МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕ - СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН

Акционерное общество «ЎЗБЕКИСТОН ТЕМИР ЙЎЛЛАРИ»

Ташкентский институт инженеров железнодорожного транспорта

На правах рукописи

УДК 621.395.34

Бахромов Х.Б.

«Принципы реализации IP-телефонии»

Специальность: 5А350102-Устройства и системы передачи информации

Диссертация
на соискание ученой степени магистра

Научный руководитель
Д.т.н.,проф. Халиков А.А.
_____

Ташкент-2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

СТРАТЕГИЯ ДЕЙСТВИЙ

по пяти приоритетным направлениям развития Республики Узбекистан в 2017-2021 годах

Развитие сферы образования и науки:

- продолжение курса дальнейшего совершенствования системы непрерывного образования, повышения доступности качественных образовательных услуг, подготовки высококвалифицированных кадров

- в соответствии с современными потребностями рынка труда; осуществление целенаправленных мер по укреплению материально-технической базы образовательных учреждений путем проведения работ по их строительству, реконструкции и капитальному ремонту, оснащение современным учебным и лабораторным оборудованием, компьютерной техникой, учебно-методическими пособиями;

- расширение сети дошкольных образовательных учреждений, коренное улучшение условий в дошкольных образовательных учреждениях для всестороннего интеллектуального, эстетического и физического развития детей, обеспечение доступности и значительного повышения охвата детей дошкольным образованием, повышение уровня квалификации педагогов и специалистов;

- кардинальное повышение качества общего среднего образования, углубленное изучение иностранных языков, информатики, других важных и востребованных предметов, включая математику, физику, химию, биологию;

- строительство новых, реконструкция существующих объектов детского спорта и детских школ музыки и искусства в целях привлечения детей

к массовым занятиям спортом, приобщению их к миру музыки и искусства;

- совершенствование работ по подготовке и трудоустройству учащихся профессиональных колледжей по специальностям, отвечающим требованиям

рыночной экономики и потребностям работодателей;

- повышение качества и эффективности деятельности высших образовательных учреждений на основе внедрения международных стандартов обучения и оценки качества преподавания, поэтапное увеличение квоты приема в высшие образовательные учреждения;

- стимулирование научно-исследовательской и инновационной деятельности, создание эффективных механизмов внедрения научных и инновационных достижений в практику, создание при вузах и НИИ научно-экспериментальных специализированных лабораторий, центров высоких технологий, технопарков.

Совершенствование государственной молодежной политики:

- воспитание физически здоровой, духовно и интеллектуально развитой, самостоятельно мыслящей, преданной Родине молодежи с твердыми жизненными взглядами, повышение его социальной активности в процессе углубления демократических реформ и развития гражданского общества;

- трудоустройство и привлечение в сферу частного предпринимательства выпускников средних специальных, профессиональных и высших образовательных учреждений;

- поддержка и реализация творческого и интеллектуального потенциала молодого поколения, формирование здорового образа жизни среди детей и молодежи, широкое привлечение их к физической культуре и спорту; социальная защита молодежи, создание для молодых семей достойных жилищных и социально-бытовых условий;

- организация эффективной деятельности органов государственной власти и управления, образовательных учреждений, молодежных и иных организаций в реализации государственной молодежной политики.

У IP-телефонии есть достаточное количествопреимуществ, чтобы вскоре распространиться по всей нашей стране; учитывая экономические аспектыи послание Президента Республики «Лидирующие экономики мира будут функционировать в более сложных, конкурентных условиях и предпримут превентивные меры по подготовке к следующему экономическому циклу, наращивая производительность рабочей силы, инвестирование в инфраструктуру и телекоммуникации, укрепляя финансовые системы, повышая эффективность государственного управления, а также создавая благоприятные условия для развития бизнеса».

VoIP — система связи, обеспечивающая передачу речевого сигнала по сети Интернет или по любым другим IP-сетям. Сигнал по каналу связи передаётся в цифровом виде и, как правило, перед передачей преобразовывается (сжимается) с тем, чтобы удалить избыточность.

Осталось в прошлом то время, когда операторы с опасением относились к использованию IP-телефонии, считая уровень защищенности таких сетей низким. Сегодня уже можно говорить о том, что IP-телефония стала неким стандартом в телефонных коммуникациях. Это объясняется удобством, относительной надежностью и относительно невысокой стоимостью IP-телефонии по сравнению с аналоговой связью. Можно утверждать, что IP-телефония повышает эффективность ведения бизнеса и позволяет осуществлять такие ранее недоступные операции, как интеграция с различными бизнес-приложениями.

Если говорить о недостатках и уязвимостях IP-телефонии, прежде всего следует отметить те же «болезни», какими страдают другие службы, использующие протокол IP. Несмотря на то, что при построении инфраструктуры IP-телефонии данную службу обычно отделяют от сегментов сети, в которых «ходят» не голосовые данные, это еще не является гарантией безопасности. Сегодня большое количество компаний интегрируют IP-телефонию с другими приложениями, например с электронной почтой. С одной стороны, таким образом появляются

дополнительные удобства, но с другой — и новые уязвимости. Кроме того, для функционирования сети IP-телефонии требуется большое число компонентов, таких, как серверы поддержки, коммутаторы, маршрутизаторы, межсетевые экраны, IP-телефоны и т. д.[2].

Среди основных угроз, которым подвергается IP-телефонная сеть, можно выделить:

– регистрацию чужого терминала, позволяющую делать звонки за чужой счет;

– подмену абонента;

– внесение изменений в голосовой или сигнальный трафик;

– снижение качества голосового трафика;

– перенаправление голосового или сигнального трафика;

– перехват голосового или сигнального трафика;

– подделка голосовых сообщений;

– завершение сеанса связи;

– отказ в обслуживании;

– удаленный несанкционированный доступ к компонентам инфраструктуры IP-телефонии;

– несанкционированное обновление ПО на IP-телефоне (например, с целью внедрения троянской или шпионской программы);

– взлом биллинговой системы (для операторской телефонии).

Это далеко не весь перечень возможных проблем, связанных с использованием IP-телефонии. Альянс по безопасности VoIP (VOIPSA) разработал документ, описывающий широкий спектр угроз IP-телефонии, который помимо технических угроз включает вымогательство через IP-телефонию, спам и т. д.

И все же основное уязвимое место IP-телефонии — это набивший оскомину человеческий фактор. Проблема защищенности при развертывании IP-телефонной сети часто отодвигается на задний план, и выбор решения

проходит без участия специалистов по безопасности. К тому же специалисты не всегда должным образом настраивают решение, даже если в нем присутствуют надлежащие защитные механизмы, либо приобретаются средства защиты, не предназначенные для эффективной обработки голосового трафика (например, межсетевые экраны могут не понимать фирменный протокол сигнализации, использующийся в решении IP-телефонии). В конце концов, организация вынуждена тратить дополнительные финансовые и людские ресурсы для защиты развернутого решения либо мириться с его незащищенностью [3].

