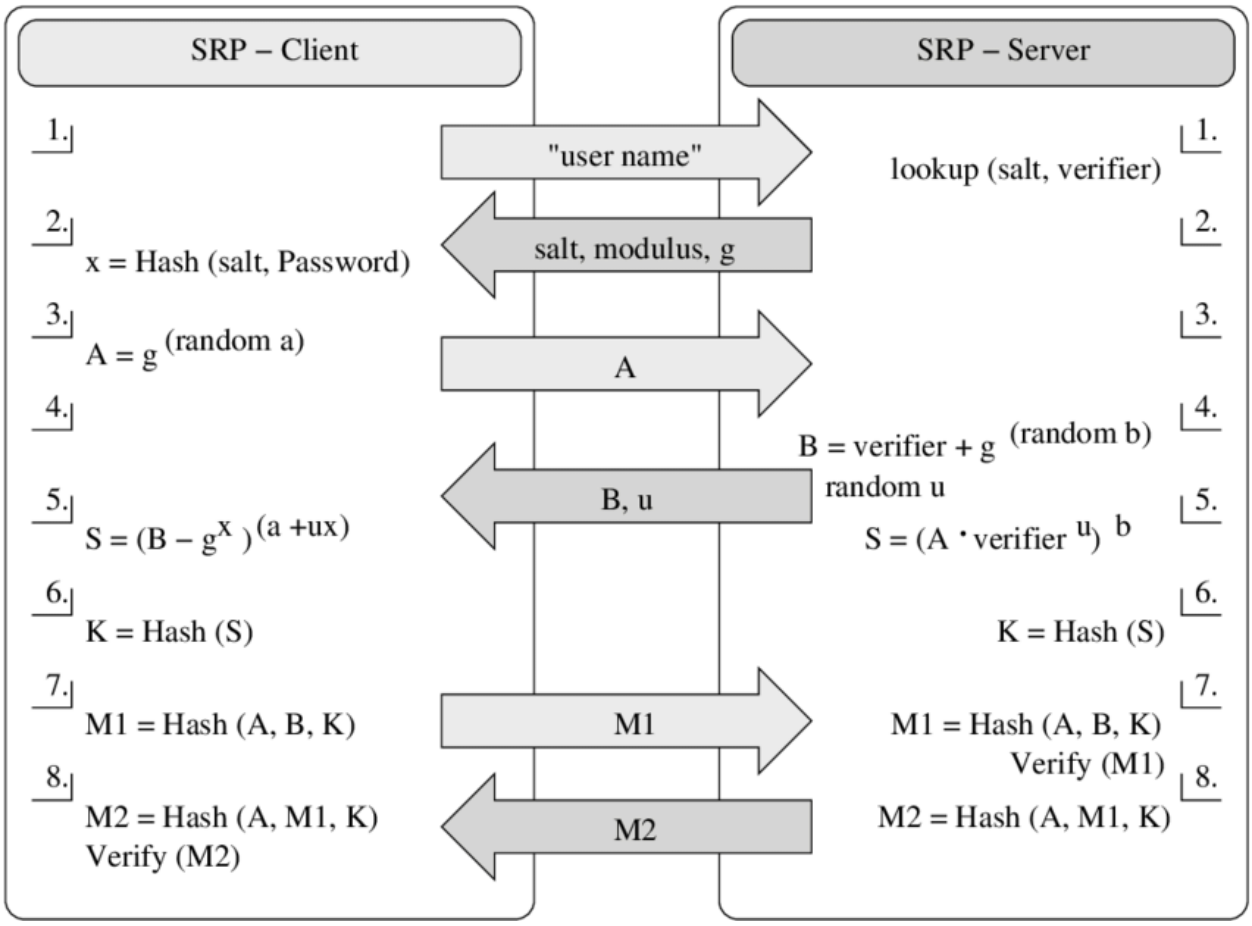


Рисунок 6.2. Принцип работы SRTP и встроенного AES

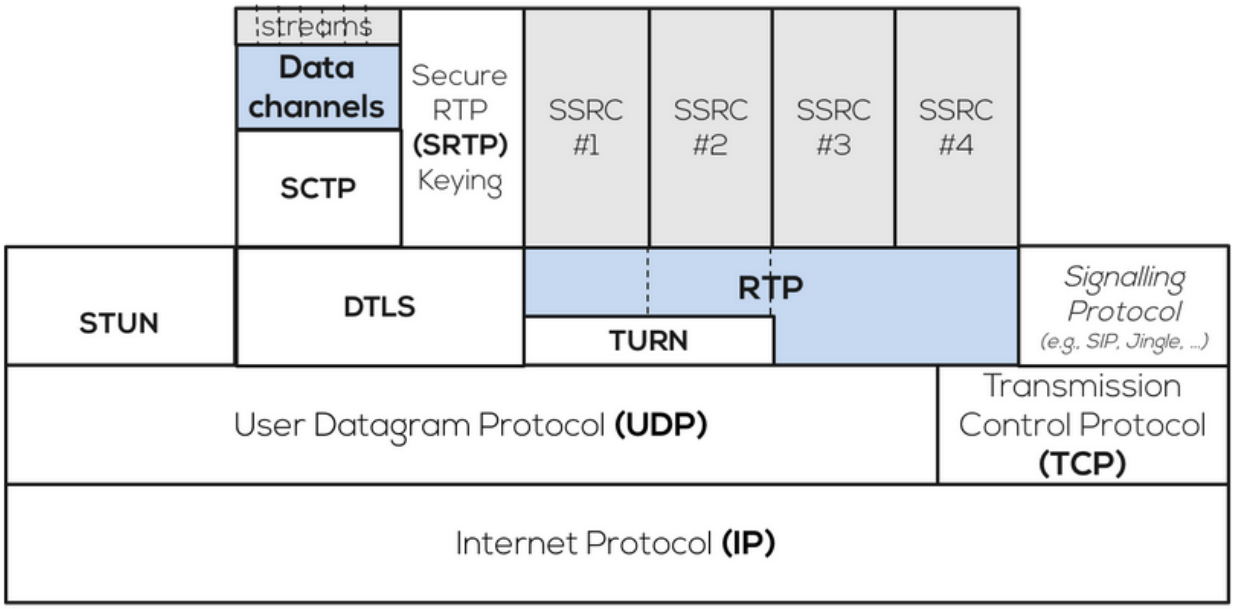


Рисунок 6.3. Устройство пакета SRTP

Помимо шифра AES, SRTP поддерживает прямое шифрование, используя так называемый «пустой шифр», который может быть принят как второй поддерживаемый шифр (или третий режим шифрования в дополнение к описаным

двум выше). Фактически, пустой шифр не выполняет шифрования (то есть алгоритм шифрования работает так, как если бы ключевой поток содержал только нули) и копирует входной поток в выходной без изменений. Это обязательная особенность для SRTP, отличающая SRTP от RTP [49].

Технически в SRTP можно легко встраивать новые алгоритмы шифрования, стандарт SRTP лишь заявляет, что, в отличие от RTP, он дополнительно объявляет, что данный протокол зашифрован, внося информацию в заголовок пакета, а также указывает контрольные суммы для проверки целостности [49]. Это означает, что SRTP как протокол может быть отдельно реализован или модифицирован независимой командой, однако тогда шифрование и первичный обмен ключами также ложится на разработчиков. При этом для общей реализации SRTP использует стандартное шифрование AES. Единственный юридически легальный способ добавить новый алгоритм шифрования для совместимости со стандартом SRTP состоит в том, чтобы опубликовать новый стандарт RFC, где должно быть ясно определено использование нового алгоритма.

Также SRTP никак не описывает процесс обмена ключами и полагается на сторонние протоколы, такие как ZRTP или MIKEY [52], или вообще входит в общий мультимедийный протокол SIP.

Подводя краткий вывод, можно констатировать, что SRTP является весьма свободным для интерпретации протоколом, что позволяет использовать его в различных отраслях помимо VOIP, например IOT или другие потоковые данные. Потенциал для модификации SRTP огромен, поэтому он является одним из основных протоколов даже спустя 18 лет после своего появления. Однако недостатком SRTP является уязвимая система аутентификации абонентов [79, 80, 103].

В целом первичный обмен информацией и ключами для шифрования – самое уязвимое место в VOIP сетях. На сегодняшний день существует большое число протоколов, предоставляющих безопасный обмен ключами по незащищенным каналам [52]. Однако для VOIP наиболее распространены и считаются удобными протоколы ZRTP, MIKEY и SIP, которые можно использовать как сервисные протоколы для SRTP. Они позволяют модифицировать аутентификацию SRTP таким образом, что программные решения, которые раньше работали с SRTP, не требуют изменений, а аутентификация становится надежнее.

6.2.2. Протокол аутентификации ZRTP

ZRTP – криптографический протокол согласования ключей шифрования, используемый в системах передачи голоса по IP-сетям (VoIP). ZRTP описывает метод получения ключей по алгоритму Диффи–Хелмана для организации Secure Real-time Transport Protocol (SRTP). ZRTP осуществляет согласование ключей в том же потоке RTP, по которому установлена аудио/видео связь, то есть не требует отдельного канала связи.

ZRTP разработан Филипом Циммерманом (Phil Zimmermann), Джоном Калласом (Jon Callas) и Аланом Джонстоном (Alan Johnston) в 2006 году. Описание протокола было подано в IETF 5 марта 2006 [56].