Актуальность темы. Сегодня большое количество компаний интегрируют IP-телефонию с другими приложениями, например с электронной почтой. С одной стороны, таким образом появляются дополнительные удобства, но с другой — и новые уязвимости. Кроме того, для функционирования сети IP-телефонии требуется большое число компонентов, таких, как серверы поддержки, коммутаторы, маршрутизаторы, межсетевые экраны, IP-телефоны и т. д. И все же основное уязвимое место IP-телефонии — это набивший оскомину человеческий фактор. Проблема защищенности при развертывании IP-телефонной сети часто отодвигается на задний план, и выбор решения проходит без участия специалистов по безопасности. К тому же специалисты не всегда должным образом настраивают решение, даже если в нем присутствуют надлежащие защитные механизмы, либо приобретаются средства защиты, не предназначенные для эффективной обработки голосового трафика (например, межсетевые экраны могут не понимать фирменный протокол сигнализации, использующийся в решении IP-телефонии).

Целью магистерской диссертации является принципы реализации IP-телефонии с учетом безопасности.

Научная новизна работы заключается в:

– удаленный несанкционированный доступ к компонентам инфраструктуры IP-телефонии;

– несанкционированное обновление ПО на IP-телефоне (например, с целью внедрения троянской или шпионской программы);

– взлом биллинговой системы (для операторской телефонии).

Практическое значение– Сегодня уже можно говорить о том, что IP-телефония стала неким стандартом в телефонных коммуникациях. Это объясняется удобством, относительной надежностью и относительно невысокой стоимостью IP-телефонии по сравнению с аналоговой связью. Можно утверждать, что IP-телефония повышает эффективность ведения бизнеса при практическом применение и позволяет осуществлять такие ранее недоступные операции, как интеграция с различными бизнес-приложениями.

Апробация работы. Материалы магистерской диссертационной работы докладывались и обсуждались на научных семинарах кафедры «Электрическая связь и радио», а также на научно-методической конференции студентов, аспирантов и соискателей в ТашИИте.

Структура и объем работы. Диссертация состоит из введения, трёх глав, заключения, приложений и списка литературы. Она содержит 70 страниц машинописного текста, 18 рисунков, а так же, 27 список литературы из наименований.

Публикации по теме диссертации:

1. Тема «Обзор сети IP-телефонии», «Ёш илмий тадкикотчи» 2017 йил 4-5 апрель, научный руководитель: Д.т.н.,проф. Халиков А.А. магистрант: Бахромов Х.
2. Тема «Место модульного обучения в современном образовании», «Илмий-педагогик ишларнинг долзарб муаммолари» 2017 йил 27 ноябрь, научный руководитель: Д.т.н.,проф. Халиков А.А. магистрант: Бахромов Х.
3. Тема «Типы угроз IP-Телефонии», «Ёш илмий тадкикотчи» 2018 йил 3-4 апрель, научный руководитель: Д.т.н.,проф. Халиков А.А. магистрант: Бахромов Х.

1. ПОСТРОЕНИЕ СЕТИ IP-ТЕЛЕФОНИИ

1.1. Транспортные технологии пакетной коммутации

Большинство производителей, располагающих широким ассортиментом продукции для пакетной телефонии, занимают «технологически нейтральное» положение и предоставляют покупателю возможность самому выбирать ту технологию, которая лучше всего соответствует его интеграционной стратегии.

Основные технологии пакетной передачи речи - FrameRelay, ATM и маршрутизация пакетов IP - различаются эффективностью использования каналов связи, степенью охвата разных участков сети, надежностью, управляемостью, защитой информации и доступа, а также стоимостью [3].

Транспортная технология ATM уже несколько лет успешно используется в магистральных сетях общего пользования и в корпоративных сетях, а сейчас ее начинают активно использовать и для высокоскоростного доступа по каналам xDSL (для небольших офисов) и SDH/Sonet (для крупных предприятий). Главные преимущества этой технологии - ее зрелость, надежность и наличие развитых средств эксплуатационного управления сетью. В ней имеются непревзойденные по своей эффективности механизмы управления качеством обслуживания и контроля использования сетевых ресурсов. Однако ограниченная распространенность и высокая стоимость оборудования не позволяют считать ATM лучшим выбором для организации сквозных телефонных соединений от одного конечного узла до другого.

Технологии FrameRelay суждено было сыграть в пакетной телефонии ту же роль, что и квазиэлектронным АТС в телефонии с коммутацией каналов: они показали пример эффективной программно управляемой техники, но имели ограниченные возможности дальнейшего развития. Пользователями недорогих услуг FrameRelay, обеспечивающих вполне предсказуемую производи-тельность, стали многие корпоративные сети, и большинство из них вполне довольны своим выбором. В краткосрочной

перспективе технология передачи речи по FrameRelay будет вполне эффективна для организации мультисервисного доступа и каналов дальней связи. Но сети FrameRelay распространены незначительно: как правило, на практике используются некоммутируемые соединения в режиме точка-точка [3].

Технология передачи речевой информации по сетям с маршрутизацией пакетов IP привлекает, в первую очередь, своей универсальностью - речь может быть преобразована в поток IP-пакетов в любой точке сетевой инфраструктуры: на магистрали сети оператора, на границе территориально распределенной сети, в корпоративной сети и даже непосредственно в терминале конечного пользователя. В конце концов, она станет наиболее широко распространенной технологией пакетной телефонии, поскольку способна охватить все сегменты рынка, будучи при этом хорошо адаптируемой к новым условиям применения. Несмотря на универсальность протокола IP, внедрение систем IP-телефонии сдерживается тем, что многие операторы считают их недостаточно надежными, плохо управляемыми и не очень эффективными. Но грамотно спроектированная сетевая инфраструктура с эффективными механизмами обеспечения качества обслуживания делает эти недостатки малосущественными. В расчете на порт стоимость систем IP-телефонии находится на уровне (или немного ниже) стоимости систем FrameRelay, и заведомо ниже стоимости оборудования ATM. При этом уже сейчас видно, что цены на продукты IP-телефонии снижаются быстрее, чем на другие изделия, и что происходит значительное обострение конкуренции на этом рынке.

1.2. Уровни архитектуры IP-телефонии

Архитектура технологии Voiceover IP может быть упрощенно представлена в виде двух плоскостей. Нижняя плоскость - это базовая сеть с маршрутизацией пакетов IP, верхняя плоскость - это открытая архитектура управления обслуживанием вызовов (запросов связи).

Нижняя плоскость, говоря упрощенно, представляет собой комбинацию известных протоколов Интернет: это - RTP (RealTimeTransportProtocol), который функционирует поверх протокола UDP (UserDatagramProtocol), расположенного, в свою очередь, в стеке протоколов TCP/IP над протоколом IP. Таким образом, иерархия RTP/UDP/IP представляет собой своего рода транспортный механизм для речевого трафика. Здесь же отметим, что в сетях с маршрутизацией пакетов IP для передачи данных всегда предусматриваются механизмы повторной передачи пакетов в случае их потери. При передаче информации в реальном времени использование таких механизмов только ухудшит ситуацию, поэтому для передачи информации, чувствительной к задержкам, но менее чувствительной к потерям, такой как речь и видеоинформация, используется механизм негарантированной доставки информации RTP/UDPD/IP. Рекомендации ITU-T допускают задержки в одном направлении не превышающие 150 мс. Если приемная станция запросит повторную передачу пакета IP, то задержки при этом будут слишком велики [4].

Теперь перейдем к верхней плоскости управления обслуживанием запросов связи. Вообще говоря, управление обслуживанием вызова предусматривает принятие решений о том, куда вызов должен быть направлен, и каким образом должно быть установлено соединение между абонентами. Инструмент такого управления - телефонные системы сигнализации, начиная с систем, поддерживаемых декадно-шаговыми АТС и предусматривающих объединение функций маршрутизации и функций создания коммутируемого разговорного канала в одних и тех же декадно-шаговых искателях. Далее принципы сигнализации эволюционировали к системам сигнализации по выделенным сигнальным каналам, к многочастотной сигнализации, к протоколам общеканальной сигнализации №7 и к передаче функций маршрутизации в соответствующие узлы обработки услуг Интеллектуальной сети.

В сетях с коммутацией пакетов ситуация более сложна. Сеть с маршрутизацией пакетов IP принципиально поддерживает одновременно целый ряд разнообразных протоколов маршрутизации [5].

Такимипротоколаминасегодняявляются: RIP - Routing Information Protocol, IGRP - Interior Gateway Routing Protocol, EIGRP – Enhanced Interior Gateway Routing Protocol, IS-IS - Intermediate System-to- intermediate System, OSPF - Open Shortest Path First, BGP – Border Gateway Protocol идр. Точно так же и для IP-телефонии разработан целый ряд протоколов.

Наиболее распространенным является протокол, специфицированный в рекомендации H.323 ITU-T, в частности, потому, что он стал применяться раньше других протоколов, которых, к тому же, до внедрения H.323 вообще не существовало.

Другой протокол плоскости управления обслуживанием вызова - SIP - ориентирован на то, чтобы сделать оконечные устройства и шлюзы более интеллектуальными и поддерживать дополнительные услуги для пользователей.

Еще один протокол - SGCP - разрабатывался, начиная с 1998 года, для того, чтобы уменьшить стоимость шлюзов за счет реализации функций интеллектуальной обработки вызова в централизованном оборудовании. Протокол IPDC очень похож на SGCP, но имеет много больше, чем SGCP, механизмов эксплуатационного управления (OAM&P). В конце 1998 года рабочая группа MEGACO комитета IETF разработала протокол MGCP, базирующийся, в основном, на протоколе SGCP, но с некоторыми добавлениями в части OAM&P.

Рабочая группа MEGACO не остановилась на достигнутом, продолжала совершенствовать протокол управления шлюзами и разработала более функциональный, чем MGCP, протокол MEGACO [2].

1.3. Различные подходы к построению сетей IP-телефонии

Чтобы стало понятно, чем конкретно отличаются друг от друга протоколы, кратко рассмотрю архитектуру сетей, построенных на базе этих протоколов, и процедуры установления и завершения соединения с их использованием [2].

1.3.1. Построение сети по рекомендации H.323

Первый в истории подход к построению сетей IP-телефонии на стандартизованной основе предложен Международным союзом электросвязи (ITU) в рекомендации H.323. Сети на базе протоколов H.323 ориентированы на интеграцию с телефонными сетями и могут рассматриваться как сети ISDN, наложенные на сети передачи данных. В частности, процедура установления соединения в таких сетях IP-телефонии базируется на рекомендации Q.931 и аналогична процедуре, используемой в сетях ISDN.

Рекомендация H.323 предусматривает довольно сложный набор протоколов, который предназначен не просто для передачи речевой информации по IP-сетям с коммутацией пакетов. Его цель - обеспечить работу мультимедийных приложений в сетях с негарантированным качеством обслуживания. Речевой трафик - это только одно из приложений H.323, наряду с видеоинформацией и данными.

Вариант построения сетей IP-телефонии, предложенный Международным союзом электросвязи в рекомендации H.323, хорошо подходит тем операторам местных телефонных сетей, которые заинтересованы в использовании сети с коммутацией пакетов (IP-сети) для предоставления услуг междугородной и международной связи. Протокол RAS, входящий в семейство протоколов H.323, обеспечивает контроль использования сетевых ресурсов, поддерживает аутентификацию пользователей и может обеспечивать начисление платы за услуги.

На рисунке представлена архитектура сети на базе рекомендации H.323. Основными устройствами сети являются: терминал (Terminal), шлюз

(Gateway), привратник (Gatekeeper) и устройство управления конференциями (MultipointControlUnit- MCU).

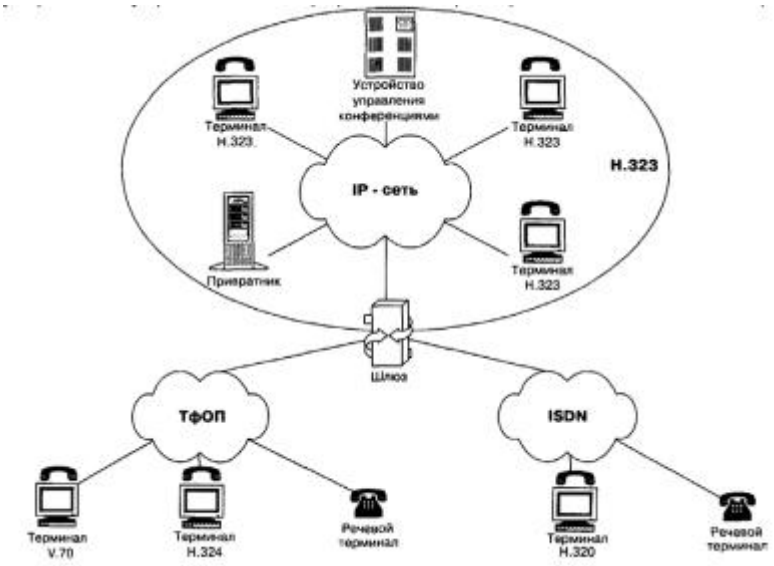

Рис.1.1. Архитектура сети H.323

Терминал H.323 - оконечное устройство пользователя сети IP-телефонии, которое обеспечивает двухстороннюю речевую (мультимедийную) связь с другим терминалом H.323, шлюзом или устройством управления конференциями [2].

Шлюз IP-телефонии реализует передачу речевого трафика по сетям с маршрутизацией пакетов IP по протоколу H.323. Основное назначение шлюза - преобразование речевой информации, поступающей со стороны ТФОП, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP. Кроме того, шлюз преобразует сигнальные сообщения систем сигнализации DSS1 и ОКС7 в сигнальные сообщения H.323 и производит обратное преобразование в соответствии с рекомендацией ITU H.246.

В привратнике сосредоточен весь интеллект сети IP-телефонии.