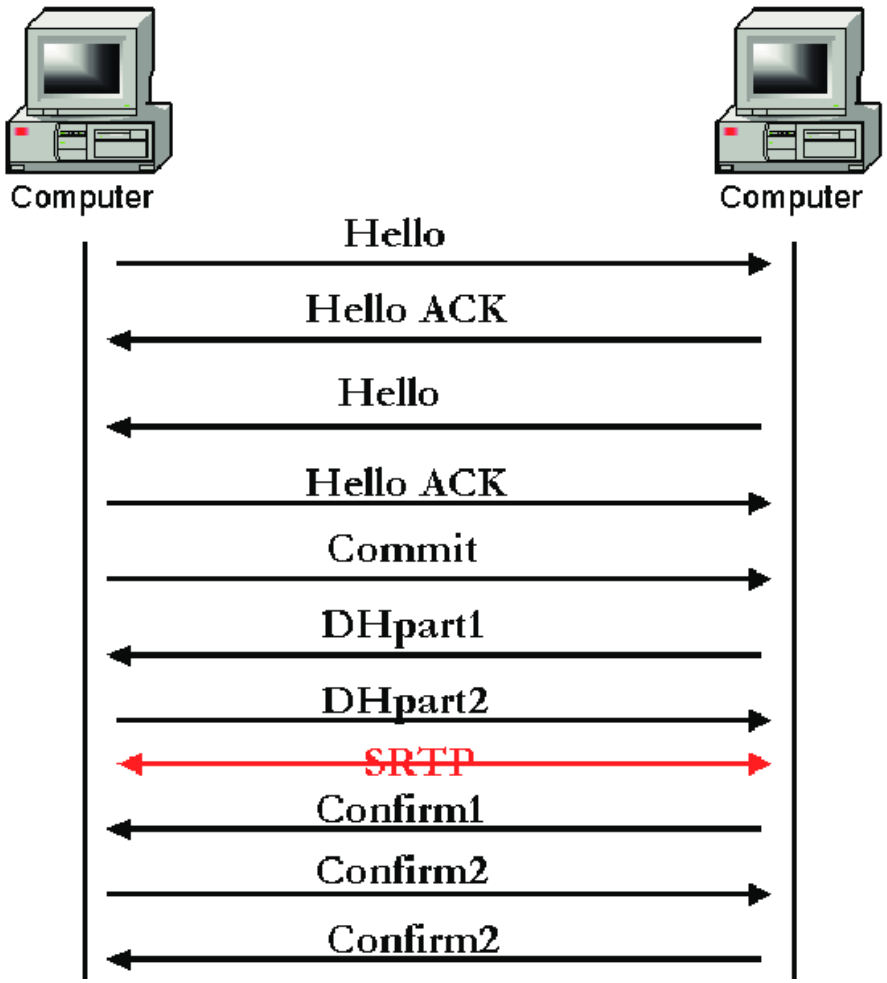


Рисунок 6.4. Порядок пакетов установления связи по ZRTP

На рисунке 6.4 стрелками условно изображены процедуры установления связи и обменами сообщениями между компьютерами пользователей в вычислительной сети, предусмотренное протоколом ZRTP.

ZRTP предлагается как способ согласования ключей шифрования с использованием метода Диффи–Хеллмана через медиапоток, устанавливаемый протоколом RTP (Real-time Transport Protocol), который образуется после инициализации вызова, используя любой тип сигнализации, например Session Initiation Protocol (SIP). Во время посыла звонка создается публичный ИД, используемый при создании ключей, которыми будет шифроваться медиапоток разговора [57]. При этом ключ действителен только в течение одного разговора, образуя сессию Secure RTP (SRTP) [49]. При разрыве соединения ключ и весь криптографический контекст уничтожается, что обеспечивает совершенную прямую секретность [57]. Таким образом, существует потенциал встраивания этого механизма в уже существующие программные продукты, шлюзы и ИП телефоны [56].

Протокол не требует ни заранее сгенерированных ключей, ни поддержки инфраструктуры обмена ключей, ни центра сертификации. Это избавляет от сложностей создания структуры авторизации, основанной на доверенной под-

держке, которая, например, применяется в шифровании SSL или SIP, позволяет обеспечивать безопасность без усложнений и полностью перейти с RTP на SRTP без экономических потерь.

Главной целью протокола является организация шифрованного канала, использующего синхронные коды шифровки [57], независимо от того, какой вид связи будет использоваться впоследствии, будь то голосовая сессия или https соединение с интернет-банком. Основной угрозой, с которой борется данный протокол, является man-in-the middle. Противодействие этой угрозе осуществляется посредствам безопасного обмена шифрами и создания единой криптозащиты между любыми двумя точками в мире.

Теоретически ZRTP может применяться совместно с любыми сигнальными протоколами, использующими RTP для передачи медиа потока, включая SIP, H.323, SCCP, MGCP Unistim и Jingle, так как в теории ZRTP не зависит от сигнализации, осуществляя обмен ключей в медиа сессии RTP. Таким образом ZRTP может стать открытым стандартом де-факто в мире IP-телефонии [56].

6.2.3. Протокол аутентификации MIKEY

Еще один протокол, призванный создать защищенный канал между двумя хостами – MIKEY (Multimedia Internet KEYing). Использование MIKEY определено в RFC 3830. MIKEY – это протокол обмена ключами, разработанный специально для мультимедийных приложений, работающих в реальном времени, таких как передача потоковых аудиоданных. Он используется для обмена ключами для шифрования голосовых сессий протокола SRTP.

Мультимедийные приложения – это совокупность современных цифровых средств коммуникаций, которые позволяют одновременно передавать, получать и преобразовывать различного рода информацию (текстовую, графическую, аудиовизуальную). К мультимедийным приложениям можно, например, отнести IP-телефонию, которая представляет собой совокупность инфокоммуникационных протоколов с использованием различных сетевых технологий и методов, обеспечивающих стандартный для телефонии функционал (от набора номера абонента до установления двустороннего взаимодействия по каналу связи). Также к IP-телефонии можно отнести и видеоконференции (Skype, Cisco Jabber). В качестве основной технологии для организации двустороннего общения в IP-телефонии используется технология VoIP, которая обеспечивает установление и поддержание в работоспособном состоянии мультимедийное приложение.

Однако VoIP сталкивается с проблемами увеличения вероятности потери IP-пакетов при больших нагрузках, появлении джиттеров, что приводит к потере качества передачи в сети Интернет. Поэтому, чтобы организовать качественный доступ к сети, а также устранить ошибки следования пакетов, VoIP необходимо использовать QoS (Quality of Service). Обеспечение качества доставки, однако, оказывает сильное влияние на производительность системы. К тому же, если в сети применяются различные протоколы безопасной передачи данных, которые, в свою очередь, используют процедуру управления ключами, то данные прото-

колы также вносят свой вклад в уменьшение производительности системы передачи данных. Дополнительная нагрузка особенно проявляется у устройств, которые имеют ограниченную вычислительную мощность. Например, к ним относятся карманные устройства.

Хотя на сегодняшний день производительность и вычислительная мощность карманных устройств значительно улучшились, процесс организации жизненного цикла ключей, начиная с регистрации пользователя и заканчивая отменой ключа, остается ресурсоемкой задачей. Одним из протоколов обмена ключами для мультимедийных приложений выступает протокол MIKEY. Данный протокол был разработан с целью уменьшить задержки при обмене ключами между небольшими взаимодействующими группами, находящимися в гетерогенных сетях [30].

Возможность обмена ключами между группами является важным свойством протокола MIKEY. Так, например, в протоколе SDP присутствуют процедуры управления ключами (в сообщениях SDP опционально используется параметр, который отвечает за ключ шифрования), но в нем нет механизмов согласования ключей. MIKEY, в свою очередь, решает эту проблему.

К протоколу MIKEY удовлетворяет следующим требованиям [30]:

1. End-to-end шифрование. Это свойство гарантирует, что ключи шифрования известны только взаимодействующим сторонам, а также безопасную передачу данных между узлами. Однако данный вид шифрования уязвим для такого рода атак, как атака «человек посередине».
2. Простота в реализации.
3. Эффективность реализации. Протокол поддерживает низкое потребление полосы пропускания, малое количество использования системных ресурсов.
4. Независимость от функциональной безопасности: обмен ключами и корректное выполнение функций транспортного уровня, таких как, например, функции передачи данных без подтверждения приема, осуществляются независимо.
5. Интеграция с другими протоколами безопасной передачи данных. Протокол поддерживает возможность передавать служебные сообщения другим протоколам.

Такие протоколы безопасной передачи данных, как SRTP (Secure Real Time Protocol) и IPSec, используются для защиты передаваемой информации, шифрования, проверки подлинности передаваемой информации между мультимедийными приложениями, работающими в реальном времени. Основная проблема, которая лежит перед данными протоколами, – это то, что они не поддерживают встроенные механизмы обмена ключами. Для разрешения данной проблемы был разработан протокол MIKEY. На данный момент SRTP является единственным протоколом безопасной передачи данных, который полагается на протокол обмена ключами MIKEY для установления первичного ключа [49]. Что касается протокола IPSec/ESP, то он также поддерживает MIKEY, но для этого

нужно реализовать соответствующий функционал, который потом уже используется для взаимодействия протоколов.

Протокол MIKEY может использоваться в следующих режимах передачи данных:

– Unicast (один-к-одному)
– Multicast
– Многоранговая сеть (многие-ко-многим, без централизованного управления).

Также поддерживается режим многие-ко-многим с централизованным управлением. Обычно используется применительно к более широкой группе пользователей, которая требует координации обмена ключами. Чаще всего пользователи, используя мультимедийные приложения, взаимодействуют и общаются друг с другом в реальном времени. В таком случае можно сказать, что конечные узлы создают между собой мультимедийные сеансы. Мультимедийный сеанс, в свою очередь, представляет из себя набор из одного или нескольких защищенных мультимедийных потоков (в случае использования протокола SRTP, то это потоки данных SRTP).

Возможность создания связей многие-ко-многим является преимуществом данного протокола над другими.

6.2.4. SIP как протокол аутентификации

Как было рассмотрено ранее (см. п. 2.8.1), SIP – это протокол установления сеанса, протокол передачи данных, описывающий способ установления и завершения пользовательского сеанса связи, включающего обмен мультимедийным содержимым, таким как IP-телефония, видео- и аудиоконференции, мгновенные сообщения, онлайн-игры. Этот протокол описывает, каким образом клиентское приложение может запросить начало соединения у другого, возможно, физически удаленного клиента, находящегося в той же сети, используя его уникальное имя.

Протокол определяет способ создания канала связи и согласования протоколов обмена информации между клиентами (например, протокол RTP используется для обмена голосовыми данными). Допускается добавление или удаление таких каналов в течение установленного сеанса, а также подключение и отключение дополнительных клиентов (то есть предусмотрена конференц-связь, когда допускается участие в обмене более двух сторон). SIP также определяет порядок завершения сеанса.

В основу протокола SIP рабочая группа MMUSIC заложила следующие принципы:

– Простота: включает в себя только шесть методов (функций)
– Независимость от транспортного уровня, возможность использования UDP, TCP, ATM и т.д.
– Персональная мобильность пользователей. Пользователи могут перемещаться в пределах сети без ограничений. Это достигается путем присвоения пользователю уникального идентификатора. При этом набор предоставляемых ус-

луг остается неизменным. О своих перемещениях пользователь сообщает с помощью сообщения REGISTER своему серверу.

- Масштабируемость сети. Структура сети на базе протокола SIP позволяет легко ее расширять и увеличивать число элементов.
- Расширяемость протокола. Протокол характеризуется возможностью дополнять его новыми функциями при появлении новых услуг.
- Интеграция в стек существующих протоколов Интернет. Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом IETF. Кроме SIP, эта архитектура включает в себя протоколы RSVP, RTP, RTSP, SDP.
- Взаимодействие с другими протоколами сигнализации. Протокол SIP может быть использован совместно с другими протоколами IP-телефонии, протоколами ТфОП и для связи с интеллектуальными сетями.

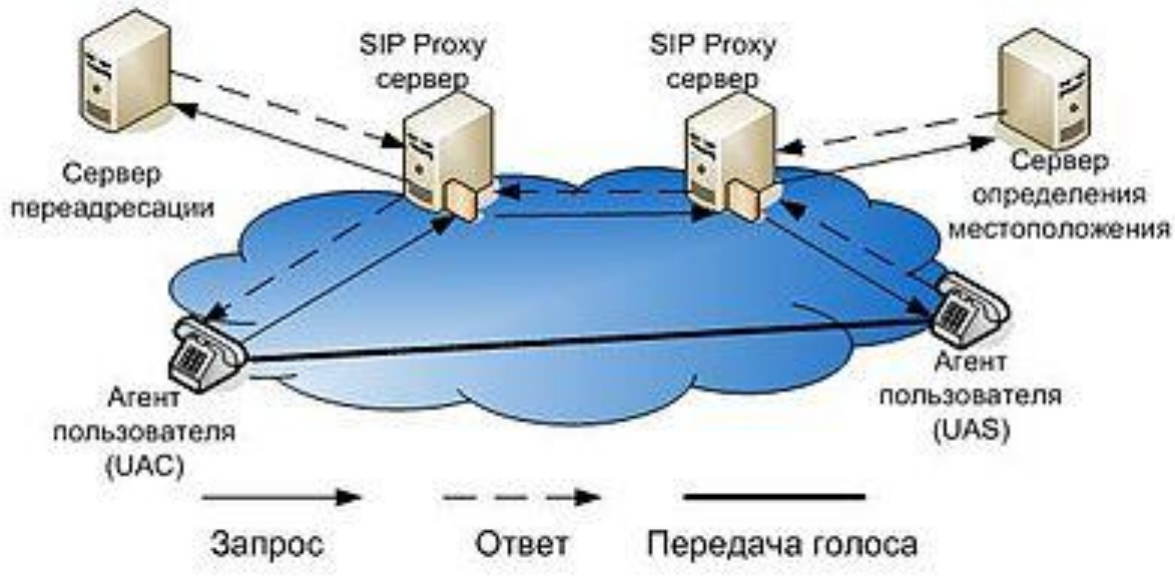


Рисунок 6.5. Архитектура SIP

Протокол SIP имеет клиент-серверную архитектуру (рисунок 6.5). Клиент выдает запросы с указанием того, что он хочет получить от сервера. Сервер принимает и обрабатывает запросы, выдает ответы, содержащие уведомление об успешности выполнения запроса, уведомление об ошибке или информацию, запрошенную клиентом. Обслуживание вызова распределено между различными элементами сети SIP. Основным функциональным элементом, реализующим функции управления соединением, является абонентский терминал. Остальные элементы сети могут отвечать за маршрутизацию вызовов, а иногда служат для предоставления дополнительных сервисов [119].

Далее будут кратко описаны основные элементы SIP.

Терминал. Когда клиент и сервер и взаимодействуют непосредственно с пользователем, они называются User Agent Client и User Agent Server (UAS, сервер агента пользователя). Если в устройстве присутствуют и UAC, и UAS, то оно

называется User Agent (UA, пользовательский агент) и по своей сути представляет собой оконечное оборудование SIP.

Сервер (UAS) и клиент (UAC) имеют возможность непосредственно взаимодействовать с пользователем. Другие клиенты и серверы SIP этого делать не могут.

Прокси-сервер представляет интересы пользователя в сети. Он принимает запросы, обрабатывает их и выполняет соответствующие действия. Прокси-сервер состоит из клиентской и серверной частей, поэтому может принимать вызовы, инициировать запросы и возвращать ответы. Прокси-сервер может не изменять структуру и содержимое передаваемых сообщений, лишь добавляя свою адресную информацию в специальное поле [45].

Сервер B2BUA. B2BUA (англ. back-to-back user agent, буквально: «пользовательский агент спина-к-спине») – вариант серверного логического элемента в приложениях, работающих с протоколом SIP. По идеологии работы B2BUA похож на прокси-сервер SIP, однако есть принципиальные различия. Сервер B2BUA работает одновременно с несколькими (как правило, двумя) конечными устройствами – терминалами, разделяя вызов или сеанс на разные плечи-участки. С каждым участком B2BUA работает индивидуально, как UAS – по отношению к инициатору и как UAC – по отношению к терминалу, принимающему вызов. Каждый из участников соединения (сеанса связи) на уровне сигнализации взаимодействует с B2BUA как с оконечным устройством, хотя в действительности сервер является посредником [119]. Ключевое отличие B2BUA – полностью независимая сигнализация всех участков вызова. Это означает, в частности, что для взаимодействия с каждым отдельным пользователем в рамках сеанса связи используются уникальные идентификаторы, а содержимое одних и тех же сообщений для разных участков будет различным. Пользовательские агенты оконечных терминалов могут взаимодействовать с B2BUA и при участии прокси-серверов [102].

Сервер B2BUA может предоставлять следующие функции:

1. Управление звонками (биллинг, перевод звонка, автоматическое разъединение и т. д.)
2. Сопряжение разных сетей (в частности, для адаптации разных диалектов протокола, зависимых от производителей)
3. Сокрытие структуры сети (частные адреса, сетевая топология и т. п.)

Довольно часто B2BUA является частью медиашлюза для того, чтобы полностью управлять медиапотоками в рамках сессии. Сигнальный шлюз, являющийся частью пограничного контроллера соединений/сеансов – наглядный пример применения B2BUA.

Таким образом подход B2BUA является комплексным решением для передачи данных, содержащим некоторые решения, позволяющие защитить не только сам канал свиязи, но и провайдера, предоставляющего услуги от различного вида атак [102].

Сервер переадресации (Redirect Server) используется для перенаправления вызова по адресу текущего местоположения пользователя.

Сервер регистрации. Протокол SIP подразумевает мобильность пользователя, то есть пользователь может перемещаться в пределах сети, получая новый адрес. Поэтому в SIP существует механизм регистрации – уведомление о новом адресе со стороны пользовательского агента (рисунок 6.6). Сервер регистрации или регистратор служит для фиксации и хранения текущего адреса пользователя и представляет собой регулярно обновляемую базу данных адресной информации.

В общем случае пользователь сообщает серверу регистрации свою адресную информацию, такую как IP-адрес или доменное имя и абонентский телефонный номер, при помощи запроса REGISTER [119]. Сервер может подтвердить успешную регистрацию или отклонить в случае, если есть проверка данных и учетная запись пользователя не найдена или регистрация для пользователя запрещена в данный момент. Регистратор может указать на необходимость логина пользователя для проверки, при этом может предложить клиенту провести аутентификацию на основе зашифрованного пароля. В качестве источника информации для аутентификации пользователя может выступать устройство или ПО, не использующее протокол SIP (например СУБД, MS Exchange, RADIUS-сервер и т. п.). Регистрация терминала пользователя на сервере имеет определенный «срок жизни» и должна подтверждаться новым запросом REGISTER со стороны клиента, в противном случае адресная информация может быть удалена. Клиент может также прислать запрос с нулевым временем жизни регистрации – запрос на принудительное удаление адресной информации из сервера (завершение регистрации) [102].

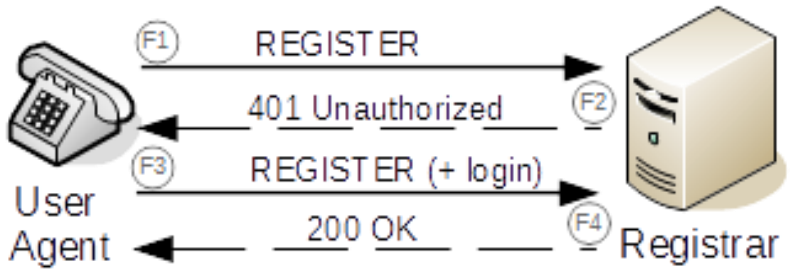


Рисунок 6.6. Регистрация пользователя в сети с аутентификацией по логину

В различных реализациях SIP-сетей может встречаться сочетание сервера регистрации и других серверов в едином приложении или устройстве, работающем через один сокет на одном порту (обычно UDP/5060), т.е. через единую точку получения и обработки запросов. Так, зачастую, регистраторы совмещаются с сервером переадресации, B2BUA или SIP-прокси. Например, многие программные АТС (например, Asterisk, Yate, РТУ) содержат функционал SIP-регистратора с проверкой регистрационных данных каждого пользователя. Информация о возможностях пользователя зарегистрироваться и устанавливать со-

единения определяются в данном случае его единой учетной записью. В свою очередь, абонентское оборудование IP-телефонии (телефоны, абонентские шлюзы) в большинстве случаев требует обязательной предварительной регистрации на сервере для дальнейшей работы в телефонной сети [17].

В результате система IP-телефонии может выглядеть аналогично системе сотовой связи – все абонентское оборудование при включении регистрируется на коммутаторе (АТС) и после этого может совершать и принимать вызовы через него, который либо переадресует запрос другому конечному пользователю, либо переправляет запрос на другой коммутатор.

Сервер определения местоположения пользователей. Пользователь, которому нужна адресная информация другого пользователя для установления соединения, не связывается с сервером определения местоположения напрямую. Эту функцию выполняют другие SIP-серверы при помощи протоколов LDAP, RWHOIS, ENUM, RADIUS или других протоколов [45].

Протокол SIP является достаточно громоздким, однако в момент своего появления был единственным решением, позволявшим развернуть VOIP-сеть. В отличие от него, другие протоколы обеспечения безопасности являются легковесными, но обслуживают лишь одну из сторон обеспечения связи. Сегодня прямые аналоги SIP активно применяются в мультимедиа, таких как стриминг аудио- и видеоконтента, а также передача данных для онлайн- игр в реальном времени.

6.2.5. Механизм аутентификации на основе блокчейна для безопасной связи VoI

Технология блокчейна (blockchain) уже активно используется для передачи потокового видео в реальном времени и телекоммуникационных алгоритмов. Существует целый ряд мультимедийных платформ с поддержкой блокчейна, такие как Theta, Livepeer, Moecp, Waltonchain, IoTeX и OriginTrail, однако их архитектуры больше фокусируются на надежности и гибкости сервисов потоковой передачи видео, а проблемы безопасности не учитываются. Использовать блокчейн в качестве средства криптографии и установки защищенного канала для VOIP впервые предложено в работе [41].

Блокчейн – это цепная структура данных, в которой все данные структурированы в блоки, соединенные на основе времени добавления. Доказано, что блокчейн криптографически защищен от манипулирования данными [22]. Несмотря на свою короткую историю, блокчейн был успешно интегрирован во множество приложений и отраслей промышленности благодаря своим преимуществам в области безопасности. Помимо финансовых применений, таких как биткойн и аналогичные приложения, блокчейн доказал свою роль в качестве безопасной и децентрализованной базы данных [8]. Децентрализованное хранилище в блокчейне может использоваться для хранения обширных сложных данных в надежно соединенных блоках. Децентрализованный и безопасный характер блокчейна делает его многообещающим решением для видеоконференций [8].