Сеть, построенная в соответствии с рекомендацией H.323, имеет зонную архитектуру. Привратник выполняет функции управления одной зоной сети IP-телефонии, в которую входят: терминалы, шлюзы, устройства

управления конференциями, зарегистрированные у данного привратника. Отдельные фрагменты зоны сети H.323 могут быть территориально разнесены и соединяться друг с другом через маршрутизаторы.

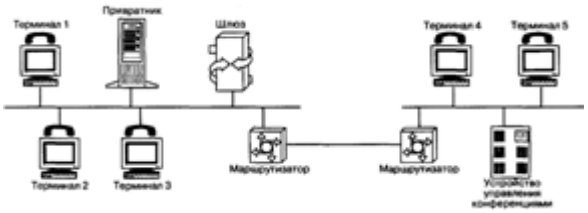

Рис.1.2. Зона сети H.323

Наиболее важными функциями привратника являются:

– регистрация оконечных и других устройств;

– контроль доступа пользователей системы к услугам IP-телефонии при помощи сигнализации RAS;

– преобразование вызываемого пользователя (объявленного имени абонента, телефонного номера, адреса электронной почты и др.) в транспортный адрес сетей с маршрутизацией пакетов IP (IP адрес + номер порта TCP);

– контроль, управление и резервирование пропускной способности сети;

– ретрансляция сигнальных сообщений H.323 между терминалами.

В одной сети IP-телефонии, отвечающей требованиям рекомендации ITU H.323, может находиться несколько привратников, взаимодействующих друг с другом по протоколу RAS.

Кроме основных функций, определенных рекомендацией H.323, привратник может отвечать за аутентификацию пользователей и начисление платы (биллинг) за телефонные соединения. Устройство управления конференциями обеспечивает возможность организации связи между тремя или более участниками [4].

Рекомендация H.323 предусматривает три вида конференции: централизованная (т.е. управляемая MCU, с которым каждый участник конференции соединяется в режиме точка-точка), децентрализованная (когда каждый участник конференции соединяется с остальными ее участниками в режиме точка-группа точек) и смешанная.

Преимуществом централизованной конференции является сравнительно простое терминальное оборудование, недостатком - большая стоимость устройства управления конференциями.

Для децентрализованной конференции требуется более сложное терминальное оборудование и желательно, чтобы в сети IP поддерживалась передача пакетов IP в режиме многоадресной рассылки (IP multicasting). Если этот режим в сети не поддерживается, терминал должен передавать речевую информацию каждому из остальных участников конференции в режиме точка-точка.

Устройство управления конференциями состоит из одного обязательного элемента - контроллера конференций (MultipointController - MC), и, кроме того, может включать в себя один или более процессоров для обработки пользовательской информации (MultipointProcessor - MP). Контроллер может быть физически совмещен с привратником, шлюзом или устройством управления конференциями, а последнее, в свою очередь, может быть совмещено со шлюзом или привратником.

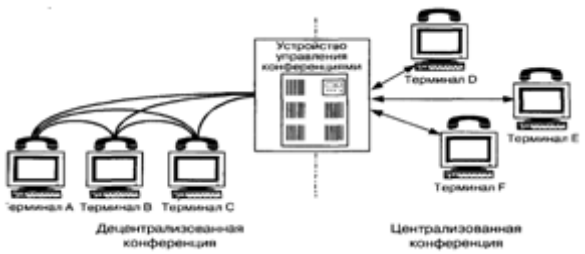

Рис.1.3. Виды конференции в сетях H.323

Контроллер конференций используется для организации конференции любого вида. Он организует обмен между участниками конференции данными о режимах, поддерживаемых их терминалами, и указывает, в каком режиме участники конференции могут передавать информацию, причем в ходе конференции этот режим может изменяться, например, при подключении к ней нового участника.

Так как контроллеров в сети может быть несколько, для каждой вновь создаваемой конференции должна быть проведена специальная процедура выявления того контроллера, который будет управлять данной конференцией. При организации централизованной конференции, кроме контроллера MC, должен использоваться процессор MP, обрабатывающий пользовательскую информацию. Процессор MP отвечает за переключение или смешивание речевых потоков, видеоинформации и данных. Для децентрализованной конференции процессор не нужен [5].

Существует еще один элемент сети H .323 - прокси-сервер H.323, т.е. сервер-посредник. Этот сервер функционирует на прикладном уровне и может проверять пакеты с информацией, которой обмениваются два приложения. Прокси-сервер может определять, с каким приложением (H.323 или другим) ассоциирован вызов, и осуществлять нужное соединение. Прокси-сервер выполняет следующие ключевые функции:

– подключение через средства коммутируемого доступа или локальные сети терминалов, не поддерживающих протокол резервирования ресурсов (RSVP). Два таких прокси-сервера могут образовать в IP-сети туннельное соединение с заданным качеством обслуживания;

– маршрутизацию трафика H.323 отдельно от обычного трафика данных;

– обеспечение совместимости с преобразователем сетевых адресов, поскольку допускается размещение оборудования H.323 в сетях с пространством адресов частных сетей;

– защиту доступа - доступность только для трафика H.323.

Протокол RAS (RegistrationAdmissionStatus) обеспечивает взаимодействие оконечных и других устройств с привратником.

Основными функциями протокола являются: регистрация устройства в системе, контроль его доступа к сетевым ресурсам, изменение полосы пропускания в процессе связи, опрос и индикация текущего состояния устройства. В качестве транспортного протокола используется протокол с негарантированной доставкой информации UDP.

Протокол H.225.0 (Q.931) поддерживает процедуры установления, поддержания и разрушения соединения. В качестве транспортного протокола используется протокол с установлением соединения и гарантированной доставкой информации TCP.

По протоколу H.245 происходит обмен между участниками соединения информацией, которая необходима для создания логических каналов. По этим каналам передается речевая информация, упакованная в пакеты RTP/UDP/IP.

Выполнение процедур, предусмотренных протоколом RAS, является начальной фазой установления соединения с использованием сигнализации H.323. Далее следуют фаза сигнализации H.225.0 (Q.931) и обмен управляющими сообщениями H.245. Разрушение соединения происходит в обратной последовательности: в первую очередь закрывается управляющий канал H.245 и сигнальный канал H.225.0, после чего привратник по каналу RAS оповещается об освобождении ранее занимавшейся полосы пропускания [2].

Сложность протокола H.323 демонстрирует рисунок 1.7, на котором представлен упрощенный сценарий установления соединения между двумя пользователями. В данном сценарии предполагается, что конечные пользователи уже знают IP-адреса друг друга. В обычном случае этапов бывает больше, поскольку в установлении соединения участвуют привратники и шлюзы.

Рассмотрим шаг за шагом этот упрощенный сценарий.