Блокчейн изначально был разработан как линейная инфраструктура, основанная на связанных структурах данных и стратегиях хеширования. Однако в последнее время для приложений реального времени внедряются нелинейные инфраструктуры, поскольку они могут обрабатывать большие данные на основе теории графов и информационных моделей массового обслуживания, что делает эту технологию идеальной для приложений, не допускающих задержек в системах видеоконференцсвязи [8, 22].

В данной работе предполагается использовать частный блокчейн, узлами которого являются заранее заверенные хосты.

Предлагаемая структура безопасности видеоконференцсвязи на основе блокчейна (рисунок 6.7) состоит из трех основных уровней:

1. уровень устройств (device layer),
2. пограничный уровень (edge layer),
3. облачный уровень (cloud layer).

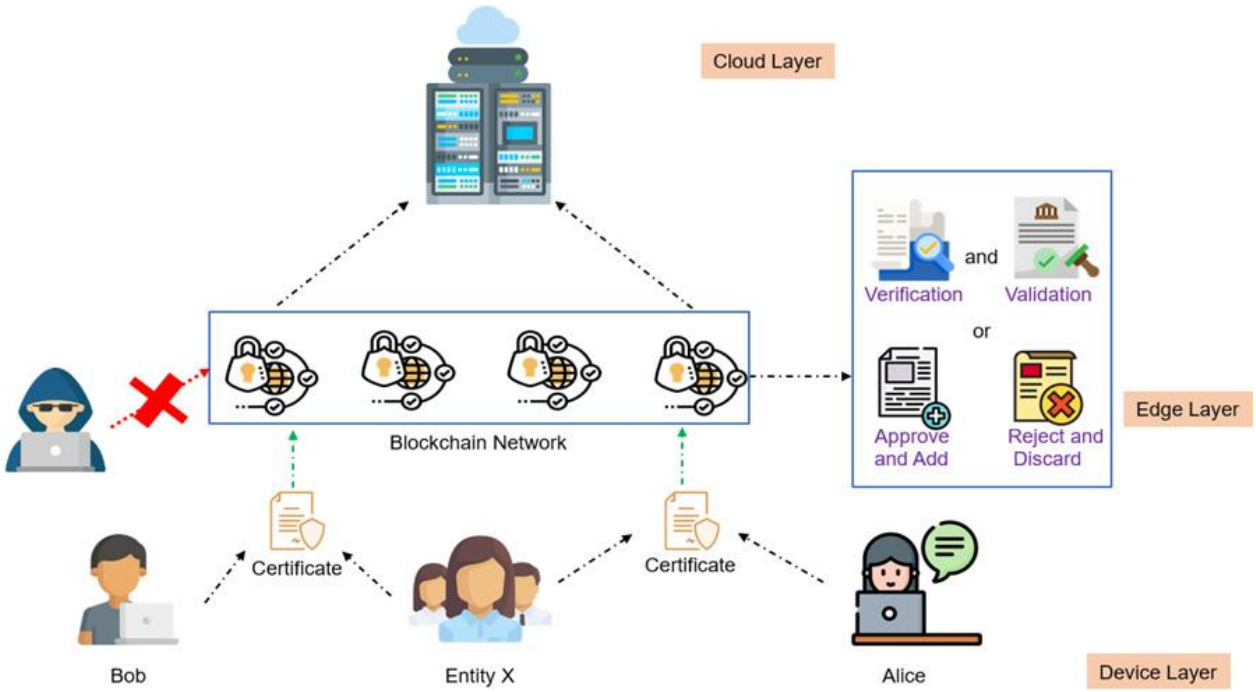


Рисунок 6.7. Структура системы защиты для для VOIP на основе блокчейна

Уровень устройств включает несколько пользователей, присоединяющихся к устройствам видеоконференцсвязи, таким как телефоны, компьютеры, камеры, проекторы, и к интернет-соединениям, таким как сети 5G. Уровень пользователя основан на неоднородности; честные и недобросовестные пользователи – все части этого слоя.

Пограничный слой – это место, где находится рассматриваемая цепочка блоков. На этом уровне блокчейн используется для проверки, проверки и аутентификации пользователей. Честные пользователи будут добавлены в реестр Blockchain как транзакция с подписанным сертификатом. Хотя нечестные устройства будут исключены из реестра, в системе видеоконференцсвязи смогут

участвовать только пользователи с подписанными проверенными сертификатами. Инструменты, демонстрирующие признаки манипуляции, будут переданы в блокчейн и отклонены из канала связи.

Последний слой предлагаемой структуры – это облачный слой. Облачный уровень – это место, где находится центр обработки данных, и он служит средством связи между пользователями. Видео в реальном времени загружаются из центра обработки данных на облачном уровне. Облачный центр обработки данных управляет всеми пользователями и размещает приложения для видеоконференций, такие как программное обеспечение Zoom.

В системе используется частный блокчейн. Доверенный объект контролирует блокчейн. Предполагается, что доверенный объект является поставщиком платформы видеоконференцсвязи. Поставщик платформы выберет группу других доверенных узлов или пользователей для проверки и проверки других пользователей. Частный блокчейн считается облегченной формой блокчейна и, следовательно, потребляет меньше энергии и времени на этапе консенсуса. Кроме того, он больше подходит для приложений реального времени, таких как системы видеоконференцсвязи.

Методы шифрования и дешифрования выполняются на стороне поставщика услуг. Этапы аутентификации и проверки подлинности пользователей могут быть описаны следующим образом:

1. Первый пользователь, который намеревается начать вызов видеоконференции, должен отправить поставщику услуг запрос со своей идентификацией устройства, используемым псевдонимом, меткой времени и одноразовым номером. Временная метка и одноразовый номер используются для проверки согласованности сообщений, отправленных одним и тем же пользователем.
2. Поставщик платформы видеоконференцсвязи проверит идентификацию первого отправителя и оценит действительность этого пользователя.
3. Если поставщик услуг сочтет первого пользователя честным, будет инициализирован протокол консенсуса блокчейна. Поставщик услуг отправит открытый ключ первому пользователю. Этот ключ вычисляется в дайджесте MD5 и имеет 128-битное хэш-значение.
4. Первый пользователь использует полученный открытый ключ для шифрования сообщения и отправки его пользователям, которые намерены присоединиться к вызову видеоконференции, включая временную метку и одноразовый номер. Поскольку одноразовый номер и временная метка каждый раз – разные, этот шаг исключает возможность ответной атаки. Более того, необходимо принять заданную временную задержку, и если временная задержка будет превышена, получатель будет знать, что в системе происходит атака «человек посередине».
5. Каждый пользователь, получивший сообщение от первого пользователя, перешлет сообщение на предварительно выбранные узлы проверки блокчейна с полученным зашифрованным сообщением, отметкой времени и одноразовым

номером, добавив новую временную метку, указывающую время приема сообщения.

6. Предварительно выбранные узлы проверки блокчейна, предварительно зная открытый ключ поставщика услуг, расшифруют и проверят полученное сообщение и временные метки. Система имеет определенную величину допустимой временной задержки. Этап расшифровки и детали выходят за рамки данного исследования.
7. Если временная метка превышает допустимую системой временную задержку или если сообщение неверно, узел проверки объявит пользователя вредоносным. В противном случае пользователь будет заявлен как честный.
8. Все участвующие узлы проверки продолжают отправлять ответы поставщику услуг до тех пор, пока количество полученных сообщений не превысит 51% участвующих узлов. Как только получено необходимое количество сообщений, система достигает консенсуса.
9. Поставщик услуг проверит полученные ответы. Если пользователь оценивается как честный, создается новый блок. В противном случае идентификация злоумышленника будет сохранена на сервере поставщика услуг на облачном уровне, и этому пользователю будет отказано в доступе к вызову видеоконференции.
10. Если один и тот же идентификатор пользователя будет объявлен вредоносным устройством более пяти раз, устройство будет отключено от сервиса или использовано в качестве штрафа. В то же время честные устройства, однажды идентифицированные, смогут подключиться к сервису и участвовать в вызове видеоконференции и проходить последующую проверку.

Как обсуждалось выше, сервер на облачном уровне будет хранить идентификацию всех вредоносных узлов и накапливать эти объекты в своей памяти, сопоставляя количество раз, когда одно и то же устройство было объявлено вредоносным узлом. Если это число превысит пять, устройству будет отказано в использовании системы навсегда. Более того, честные устройства, участвующие в нескольких раундах и зарекомендовавшие себя честными, могут стать узлами проверки в будущем.

6.2.6. VPN для VOIP

Телефонные звонки, как правило, не очень безопасны. Киберпреступники используют множество различных тактик, чтобы прослушивать звонки, поступающие на мобильный телефон пользователя. Для них это на удивление легко – преступники могут использовать радиочастотные сканеры и интерпретатор цифровых данных, чтобы подслушивать незащищенные звонки. Однако с помощью системы VoIP можно настроить VPN для защиты телефонных звонков в сети.

Объединив VPN с вашей телефонной системой VoIP, вы сможете защитить весь свой голосовой трафик и трафик данных, а также защитить устройства, на которых работают ваши сотрудники. Вы предоставляете своим командам

шифрование для безопасной обработки всех видов звонков, где бы они ни находились.

VPN (виртуальная частная сеть) – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети, например, Интернет. Несмотря на то, что для коммуникации используются сети с меньшим или неизвестным уровнем доверия (например, публичные сети), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств защиты от повторов и изменений передаваемых по логической сети сообщений) [51].

Возьмем, к примеру, компанию технической поддержки, которая обрабатывает звонки в службу поддержки для различных клиентов. Когда крупные корпорации хотят передать свои операции по поддержке клиентов на аутсорсинг, эта компания технической поддержки является их первым выбором. Вместо того, чтобы иметь большой физический офис колл-центра, эта компания заставляет своих сотрудников принимать звонки из своих домашних офисов. Сотрудники могут работать из дома в разных часовых поясах, и компания использует передачу голоса по IP для обеспечения такой гибкости. Использование VoIP существенно снижает их эксплуатационные расходы.

Клиент управляет своей инфраструктурой VoIP из своего центра обработки данных. Их VoIP-решение по своей сути не поддерживает безопасность – защищенные протоколы VoIP, такие как SIPS и SRTP, не используются, что означает, что существуют некоторые риски безопасности VoIP, которые компания должна устранить. Поскольку их сотрудники работают из дома, для настройки сети целесообразно использовать OpenVPN [96].

Протокол OpenVPN использует TLS/SSL и поэтому является дружественным к NAT (Network Address Translation, механизм преобразования сетевых адресов). Он может легко туннелировать протоколы VoIP через NAT. Использование IP-адресов, назначенных VPN, также создает впечатление, что VoIP-устройства находятся в той же частной сети, что и защищенный VoIP-сервер. Это упрощает реализацию VoIP, поскольку ей не нужно иметь дело с обходом NAT [51].

VoIP-связь защищена путем ее туннелирования внутри VPN. Только определенные входящие порты, используемые VPN-клиентами, должны быть открыты для входящего трафика в центре обработки данных, где находится защищенный VoIP-сервер. Это сопоставимо с необходимостью открывать широкий спектр портов, которые обычно используют SIP и SRTP. Защита VoIP с помощью OpenVPN отвечает всем потребностям клиента.

Клиент должен установить сервер доступа OpenVPN в центре обработки данных, где находится защищенный VoIP-сервер, и настроить контроль доступа таким образом, чтобы разрешить доступ только к защищенному VoIP-серверу. Профили автоматического входа в системусоздаются и распространяются среди сотрудников для импорта в их VoIP-телефоны. Для сотрудников, желающих ис-

пользовать офисный телефон, рекомендуются аналоговые телефонные адаптеры, поддерживающие OpenVPN, такие как Yeastar, или IP-телефоны, такие как Snom Technology [42].

Использование технологии OpenVPN обеспечивает безопасность как защищенного VoIP-сервера в центре обработки данных, так и VoIP-коммуникаций. Решение VoIP не создает сложности обхода NAT, и сотрудники могут использовать выбранное ими устройство для ведения бизнеса.

6.2. Инструментарий

6.2.1. Платформа Asterisk

Asterisk (см. также п. 2.11.1) – это платформа с открытым исходным кодом для создания коммуникационных приложений. Asterisk (рисунок 6.8) превращает обычный компьютер в коммуникационный сервер. Asterisk поддерживает системы IP-АТС, шлюзы VoIP, серверы конференций и другие специализированные решения. Платформа Asterisk используется малыми и крупными предприятиями, колл-центрами, операторами связи и государственными учреждениями по всему миру. Код платформы Asterisk является бесплатным и открытым, разработка спонсируется Sangoma [17].

Рисунок 6.8. Логотип компании Asterisk

Сегодня в более чем 170 странах используется более миллиона систем связи на базе Asterisk. Asterisk используется почти всем списком клиентов Fortune 1000. Чаще всего развертываемый системными интеграторами и разработчиками, Asterisk может стать основой для полной системы бизнес-телефонии или использоваться для улучшения или расширения существующей системы или для устранения разрыва между системами [17].

Asterisk в комплексе с необходимым оборудованием обладает всеми возможностями классической АТС, поддерживает множество VoIP-протоколов и предоставляет богатые функции управления звонками, среди них:

- Голосовая почта,
- Конференцсвязь,
- IVR (интерактивное голосовое меню),
- Центр обработки звонков (постановка звонков в очередь и распределение их по абонентам, используя различные алгоритмы),
- Call Detail Record (подробная запись о вызове),
- Интеграция с CRM-системами.

Для создания дополнительной функциональности можно воспользоваться собственным языком Asterisk для написания плана нумерации, написав модуль на языке Си, либо воспользовавшись Asterisk Gateway Interface (AGI) – гибким и

универсальным интерфейсом для интеграции с внешними системами обработки данных. Модули, выполняющиеся через AGI, могут быть написаны на любом языке программирования [17].

6.2.2. Проект OpenVPN

Упомянутый в разделе 6.2.6 OpenVPN [43] – это проект с открытым исходным кодом. Протокол OpenVPN зарекомендовал себя как стандарт де-факто в сетевом пространстве с открытым исходным кодом с более чем 50 миллионами загрузок. OpenVPN – полностью поддерживаемый сообществом проект OSS, использующий лицензию GPL. В проекте участвует много разработчиков и участников из OpenVPN Inc. и более широкого сообщества OpenVPN. Кроме того, существует множество проектов, расширяющих или иным образом связанных с OpenVPN [43].

Рисунок 6.9. Логотип OpenVPN

6.5. Рекомендации по обеспечению информационной безопасности при использовании технологий IP-телефонии

6.5.1. Защита IP-телефонии

Решение задач информационной безопасности должно быть комплексным, поскольку каждый способ защиты не только закрывает свою часть информационного периметра, но и дополняет другие решения.

Рисунок 6.10. Реализация IP-телефонии

Пример реализации схемы защиты IP-телефонии представлен на рисунке 6.10. Сервер телефонии на базе IP-АТС Asterisk имеет прямой выход в сеть интернет для обслуживания удаленных филиалов и связи с SIP-провайдером, предоставляющим доступ к внешним линиям связи. Аутентификация пользователей происходит по IP-адресам [17].

6.5.2. Применение межсетевых экранов

Межсетевой экран пропускает исходящий трафик от сервера телефонии к SIP-провайдеру и фильтрует входящий по определенным правилам. Рациональным решением можно считать закрытие на межсетевом экране всех сетевых портов для IP-телефонии, кроме необходимых для ее корректной работы и администрирования. Этот же метод защиты целесообразно применять на самом сервере телефонии, чтобы защитить его от внутренних атак. В [45] показано, как реализуется межсетевой экран в SIP – B2BUA.

Таким образом, сервер телефонии доступен из внешних сетей только по определенным служебным портам, подключение к которым, из соображений безопасности, будет выполняться с применением шифрования.

6.5.3. Шифрование телефонных разговоров

Для защиты конфиденциальных переговоров и минимизации возможности попадания конфиденциальной или коммерческой информации в руки злоумышленника необходимо защитить передаваемые по открытым каналам связи данные от перехвата и прослушивания.

Поскольку для совершения звонка клиент и сервер предварительно обмениваются служебными данными для установления соединения, данную проблему можно разделить на две составляющих – защиту служебных данных IP-телефонии и защиту голосового трафика. В качестве средства защиты могут быть использованы протокол TLS для защиты SIP сигналов и протокол SRTP (Secure Real Time Protocol) для защиты голосового трафика.

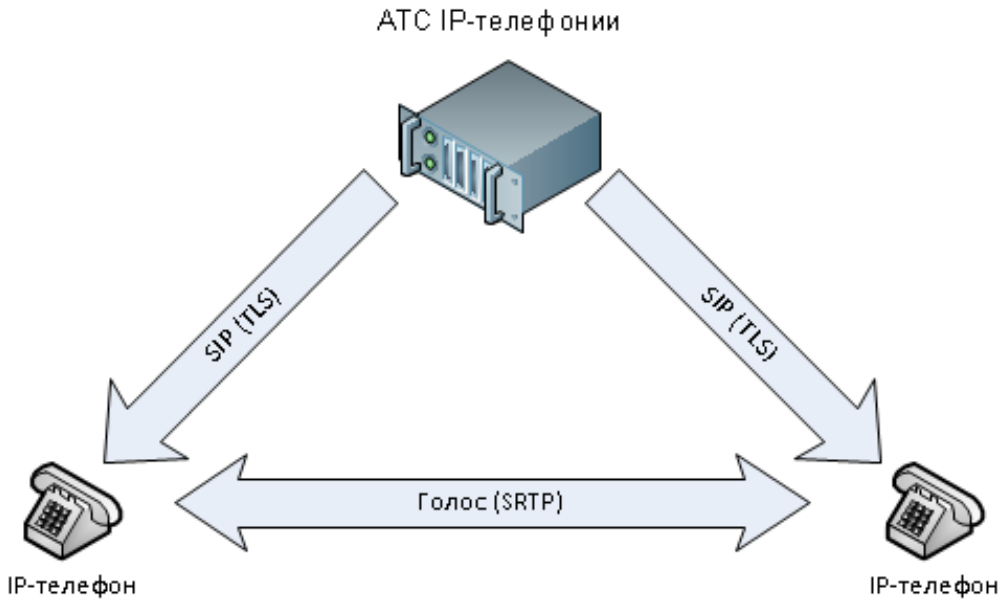


Рисунок 6.11. Шифрование IP-телефонии

TLS – криптографический протокол, обеспечивающий защищенную передачу данных между узлами в сети, является стандартным методом для шифрования SIP-протокола. TLS обеспечивает конфиденциальность и целостность передаваемой информации, осуществляет аутентификацию.

После установления защищенного соединения начинается передача голосовых данных, обезопасить которые позволяет применение протокола SRTP [77].

Протокол SRTP считается одним из лучших способов защиты IP телефонии на базе IP-АТС Asterisk. Основное преимущество этого протокола – отсутствие какого-либо влияния на качество связи. Схема работы протокола SRTP выглядит так: каждому совершаемому вами звонку присваивается уникальный код, который делает подслушивание разговоров неавторизированными в системе пользователями практически невозможным [17]. Благодаря этому протокол SRTP выбирают как для обычных, так и для конфиденциальных звонков.

Не следует забывать о необходимости защиты подключения сервера телефонии к внешним каналам связи (мобильная связь, телефонные сети общего пользования).

6.5.4. Применение шифрованных туннелей VPN

В случае организации систем с повышенными требованиями к защите IP-телефонии возможно подключение удаленных пользователей посредством виртуальных частных сетей (VPN). Содержание перехваченных пакетов, отправленных по шифрованным VPN-туннелям, понятно только владельцам ключа шифрования. Этот же метод применим для защиты подключений к поставщикам услуг IP-телефонии. На текущий момент многие VoIP-провайдеры предлагают возможность VPN-подключения [77] (рисунок 6.12).

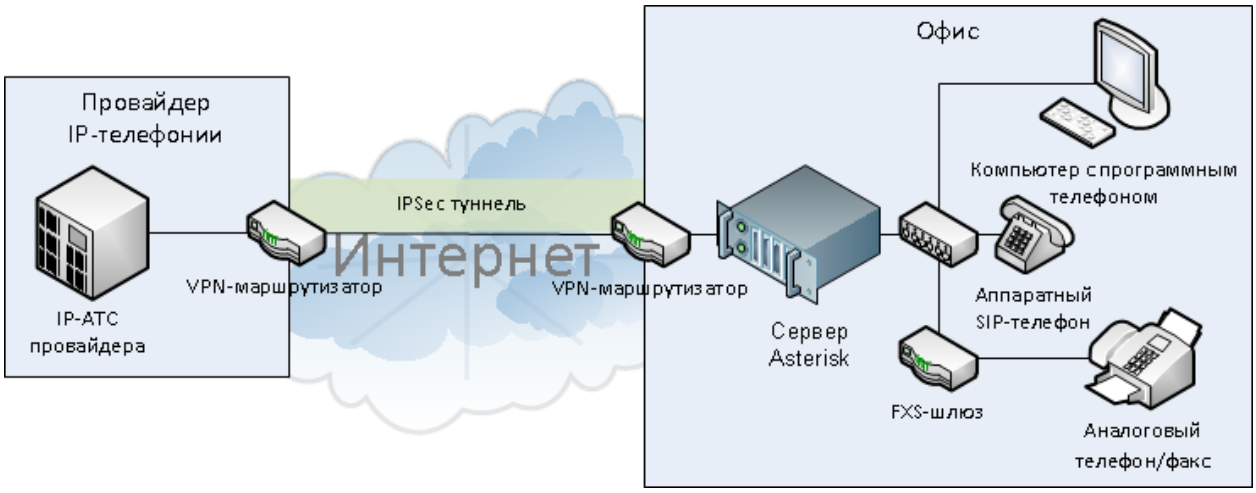


Рисунок 6.12. Схема работы IP-телефонии через VPN-туннель

Однако технология VPN имеет ряд недостатков, ограничивающих ее применение**:**

– снижение качества связи из-за задержек, создаваемых шифрованием;

– повышенная нагрузка на каналы связи и оборудование за счет необходимости шифрования;
– усложнение сетевой структуры.