1) Оконечное устройство пользователя А посылает запрос соединения - сообщение SETUP - к оконечному устройству пользователя В на TCP-порт1720;

2) Оконечное устройство вызываемого пользователя В отвечает на сообщение SETUP сообщением ALERTING, означающим, что устройство свободно, а вызываемому пользователю подается сигнал о входящем вызове;

3) После того, как пользователь В принимает вызов, к вызывающей стороне А передается сообщение CONNECT с номером TCP-порта управляющего канала H.245;

4) Оконечные устройства обмениваются по каналу H.245 информацией о типах используемых речевых кодеков (G.729, G.723.1 и т.д.), а также о других функциональных возможностях оборудования, и оповещают друг друга о номерах портов RTP, на которые следует передавать информацию;

5) Открываются логические каналы для передачи речевой информации;

6) Речевая информация передаётся в обе стороны в сообщениях протокола RTP; кроме того, ведется контроль передачи информации при помощи протокола RTCP.

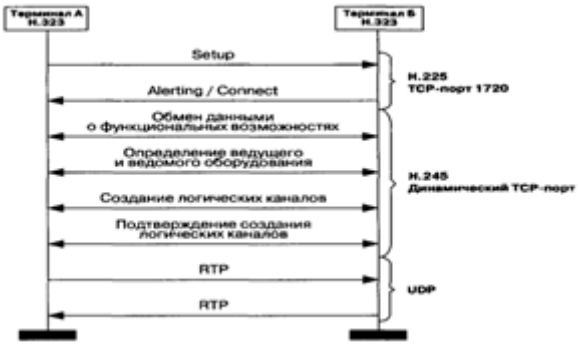

Рис.1.4. Упрощённый сценарий установления соединения в сети H.323

Приведенная процедура обслуживания вызова базируется на протоколе H.323 версии 1. Версия 2 протокола H.323 позволяет передавать информацию, необходимую для создания логических каналов, непосредственно в сообщении SETUP протокола H.225.0 без использования

протокола H.245. Такая процедура называется «быстрый старт» (FastStart) и позволяет сократить количество циклов обмена информацией при установлении соединения. Кроме организации базового соединения, в сетях H.323 предусмотрено предоставление дополнительных услуг в соответствии с рекомендациями ITU H.450.X [5].

Следует отметить еще одну важную проблему - качество обслуживания в сетях H.323. Оконечное устройство, запрашивающее у привратника разрешение на доступ, может, используя поле transportQoS в сообщении ARQ протокола RAS, сообщить о своей способности резервировать сетевые ресурсы. Рекомендация H.323 определяет протокол резервирования ресурсов (RSVP) как средство обеспечения гарантированного качества обслуживания, что предъявляет к терминалам требование поддержки протокола RSVP. К сожалению, протокол RSVP используется отнюдь не повсеместно, что оставляет сети H.323 без основного механизма обеспечения гарантированного качества обслуживания. Это - общая проблема сетей IP-телефонии, характерная не только для сетей H.323.

1.3.2. Сеть на базе протокола SIP

Второй подход к построению сетей IP-телефонии, предложенный рабочей группой MMUSIC комитета IETF в документе RFC 2543, основан на использовании протокола SIP - SessionInitiationProtocol [7].

SIP представляет собой текстоориентированный протокол, который является частью глобальной архитектуры мультимедиа, разработанной комитетом InternetEngineeringTaskForce (IETF). Эта архитектура также включает в себя протокол резервирования ресурсов (ResourceReservationProtocol, RSVP, RFC 2205), транспортный протокол реального времени (Real-TimeTransportProtocol, RTP, RFC 1889), протокол передачи потоков в реальном времени (Real-TimeStreamingProtocol, RTSP, RFC 2326), протокол описания параметров связи (SessionDescriptionProtocol, SDP, RFC 2327), протокол уведомления о связи

(SessionAnnouncementProtocol, SAP). Однако функции протокола SIP не зависят от любого из этих протоколов.

Сразу следует отметить, что хотя на сегодня наиболее широкое распространение получил протокол H.323, всё большее количество производителей старается предусмотреть в своих новых продуктах поддержку протокола SIP. Пока это - единичные явления и серьезной конкуренции протоколу H.323 они составить не могут. Однако, учитывая темпы роста популярности протокола SIP, весьма вероятно, что в ближайшем будущем решения на его базе займут значительную нишу рынка IP-телефонии.

Подход SIP к построению сетей IP-телефонии намного проще в реализации, чем H.323, но меньше подходит для организации взаимодействия с телефонными сетями. В основном это связано с тем, что протокол сигнализации SIP, базирующийся на протоколе HTTP, плохо согласуется с системами сигнализации, используемыми в ТфОП. Поэтому протокол SIP более подходит поставщикам услуг Интернет для предоставления услуги IP-телефонии, причем эта услуга будет являться всего лишь частью пакета услуг.

Тем не менее, протокол SIP поддерживает услуги интеллектуальной сети (IN), такие как преобразование (мэппинг) имён, переадресация и маршрутизация, что существенно для использования SIP в качестве протокола сигнализации в сети общего пользования, где приоритетной задачей оператора является предоставление широкого спектра телефонных услуг. Другой важной особенностью протокола SIP является поддержка мобильности пользователя, т.е. его способности получать доступ к заказанным услугам в любом месте и с любого терминала, а также способности сети идентифицировать и аутентифицировать пользователя при его перемещении из одного места в другое. Это свойство SIP не уникально, и, например, протокол H.323 тоже в значительной степени поддерживает такую возможность. Сейчас настал момент, когда эта возможность станет главной

привлекательной чертой сетей IP-телефонии нового поколения. Данный режим работы потребует дистанционной регистрации пользователей на сервере идентификации и аутентификации [2].

Перейдем непосредственно к архитектуре сетей, базирующихся на протоколе SIP.

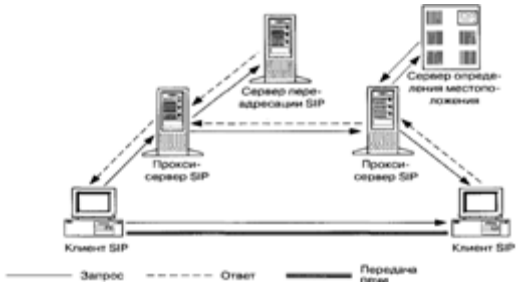

Рис.1.5. Пример сети на базе протокола SIP

Сеть SIP содержит основные элементы трех видов: агенты пользователя, прокси-серверы и серверы переадресации. Агенты пользователя (UserAgent или SIP client) являются приложениями терминального оборудования и включают в себя две составляющие: агент пользователя - клиент (UserAgentClient - UAC) и агент пользователя - сервер (UserAgentServer - UAS), иначе известные как клиент и сервер соответственно. Клиент UAC инициирует SIP-запросы, т.е. выступает в качестве вызывающей стороны. Сервер UAS принимает запросы и возвращает ответы, т.е. выступает в качестве вызываемой стороны.

Кроме того, существует два типа сетевых серверов SIP: прокси-серверы (серверы-посредники) и серверы переадресации. Серверы SIP могут работать как в режиме с сохранением состояний текущих соединений (statefull), так и в режиме без сохранения состояний текущих соединений (stateless). Сервер SIP, функционирующий в режиме stateless, может обслужить сколь угодно большое количество пользователей, в отличие от привратника H.323, который может одновременно работать с ограниченным количеством пользователей.

Прокси-сервер (Proxy-server) действует «от имени других клиентов» и содержит функции клиента (UAC) и сервера (UAS). Этот сервер интерпретирует и может перезаписывать заголовки запросов перед отправкой их к другим серверам (рисунок 1.9). Ответные сообщения следуют по тому же пути обратно к прокси-серверу, а не к клиенту.

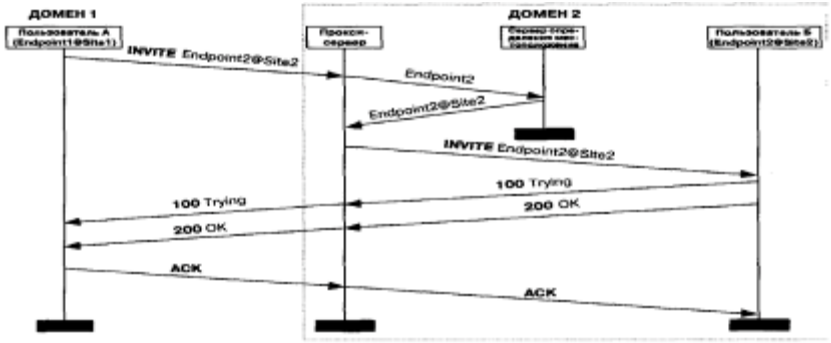

Рис.1.6. Сеть SIP с прокси-сервером

На рисунке представлен алгоритм установления соединения с помощью протокола SIP при участии прокси-сервера:

1) Прокси-сервер принимает запрос соединения INVITE от оборудования вызывающего пользователя;

2) Прокси-сервер устанавливает местонахождение клиента с помощью сервера определения местоположения (locationserver);

3)Прокси-сервер передает запрос INVITE вызываемому пользователю;

4) Оборудование вызываемого пользователя уведомляет последнего о входящем вызове и возвращает прокси-серверу сообщение о том, что запрос INVITE обрабатывается (код 100). Прокси-сервер, в свою очередь, направляет эту информацию оборудованию вызывающего пользователя;

5) Когда вызываемый абонент принимает вызов, его оборудование извещает об этом прокси-сервер (код 200), который переправляет информацию о том, что вызов принят, к оборудованию вызывающего пользователя;

6) Вызывающая сторона подтверждает установление соединения передачей запроса АСК, которое прокси-сервер переправляет вызываемой стороне. Установление соединения закончено, абоненты могут обмениваться речевой информацией [2].

Сервер переадресации (Redirectserver) определяет текущее местоположение вызываемого абонента и сообщает его вызывающему пользователю (рис.1.10). Для определения текущего местоположения вызываемого абонента сервер переадресации обращается к серверу определения местоположения, принципы работы которого в документе RFC 2543 не специфицированы.

Алгоритм установления соединения с использованием протокола SIP при участии сервера переадресации выглядит следующим образом:

1) Сервер переадресации принимает от вызывающей стороны запрос соединения INVITE и связывается с сервером определения местонахождения, который выдает текущий адрес вызываемого клиента;

2) Сервер переадресации передает этот адрес вызывающей стороне. В отличие от прокси-сервера, запрос INVITE к оборудованию вызываемого пользователя сервер переадресации не передает;

3) Оборудование вызывающего пользователя подтверждает завершение транзакции с сервером переадресации запросом АСК;

4) Далее оборудование вызывающего пользователя передает запрос INVITE на адрес, полученный от сервера переадресации;

5) Оборудование вызываемого пользователя уведомляет последнего о входящем вызове и возвращает вызывающему оборудованию сообщение о том, что запрос INVITE обрабатывается (код 100);

6) Когда вызываемый абонент принимает вызов, об этом извещается оборудование вызывающего пользователя (код 200).Установление соединения закончено, абоненты могут обмениваться речевой информацией.

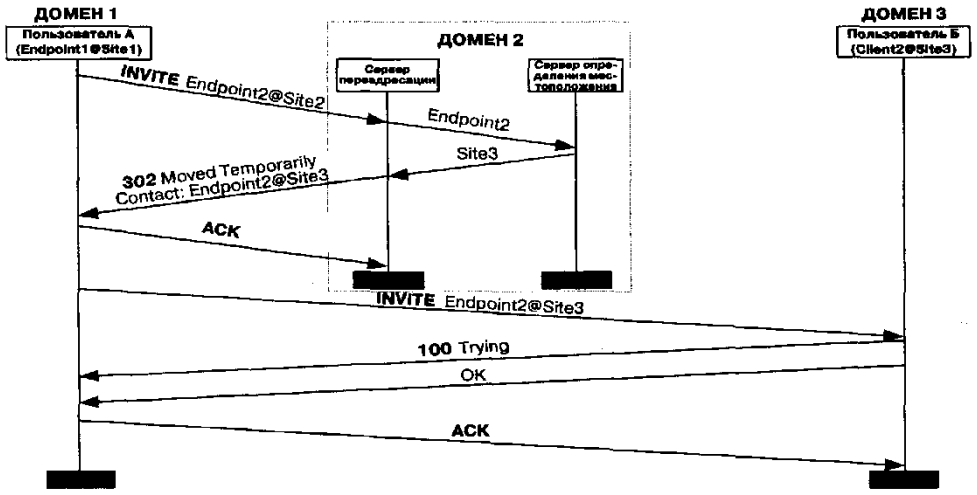

Рис.1.7. Сеть SIP с сервером переадресации

Существует также и бессерверный вариант соединения, когда один терминал может передать запрос другому терминалу непосредственно [4].

Протокол SIP предусматривает 5 запросов и ответов на них.

Сигнализация SIP дает возможность пользовательским агентам и сетевым серверам определять местоположение, выдавать запросы и управлять соединениями.

INVITE - запрос привлекает пользователя или услугу к участию в сеансе связи и содержит описание параметров этой связи. С помощью этого запроса пользователь может определить функциональные возможности терминала своего партнера по связи и начать сеанс связи, используя ограниченное число сообщений и подтверждений их приема.

ACK - запрос подтверждает прием от вызываемой стороны ответа на команду INVITE и завершает транзакцию.

OPTIONS - запрос позволяет получить информацию о функциональных возможностях пользовательских агентов и сетевых серверов. Однако этот запрос не используется для организации сеансов связи.

BYE - запрос используется вызывающей и вызываемой сторонами для разрушения соединения. Перед тем как разрушить соединение,

пользовательские агенты отправляют этот запрос к серверу, сообщая о намерении прекратить сеанс связи.

CANCEL - запрос позволяет пользовательским агентам и сетевым серверам отменить любой ранее переданный запрос, если ответ на нее еще не был получен [5].

1.3.3. Сеть на базе MGCP

Третий подход к построению сетей IP-телефонии, основанный на использовании протокола MGCP, также предложен комитетом IETF, рабочей группой MEGACO.