Применение перечисленных методов защиты сервера позволит свести к минимуму вероятность взлома, а при успешном обходе системы безопасности минимизировать ущерб [96].

Резюме

Методы обеспечения информационной безопасности появились в момент зарождения информационных сетей и постоянно прогрессируют. Но абсолютную гарантию информационной безопасности, к сожалению, не сможет дать ни один комплекс мер. Рассмотренные выше аспекты лишь частично решают задачу построения защищенной коммуникационной системы**.** На практике следует рассматривать всю инфраструктуру корпоративной сети, проводить глубокий анализ требуемого уровня защиты [62, 63]. Необходимо учитывать не только обеспечение безопасности IP-телефонии, но и выходы на внешние каналы связи. Только такой подход, вместе с постоянным совершенствованием систем информационной безопасности, позволит создать надежную и защищенную систему.

Вопросы для самопроверки

1. Назовите основные виды угроз информационной безопасности при использовании технологий IP-телефонии.
2. Поясните протокол шифрования данных SRTP.
3. В чем состоит применение SIP как протокола аутентификации?
4. Каков функционал сервера регистрации в протоколе SIP?
5. Почему сегодня целесообразно применение аутентификации на основе блокчейна для безопасной связи VoIP?
6. Для чего применяют VPN для VOIP?
7. В чем особенности и недостатки применения Asterisk и OpenVPN?
8. Почему и как применяют современные сетевые экраны?
9. Почему и как применяют шифрованные туннели VPN?
10. Приведите и кратко обоснуйте рекомендации по обеспечению информационной безопасности при использовании технологий IP-телефонии.

ЗАКЛЮЧЕНИЕ

IP-телефония обладает рядом преимуществ, таких как низкая стоимость, мобильность, отсутствие дополнительных кабелей, гибкость, видеоконференцсвязь, сеть унифицированных коммуникаций (UC), интеллектуальное решение для мобильности подключения, простая в использовании технология WebRTC, богатый функциональными возможностями коммуникационный аспект, простота установки и настройки, простота масштабируемости, экономия затрат при повышении производительности.

В IP-телефонии используются протоколы SIP, H.323, RTP, RTCP, SRTP, SDP и др. Они имеют разный функционал, но самым популярным является протокол SIP. Используются кодеки G.729, G.711 и импульсно-кодовая модуляция.

IP-телефония также имеет ряд проблем, в том числе потребность в источнике питания, сжатие голоса, проблемы Интернет-провайдера, но в целом использование IP-телефонии является хорошим и эффективным решением.

Перспективы развития технологий IP-телефонии имеют множество направлений. Развитие информационных технологий в целом напрямую влияет на развитие VoIP. Основными тенденциями роста индустрии становятся интеграция искусственного интеллекта (ИИ), интернета вещей (IoT) и новых технологий обеспечения безопасности, пришедших с развитием мобильной связи.

На фоне общего снижения темпов роста доходов от традиционных услуг мобильной связи, таких как телефония и Интернет, операторам приходится осваивать новые ниши. Одним из таких перспективных рынков является Интернет вещей (IoT). В результате опроса, проведенного TMForum – международной организации, которая занимается вопросами развития и оптимизации бизнеса операторов связи, эксперты отрасли пришли к единому мнению: сейчас именно то время, когда MVNO стоит задуматься о реализации IoT. Вовлечение MVNE позволяет виртуальным мобильным операторам освоить перспективные ниши, к которым относится IoT, гораздо быстрее и эффективнее.

Из-за того, что в современных реалиях предприятия больше не являются такими централизованными, какими были раньше, важной задачей для технических специалистов является обеспечение защищенного канала для доступа ко внутренним ресурсам, в том числе из внешней сети. Важно обеспечить конфиденциальность, целостность и доступность системы, учесть все возможные угрозы безопасности, такие как перехват данных и манипуляция ими, подмена и взлом пользовательских данных, ограничение доступности.

Поэтому можно считать вполне рациональным увеличение максимального количества обеспечиваемых соединений при снижении затрат ресурсов на каждое соединение. Здесь появляется мотивация использовать дополнительные технологии, поддерживаемые VoLTE. К ним может относиться сжатие заголовков, группирование пакетов интервала времени передачи, работа с QoS.

Улучшение качества звука также повысит эффективность. Качество звука зависит от используемого кодека. В мобильных сетях распространены кодеки AMR, такие как AMR Narrowband (узкополосный, до 3700 Гц), AMR Wideband

(широкополосный, до 7000 Гц), AMR Super Wideband (сверхширокополосный, до 14000 Гц). Тесты показали, что для VoLTE оптимален широкополосный кодек. Он обеспечивает хорошее качество голоса в свободной сети, но при этом не слишком большой объем данных позволяет сохранять качество и в условиях загруженной сети. При работе с AMR Wideband также сохраняется стабильно низкая задержка передачи данных [6].

Для сокращения времени установления вызова оператор может настроить пейджинг вызовов узлом MME (Mobile Management Entity). В таком случае узел способен применить отдельные правила для вызовов VoLTE, чтобы снизить время соединения.

Цифровой характер VoIP означает, что он может стать целью хакеров. Машинное обучение будет работать над остановкой таких кибератак, со временем совершенствуясь за счет обработки большего количества данных, чтобы идти в ногу с достижениями в области взлома VoIP. ИИ можно обучать с помощью методов тестирования программного обеспечения, таких как тестирование функциональных протоколов для обнаружения ошибок в системах VoIP, которые могут быть использованы.

VoIP позволяет предприятиям получать важные данные о вызывающих абонентах, такие как личность, местоположение, намерения и история вызовов, еще до того, как разговор состоится. Голосовой ИИ может помочь звонящим через систему интерактивного голосового ответа (IVR) направить их по нужным каналам, будь то другой ИИ или представитель человека, используя собранные данные. С помощью прогнозирующих моделей машинного обучения ИИ также может рекомендовать операторам следующее оптимальное действие на основе истории вызовов и прошлых разговоров. Разговоры можно значительно сократить, сократив время ожидания в очереди между звонящими, или их можно направить на дополнительные продажи.

Многие запросы клиентов могут быть решены с помощью автоматизации. Часто задаваемые вопросы, общие проблемы с устранением неполадок, планирование встреч и заказ продуктов – все это может обрабатываться с помощью голосового ИИ через IVR. Это позволит людям-операторам решать сложные задачи, снижая затраты на найм и обучение только для того, чтобы иметь возможность принимать простые звонки.

ИИ также достаточно продвинулся, чтобы брать на себя более сложные процессы. Он может назначать встречи, отправлять приглашения, корректировать бронирование и создавать маршруты на основе данных, извлеченных из речи звонящего и истории звонков. Дальнейшее развитие с помощью машинного обучения только расширит возможности ИИ для еще большей оптимизации задач.

Переход от стационарных телефонов к VoIP неизбежен, особенно в мире бизнес-телефонии, где компании сталкиваются с масштабным переходом на удаленную работу и ищут все конкурентные преимущества для обеспечения превосходного обслуживания клиентов. Будущие технологии ИИ и машинного обучения дополняют растущее распространение технологий IP-телефонии.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. 3CX: Что такое IP-телефония [Электронный ресурс]. URL: https://www.3cx.ru/voip-sip/what-is-ip-telephony/
2. 5 Key advantages to VoIP CRM integration [Электронный ресурс]. URL: https://www.yeastar.com/blog/5-key-advantages-voip-crm-integration/ (Дата обращения 15.03.2022)
3. 75 Key VoIP Statistics: 2022 Data Analysis & Market Share [Электронный ресурс]. URL: https://financesonline.com/voip-statistics (Дата обращения: 09.03.2022)
4. Abualhaj, M. M. An Effective Method to Improve VoIP Technology Bandwidth Utilization over ITTP Protocol / Abualhaj, M. M., S. N. AlKhatib, Q. Y. Shambour. – 2020.
5. Advantage Imaging Supply: Which Industries Benefit Most from VoIP Phone Systems? // [Электронный ресурс] URL: https://www.aisink.com/2018/09/17/which-industries-benefit-most-from-voip-phone-systems/
6. AMR-WB (Adaptive Multi-Rate Wideband) [Электронный ресурс]. URL: http://celnet.ru/amrwb.php (Дата обращения 13.03.2022)
7. Anand R. Prasad, Alf Zugenmaier, Adrian Escott and Mirko Cano Soveri. 3GPP 5G Security [Электронный ресурс]. URL: https://www.3gpp.org/news–events/1975–sec_5g (Дата обращения: 15.03.2022).
8. Blockchain Will Change Everything, Even VoIP [Электронный ресурс]. URL: https://getvoip.com/blog/2017/05/08/blockchain-and-voip (Дата обращения: 10.03.2022)
9. Bolot, J. C. RTP Payload for Redundant Audio Data / J. C. Bolot, M. J. Handley, V. Hardman, I. Kouvelas, C. Perkins. 1997.
10. Charnes A., Cooper W.W. Programming with linear fractional functionals // Naval Research Logistics Quarterly. 1962. №9. – P. 181-185 (дата обращения: 17.03.2022).
11. CNews. VoIP против операторов сотовой связи: быть войне? [Электронный ресурс] URL: https://www.cnews.ru/reviews/free/telecom2011/articles/articles5.shtml (Дата обращения: 15.03.2022)
12. Comparison of VOIP signaling protocol H.323 Vs SIP [Электронный ресурс]. URL: https://www.researchgate.net/publication/294865196_ Comparison_of_VOIP_signaling_protocol_H323_Vs_SIP (Дата обращения 12.03.2022)
13. Definition of Mobile Virtual Network Enabler (MVNE) - Gartner Information Technology Glossary // Gartner | Delivering Actionable, Objective Insight to Executives and Their Teams URL: https://www.gartner.com/en/information-technology/glossary/mvne-mobile-virtual-network-enabler (дата обращения: 01.03.2022).