При разработке этого протокола рабочая группа MEGACO опиралась на сетевую архитектуру, содержащую основные функциональные блоки трех видов:

– шлюз - MediaGateway (MG), который выполняет функции преобразования речевой информации, поступающей со стороны ТфОП с постоянной скоростью передачи, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP (кодирование и упаковку речевой информации в пакеты RTP/UDP/IP, а также обратное преобразование);

– контроллер шлюзов - CallAgent, которой выполняет функции управления шлюзами;

– шлюз сигнализации - SignalingGateway (SG), который обеспечивает доставку сигнальной информации, поступающей со стороны ТфОП, к контроллеру шлюзов и перенос сигнальной информации в обратном направлении.

Таким образом, весь интеллект функционально распределенного шлюза сосредоточен в контроллере, функции которого могут быть распределены между несколькими компьютерными платформами [7].

Шлюз сигнализации выполняет функции STP - транзитного пункта сети сигнализации ОКС7. Сами шлюзы выполняют только функции преобразования речевой информации. Один контроллер управляет

одновременно несколькими шлюзами.В сети могут присутствовать несколько контроллеров.

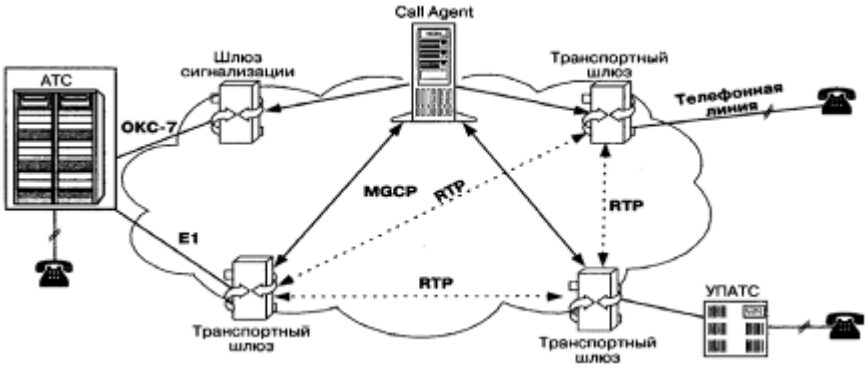

Рис.1.8. Архитектура сети на базе протокола MGCP

Предполагается, что они синхронизованы между собой и согласованно управляют шлюзами, участвующими в соединении. Вместе с тем, MEGACO не определяет протокола для синхронизации работы контроллеров. В ряде работ, посвященных исследованию возможностей протокола MGCP, для этой цели предлагается использовать протоколы H.323, SIP или ISUP/IP. Сообщения протокола MGCP переносятся протоколом без гарантированной доставки сообщений UDP. Рабочая группа SIGTRAN комитета IETF в настоящее время разрабатывает механизм взаимодействия контроллера шлюзов и шлюза сигнализации.

Шлюз сигнализации должен принимать поступающие из ТфОП пакеты трех нижних уровней системы сигнализации ОКС7 (уровней подсистемы переноса сообщений MTP) и передавать сигнальные сообщения верхнего, пользовательского, уровня к контроллеру шлюзов. Шлюз сигнализации также должен уметь передавать по IP-сети приходящие из ТфОП сигнальные сообщения Q.931.

Основное внимание рабочей группы SIGTRAN уделяется вопросам разработки наиболее эффективного механизма передачи сигнальной информации по IP-сетям. Следует отметить, что существует несколько причин, по которым пришлось отказаться от использования для этой цели протокола TCP. Рабочая группа SIGTRAN предлагает использовать для

передачи сигнальной информации протокол StreamControlTransportProtocol (SCTP), имеющий ряд преимуществ перед протоколом TCP, основным из которых является значительное снижение времени доставки сигнальной информации и, следовательно, времени установления соединения - одного из важнейших параметров качества обслуживания.

Если в ТфОП используется сигнализация по выделенным сигнальным каналам (ВСК), то сигналы сначала поступают вместе с пользовательской информацией в транспортный шлюз, а затем передаются в контроллер шлюзов без посредничества шлюза сигнализации [8].

Отметим, что протокол MGCP является внутренним протоколом для обмена информацией между функциональными блоками распределенного шлюза, который извне представляется одним шлюзом. Протокол MGCP является master/slave протоколом. Это означает, что контроллер шлюзов является ведущим, а сам шлюз - ведомым устройством, которое должно выполнять все команды, поступающие от контроллера CallAgent.

Вышеописанное решение обеспечивает масштабируемость сети и простоту управления сетью через контроллер шлюзов. Шлюзы не должны быть интеллектуальными устройствами, требуют меньшей производительности процессоров и, следовательно, становятся менее дорогими. Кроме того, очень быстро вводятся новые протоколы сигнализации или дополнительные услуги, так как эти изменения затрагивают только контроллер шлюзов, а не сами шлюзы.

Третий подход, предлагаемый организацией IETF (рабочая группа MEGACO), хорошо подходит для развертывания глобальных сетей IP-телефонии, приходящих на смену традиционным телефонным сетям.

Рассмотрим алгоритмы установления и разрушения соединения с использованием протокола MGCP. Первый пример охватывает взаимодействие протокола MGCP с протоколом ОКС7 (рисунок 1.12).

1) От телефонной станции АТС-А к шлюзу сигнализации SG1 по общему каналу сигнализации поступает запрос соединения в виде сообщения

IAM протокола ISUP. На рисунке 1.12 шлюз сигнализации SG1 и SG2 совмещены с транспортными шлюзами TGW1 и TGW2 соответственно. Шлюз SG1 передает сообщение IAM к контроллеру шлюзов, который обрабатывает запрос и определяет, что вызов должен быть направлен к АТС-Б посредством шлюза TGW2.

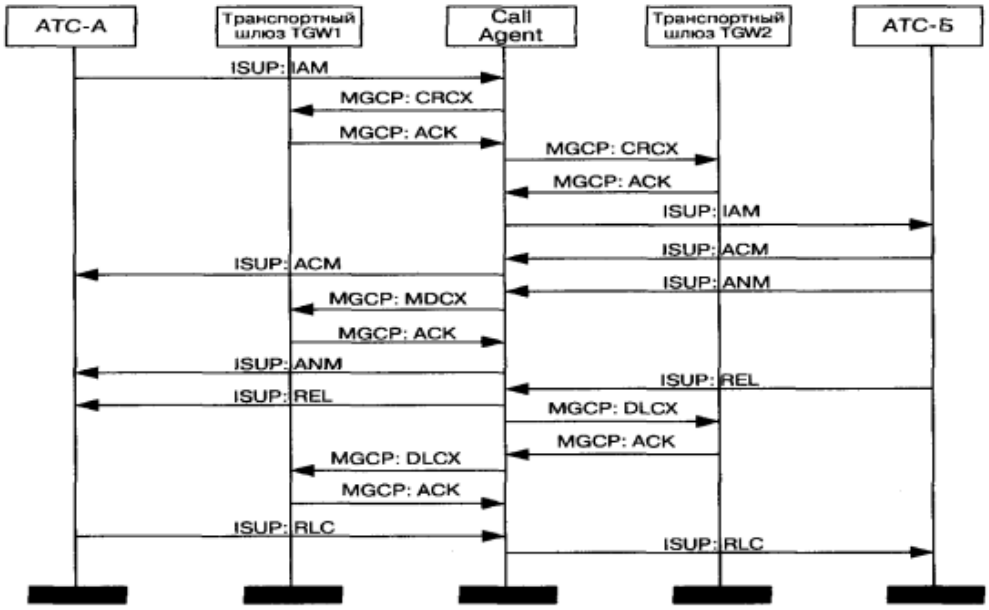

Рис.1.9.Установление и разрушение соединения с использованием протокола MGCP (Пример 1)

2) Контроллер резервирует порт шлюза TGW1 (разговорный канал). С этой целью он передает к шлюзу команду CreateConnection. Отметим, что порт шлюза TGW1 может только принимать информацию (режим «recvonly»), так как он еще не осведомлен о том, по какому адресу и каким образом ему следует передавать информацию.