14. E2E шифрование WebRTC в Chrome [Электронный ресурс]. – Режим доступа: https://webrtcbydralex.com/index.php/2020/03/30/secure-frames-sframes-end-to-end-media-encryption-with-webrtc-now-in-chrome/. – Дата доступа: 20.03.2022.
15. Ezzat Amin. Improving VoIP Quality by Using Fuzzy Logic Prediction models [Электронный ресурс]. URL: https://www.researchgate.net/publication/334646132_Improving_VoIP_Quality_by_Using_Fuzzy_Logic_Prediction_models (Дата обращения: 13.03.2022)
16. Fortuna, P. Header Compressed VoIP in IEEE 802.11 / Fortuna P., M. Ricardo. 2009.
17. Getting Started with Asterisk // Asterisk [Электронный ресурс]. URL: https://www.asterisk.org/ (дата доступа 14.03.2022)
18. Ghannam Aljabari. Integrating VoIP Systems with The Internet of Things. 2015. С. 1–4.
19. Global Mobile Virtual Network Operator (MVNO) Market Survey 2022 With Top Countries Data: [Электронный ресурс]. URL: https://www.wicz.com/story/45571134/global-mobile-virtual-network-operator-(mvno). (дата доступа: 15.03.2022)
20. Gupta N. Comparative Analysis of Voice Codecs over Different Environment Scenarios in VoIP / N. Gupta, N. Kumar, H. Kumar. 2018
21. Gurrapu S., Mehta S., Panbude S.– Comparative Study For Performance Analysis Of Voip Codecs Over Wlan In Nonmobility Scenarios. 2016
22. How Does Ethereum Work? [Электронный ресурс]. URL: https://www.coindesk.com/learn/how-does-ethereum-work (Дата обращения: 09.03.2022)
23. Interactive Voice Response (IVR) Systems - Global Market Trajectory & Analytics [Электронный ресурс]. – Режим доступа: https://www.researchandmarkets.com/reports/338501/interactive_voice_response_ivr_systems_global?utm_source=BW&utm_medium=PressRelease&utm_code=8b8grt&utm_campaign=1646749+-+Global+Interactive+Voice+Response+Systems+Industry+to+2026+-+Speech+Enabled+IVR+Becoming+the+Preferred+User+Interface&utm_exec=jamu273prd. – Дата доступа: 20.03.2022.
24. Itech. Обзор технологий SDN/NFV [Электронный ресурс]. URL: https://itechinfo.ru/content/technologies-sdnnfv (Дата обращения: 15.03.2022)
25. James Anthony. 12 VoIP Trends for 2022/2023: Latest Predictions To Watch Out For [Электронный ресурс]. URL: https://financesonline.com/voip-trends/ (Дата обращения: 15.03.2022).
26. Kim K. Performance Comparison of Various VoIP Codecs in Wireless Environments / K. Kim, Y. Choi. 2011.
27. Lucy Fuggle. 9 VoIP Trends to Pay Attention to in 2022 [Электронный ресурс]. URL: https://blog.hubspot.com/service/9–voip–trends–for–2020–to–pay–attention–to (Дата обращения: 07.03.2022).

28. Man Li, Wenbin Gu, Wei Chen. Smart Home. – 2018. – С. 394–400. 71
29. Mike Elgan. VoIP trends: the future of the VoIP industry is clear (and flexible) [Электронный ресурс]. URL: https://www.verizon.com/business/resources/articles/s/the–future–of–the–voip–industry/ (Дата обращения: 15.03.2022).
30. MIKEY: Multimedia Internet KEYing/ J. Arkko, E. Carrara и др. [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc3830 (дата доступа 14.03.2022)
31. Mobile Virtual Network Operator – MVNO (рынок России): // Tadvisor. [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Mobile_Virtual_Network_Operator_-_MVNO_(рынок_России). (дата доступа: 17.03.2022)
32. MVNO Russia 2021: [Электронный ресурс]. URL: https://www.tmtconferences.ru/events/mvno2021/ (дата доступа: 15.03.2022)
33. MVNO Types & Operational Models: [Электронный ресурс]. URL: https://www.yozzo.com/mvno-academy/mvno-types-and-operational-models/. (дата доступа: 17.03.2022)
34. Nestor Gilbert. 10 VoIP Software Trends for 2022/2023: Latest Predictions To Watch Out For [Электронный ресурс]. URL: https://financesonline.com/voip-software-trends/ (Дата обращения: 15.03.2022).
35. Nistico A. A comparative study of RTC applications / A. Nistico, D. Markudova, M. Trevisan, M. Meo, G. Carofiglio. 2022
36. Osborne C.. (2017). VoIPtalk admits to possible data breach | ZDNet. [Электронный ресурс]. URL: http://www.zdnet.com/article/ voiptalk-admits-to-possible-data-breach (Дата обращения 08.03.2022)
37. PERC Lite [Электронный ресурс]. – Режим доступа: https://datatracker.ietf.org/doc/html/draft-murillo-perc-lite-01. – Дата доступа: 20.03.2022.
38. Raspberry Pi Foundation [Электронный ресурс]. URL: https://www.raspberrypi.org. (Дата обращения: 12.03.2022).
39. Rescorla, E. Datagram Transport Layer Security / E. Rescorla, N. Modadugu. 2006.
40. Robust Header Compression [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Robust_Header_Compression. – Дата доступа: 20.03.2022.
41. Scalable Lightweight Blockchain-Based Authentication Mechanism for Secure VoIP Communication / Abir El Azzaoui, Min Yeong Choi и др. [Электронный ресурс]. URL: http://hcisj.com/articles/?HCIS202212008 (дата доступа 14.03.2022)
42. Secure access and network connectivity reimagined // OpenVPN [Электронный ресурс]. URL: https://openvpn.net/ (дата доступа 14.03.2022)
43. Secure End-to-End VoIP System Based on Ethereum Blockchain [Электронный ресурс]. URL:

http://www.jocm.us/uploadfile/2018/0817/20180817033654165.pdf (Дата обращения: 09.03.2022)
44. Selective Forwarding Units (SFU) в WebRTC [Электронный ресурс]. – Режим доступа: https://www.frozenmountain.com/hubfs/5%20-%20pdfs/frozenmountain-sfu-selective-forwarding-whitepaper.pdf. (Дата обращения: 20.03.2022).
45. Session Initiation Protocol // Wikipedia [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Session_Initiation_Protocol (дата доступа 14.03.2022)
46. Seytnazarov S. Qos-Aware Adaptive a-Mpdu Aggregation Scheduler for Voice Traffic in Aggregation-Enabled High Throughput WLANs / Seytnazarov S., K. Young-Tak. 2017.
47. Software Defined Network [Электронный ресурс]. URL: http://sdn.ifmo.ru/projects/sdn/index_html (Дата обращения: 15.03.2022)
48. The impact of Artificial Intelligence on communication networks and services [Электронный ресурс]. URL: https://www.itu.int/dms_pub/itu-s/opb/journal/S-JOURNAL-ICTF.VOL1-2018-1-PDF-E.pdf (Дата обращения: 11.03.2022).
49. The Secure Real-time Transport Protocol (SRTP) / M. Baugher, D. McGrew и др. [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc3711 (дата доступа 11.03.2022)
50. Vermesan O. and Friess P., eds. Internet of Things–From Research and Innovation to Market Deployment. River Publishers. 2014. С. 31–39.
51. Virtual private network // Wikipedia [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Virtual_private_network (дата доступа 14.03.2022)
52. Voice over IP: // Wikipedia [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Voice_over_IP. (дата доступа 14.03.2022)
53. VoIP кодеки – подробное описание и характеристики [Электронный ресурс] URL: https://wiki.merionet.ru/ip-telephoniya/5/voip-codecs/
54. WebRTC Security Architecture [Электронный ресурс]. – Режим доступа: https://datatracker.ietf.org/doc/draft-ietf-rtcweb-security-arch/17/. (Дата доступа: 20.03.2022).
55. What Are VoIP Codecs & How Do They Affect Call Sound Quality? [Электронный ресурс]. – Режим доступа: https://www.nextiva.com/blog/voip-codecs.html#:~:text=A%20VoIP%20codec%20is%20a,two%20terms%3A%20Compression%20and%20Decompression. (Дата доступа: 20.03.2022).
56. ZRTP // Wikipedia [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/ZRTP (дата доступа 14.03.2022)
57. ZRTP: Media Path Key Agreement for Unicast Secure RTP draft-zimmermann-avt-zrtp-21 / P. Zimmermann [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/draft-zimmermann-avt-zrtp-21 (дата доступа 11.03.2022)

58. Афанасьев Г.И., Белоногов И.Б., Семкин П.С.: Дальнейшее совершенствование IP-телефонии - SIP-телефония // Научно-практический электронный журнал «Аллея Науки» №1(17). 2018. С. 2–3.
59. Базовая станция сотового оператора – MVNO: [Электронный ресурс]. URL: https://itpex.net/bazovaya-stantsiya-sotovogo-operatora-mvno/. (дата доступа: 16.03.2022)
60. Баскаков И.В., Пролетарский А.В., Федотов Р.А., Мельников С.А.. IP- телефония в компьютерных сетях. [Электронный ресурс]. Режим доступа: http://it-ebooks.ru/publ/computer_networks/ip_telefoniya/16-1-0-832 (дата обращения: 01.03.2022)
61. Безопасность 5G [Электронный ресурс]. URL: https://habr.com/ru/post/533078/ (Дата обращения: 12.03.2022).
62. Билятдинов К.З., Меняйло В.В. Методика оценки эффективности систем на основе модифицированного метода DEA // Вестник воздушно-космической обороны», выпуск 3(27), 2020. С. 66–74 (дата обращения: 17.03.2022).
63. Билятдинов К.З., Меняйло В.В. Модифицированный метод DEA и методика оценки эффективности технических систем / Информационные технологии, выпуск 11, 2020. С. 611
64. Ван Меггелен, Д. Asterisk. Будущее телефонии / Джим Ван Меггелен, Лейф Мадсен, Джаред Смит.
65. Виртуальные операторы сотовой связи – затяжной прыжок: [Электронный ресурс]. URL: https://3dnews.ru/570434. (дата доступа: 16.03.2022)
66. Виртуальный для IoT: [Электронный ресурс]. URL: https://telecomdaily.ru/news/2020/03/15/virtualnyy-dlya-iot. (дата доступа: 17.03.2022)
67. Владимиров С. А. Модель операторской системы мониторинга качества ip-услуг в соответствии с требованиями / С. А. Владимиров, Д. С. Кабытова. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2020. 39–54 с.
68. Волынкина Е. Рынок АТС: виртуальность вытесняет реальность? [Электронный ресурс]. URL: https://www.iksmedia.ru/articles/5354498-Rynok-ATS-virtualnost-vytesnyaet.html (Дата обращения: 16.03.2022).
69. Гасс Я. М. Моделирование экономической эффективности деятельности виртуальных операторов мобильной связи на основе оценки структуры доходов и затрат / Я. М. Гасс, В. О. Тихвинский, Р. Ю. Уманский. Москва: Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, 2020. 64–78 с.
70. Голосовые интерфейсы и проектирование виртуальных ассистентов [Электронный ресурс]. URL: https://projectorat.ru/wpm/ux-letters/ux-letter-47/. (Дата доступа: 20.03.2022).
71. Гольдштейн Б.С. Инфокоммуникационные сети и системы. BHV, 2019. ISBN 978-5-9775-4048-3

72. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP-телефония. - Радио и связь, 2020
73. Гольдштейн, Б. С. Call-центры и компьютерная телефония / Б. С. Гольдштейн, В. А. Фрейнкман. БХВ Санкт-Петербург, 2002.
74. Гольдштейн Б.С. Протокол SIP: справочник / Б.С. Гольдштейн, А. А. Зарубин, В. В. Саморезов. Санкт-Петербург, 2005.
75. Еще раз о шифровании ГОСТ 28147-89 / Хабр // Хабр. Сообщество IT-специалистов / Хабр URL: https://habr.com/ru/post/256843/ (дата обращения: 05.03.2022).
76. Зачем в России столько виртуальных операторов и кому нужен свой MVNO: // РБК Тренды. [Электронный ресурс]. URL: https://trends.rbc.ru/trends/industry/cmrm/5fe316789a79476d46b69efe (дата доступа: 16.03.2022)
77. Защита IP-телефонии // EFSOL [Электронный ресурс]. URL: https://efsol.ru/articles/protection-ip-telephony.html (дата доступа 14.03.2022)
78. История развития глобальных компьютерных сетей // Информационное общество URL: http://emag.iis.ru/arc/infosoc/emag.nsf/0/35a9f811c4118859c32569ed00419692 (дата обращения: 01.03.2022).
79. Клиентские компоненты | ИнфоТеКС // ИнфоТеКС — https://infotecs.ru/ — Безопасность информационных систем и защита данных URL: https://infotecs.ru/product/klientskie-komponenty/ (дата обращения: 05.03.2022).
80. Компоненты управления | ИнфоТеКС // ИнфоТеКС — https://infotecs.ru/ — Безопасность информационных систем и защита данных URL: https://infotecs.ru/product/komponenty-upravleniya/ (дата обращения: 05.03.2022).
81. Конференц-связь RTP с повышенной конфиденциальностью (PERC) [Электронный ресурс]. – Режим доступа: https://datatracker.ietf.org/doc/rfc8871/. – Дата доступа: 20.03.2022.
82. Лемешко В.А., Тепцова Т.С. Телемедицина: здравоохранение делает шаг в будущее // Медицинские технологии. Оценка и выбор. 2017. №4 (30). С. 30–31.
83. Литвинов А. Крупные и интересные MVNO-проекты: // Telecomdaily. [Электронный ресурс]. URL: https://telecomdaily.ru/news/2021/07/01/andrey-litvinov-plintron-rossiya-sleduyushchie-krupnye-i-interesnye-mvno-proekty-my-uvidim-s-uchastiem-riteyla (дата доступа: 15.03.2022)
84. Маликова О. Н. Основные направления развития IP-телефонии / О. Н. Маликова, А. С. Кручинин // Инновационные технологии, экономика и менеджмент в промышленности : Сборник научных статей по итогам IV международной научной конференции, Волгоград, 22–23 апреля 2021 года. – Волгоград: Общество с ограниченной ответственностью "КОНВЕРТ", 2021. – С. 218-219.

85. Масич А.Г., Масич Г.Ф. От «Инициативы GIGA UrB RAS» к киберинфраструктуре УрО РАН // Вестник Пермского федерального исследовательского центра. 2009. №4. С. 41–56.
86. Межгосударственный стандарт телеобработка данных и вычислительные сети Термины и определения. 1989-07-01. № 24402-88 // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200015767#7D20K3 (дата обращения: 01.03.2022).
87. Международная IT-компания «Taraspan»: IP Telephony: A Complete Guide to Understanding IP Telephony in 2020 [Электронный ресурс] URL: https://www.taraspan.com/blog/ip-telephony-a-complete-guide/#Second_heading
88. Наумов А.И.: Преимущества и особенности IP-телефонии // Научный аспект том 8 выпуск №4 2020. С. 1046–1047.
89. Национальный открытый университет «Интуит» [Электронный ресурс] URL:https://intuit.ru/studies/courses/8/8/lecture/239
90. Нормативные правовые акты в сфере связи. — Текст : электронный // Роскомнадзор : [сайт]. — URL: https://77.rkn.gov.ru/law/p1815/ (дата обращения: 22.03.2022).
91. Описание уровня PDCP LTE [Электронный ресурс]. URL: http://anisimoff.org/lte/pdcp.html (Дата обращения 13.03.2022)
92. Основы IP-телефонии, базовые принципы, термины и протоколы [Электронный ресурс] URL: https://habr.com/ru/post/183152/
93. Платформа vc.ru, статья «Обзор ведущих операторов IP-телефонии» [Электронный ресурс] URL: https://vc.ru/services/246942-obzor-vedushchih-operatorov-ip-telefonii.
94. Построение сетей MVNO \ MVNE для виртуальных операторов сотовой связи: [Электронный ресурс]. URL: https://www.quintatec.com/section/19/109/. (дата доступа: 15.03.2022)
95. Почему SIP лучше, чем H.323 [Электронный ресурс]. URL: https://trueconf.ru/blog/reviews/pochemu-sip-luchshe-chem-h-323.html (Дата обращения 12.03.2022)
96. Продукты ViPNet | ИнфоТеКС // ИнфоТеКС — https://infotecs.ru/ — Безопасность информационных систем и защита данных URL: https://infotecs.ru/downloads/documentacii/ (дата обращения: 05.03.2022).
97. Пролетарский А.В. Технологии TCP/IP в современных компьютерных сетях. Учебное пособие. МГТУ, 2020. – 638 с.
98. Протокол инициирования сеансов связи – SIP [Электронный ресурс] URL: http://iptop.net/sip/
99. Реализация True End-to-End Encryption, используя WebRTC Insertable Streams [Электронный ресурс]. – Режим доступа: https://webrtchacks.com/true-end-to-end-encryption-with-webrtc-insertable-streams/. – Дата доступа: 20.03.2022.

100. Росляков, А.В. IP-телефония, издание второе / А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева. Москва, 2003.
101. Российские решения для MVNO/MVNE: [Электронный ресурс]. URL: https://protei.ru/solutions/virtualnym-operatoram-mvnomvne. (дата доступа: 17.03.2022)
102. Русев Е. Применение технологии IP–телефонии для малого и среднего бизнеса: преимущества, недостатки, перспективы развития // Экономическая среда. 2018. №4(26). С. 18–24.
103. Серверные компоненты | ИнфоТеКС // ИнфоТеКС — https://infotecs.ru/ — Безопасность информационных систем и защита данных URL: https://infotecs.ru/product/setevye-komponenty/ (дата обращения: 05.03.2022).
104. Скуратовский Б. 4G и 5G: Ключевые различия между двумя поколениями сотовых сетей [Электронный ресурс]. URL: https://mediasat.info/2020/12/28/klyuchevye-razlichiya-4g-i-5g/#:~:text=% (Дата обращения: 16.03.2022).
105. СпОС компоненты: [Электронный ресурс]. URL: https://osnovalab.ru/solutions/voice/mvno/. (дата доступа: 15.03.2022)
106. Сравнение VoLTE и VoIP [Электронный ресурс]. URL: http://anisimoff.org/lte/volte_advantages.html (Дата обращения 13.03.2022)
107. Статистика по популярности видеоконференций в браузере [Электронный ресурс]. – Режим доступа: https://www.data.ai/en/insights/market-data/video-conferencing-apps-surge-coronavirus/. – Дата доступа: 20.03.2022.
108. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. Москва, Санкт-Петербург, Нижний Новгород, Воронеж, Ростов-на-Дону, Екатеринбург, Самара, Новосибирск, Киев, Харьков, Минск: Питер, 2012. 960 с.
109. Теле-соты: Настройка VoIP FXS шлюза Yeastar Neogate TAXXX для работы с 3CX // [Электронный ресурс] URL: https://ambersoti.ru/polezno-znat/golosovoj-shlyuz-dlya-ip-telefonii.html
110. Теле-соты: Настройка VoIP FXS шлюза Yeastar Neogate TAXXX для работы с 3CX // [Электронный ресурс] URL: https://ambersoti.ru/polezno-znat/golosovoj-shlyuz-dlya-ip-telefonii.html
111. Термины и определения: // Сотовая связь: история, стандарты, технологии. [Электронный ресурс]. URL: http://celnet.ru/def.php. (дата доступа: 16.03.2022)
112. Типы компьютерных сетей (классификация компьютерных сетей) // ITandLife.ru URL: https://itandlife.ru/technology/computer-networks/tipy-kompyuternyx-setej-klassifikaciya-kompyuternyx-setej/ (дата обращения: 01.03.2022).
113. Учебник по IP–телефонии [Электронный ресурс] URL: http://docplayer.com/26156301-Uchebnik-po-ip-telefonii.html
114. Федеральный закон от 27.07.2006 № 152-ФЗ (в ред. От 02.07.2021) «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31 (часть I). Ст. 3451.

115. Формула коэффициента корреляции Пирсона. — Текст : электронный // statpsy.ru : [сайт]. URL: https://statpsy.ru/pearson/formula-pirsona/ (дата обращения: 17.03.2022).
116. Цены, прайс-лист на 2022 год | ИнфоТеКС // ИнфоТеКС — https://infotecs.ru/ — Безопасность информационных систем и защита данных URL: https://infotecs.ru/product/prices.php (дата обращения: 05.03.2022).
117. Чем IoT может быть полезен MVNO: [Электронный ресурс]. URL: https://telcojournal.mcn.ru/iot-mvno-svyaz/. (дата доступа: 16.03.2022)
118. Что такое QoS: понятие и назначение функции Quality of Service // Сервис коллтрекинга и сквозной аналитики Calltouch | Система сквозной аналитики на основе call tracking-а URL: https://www.calltouch.ru/glossary/qos/ (дата обращения: 01.03.2022).
119. Что такое SIP телефония // МТТ [Электронный ресурс]. URL: https://www.mtt.ru/blog/chto-takoe-sip-telefoniia/ (дата доступа 14.03.2022)
120. Шалагинов А. Бизнес-модель конвергентного MVNO: // Telecom & IT. [Электронный ресурс]. URL: https://shalaginov.com/2017/03/31/бизнес-модель-конвергентного-mvno/. (дата доступа: 17.03.2022)
121. Электронная версия Национальной библиотеки им. Н. Э. Баумана [Электронный ресурс] URL: https://ru.bmstu.wiki/Сетевая_модель_OSI

Билятдинов Камиль Закирович
Арсеньева Анна Закировна
Меняйло Вера Владимировна

ТЕХНОЛОГИИ IP-ТЕЛЕФОНИИ

Учебное пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ № 4671
Тираж 100 экз.
Отпечатано ООО «Университетские Телекоммуникации»
199034, Санкт-Петербург, В.О., Биржевая линия, 16

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49