3) В ответе на эту команду шлюз TGW1 возвращает описание параметров сеанса связи.

4) Приняв ответ шлюза TGW1, контроллер передает команду CRCX второму шлюзу TGW2 с целью зарезервировать порт в этом шлюзе.

5) Шлюз TGW2 выбирает порт, который будет участвовать в соединении, и подтверждает прием команды CRCX. При помощи двух

команд CRCX создается однонаправленный разговорный канал для передачи вызывающему абоненту акустических сигналов или речевых подсказок и извещений. В то же время, порт шлюза TGW2 уже может не только принимать, но и передавать информацию, так как он получил описание параметров связи от встречного шлюза.

6) Далее контроллер шлюзов передает сообщение IAM к АТС-Б.

7) На сообщение IAM станция АТС-Б отвечает подтверждением ACM, которое немедленно пересылается к станции АТС-А.

8) После того как вызываемый абонент примет вызов, АТС-Б передает к контроллеру шлюзов сообщение ANM.

9) Далее контроллер заменяет в шлюзе TGW1 режим «recvonly» на полнодуплексный режим при помощи команды MDCX.

10) Шлюз TGW1 выполняет и подтверждает изменение режима.

11) Контроллер передает сообщение ANM к АТС-А, после чего начинается разговорная фаза соединения.

12) Завершение разговорной фазы происходит следующим образом. В нашем случае вызвавший абонент Б дает отбой первым. АТС-Б передает через шлюз сигнализации сообщение REL к контроллеру шлюзов.

13) Приняв сообщение REL, контроллер шлюзов завершает соединение с вызванным абонентом.

14) Шлюз подтверждает завершение соединения и передает к контроллеру собранные за время соединения статистические данные.

15) Контроллер шлюзов передает сообщение RLC к АТС-Б с целью подтвердить разъединение.

16) Параллельно контроллер завершает соединение с вызвавшей стороной

17) ШлюзTGW1 подтверждает завершение соединения и передает к контроллеру собранные за время соединения статистические данные.

18) АТС-А подтверждает завершение соединения передачей сообщения RLC, после чего соединение считается разрушенным [2].

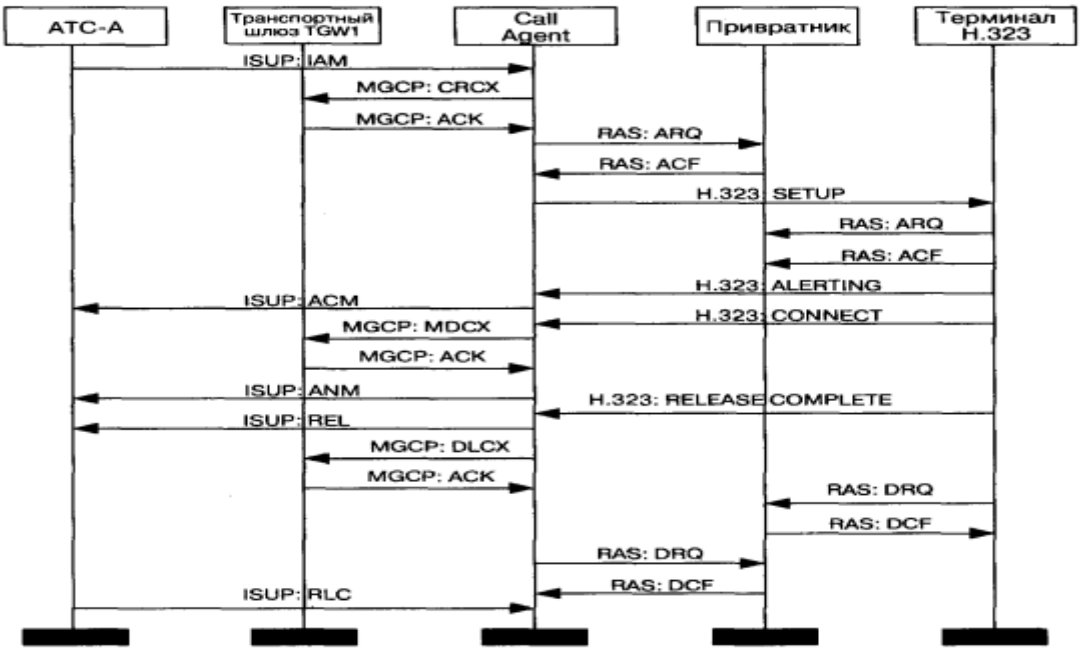

Рис.1.10. Установление и разрушение соединения с использованиемпротокола MGCP (Пример 2)

Второй пример иллюстрирует взаимодействие протокола MGCP с протоколами ОКС7 и H.323 (рис. 1.10).

1) С телефонной станции АТС-А к шлюзу сигнализации SG1 по общему каналу сигнализации поступает запрос соединения (сообщение IAM). На рисунке 1.13 шлюз сигнализации SG1 также совмещен с транспортным шлюзом TGW1. Шлюз SG1 передает сообщение IAM контроллеру шлюзов, который обрабатывает запрос и определяет, что вызов должен быть направлен к оконечному устройству вызываемого пользователя - терминалу H.323.

2) Контроллер шлюзов резервирует порт шлюза TGW1 (разговорный канал). С этой целью он передает к шлюзу команду CreateConnec-tion. И в этом примере порт шлюза TGW1 может только принимать информацию (режим «recvonly»).

3) В ответе на принятую команду шлюз TGW1 возвращает описание параметров связи.

4) Приняв ответ от шлюза TGW1, контроллер передает к привратнику сети H.323 сообщение ARQ с alias адресом вызываемого абонента.

5) В ответ на сообщение ARQ привратник передает сообщение ACF с указанием транспортного адреса своего сигнального канала.

6) Контроллер передает запрос соединения SETUP на транспортный адрес сигнального канала привратника, при этом используется процедура FastStart. Привратник пересылает сообщение SETUP к вызываемому терминалу.

7) Вызываемый терминал передает запрос допуска к ресурсам сети ARQ.

8) В ответ на запрос ARQ привратник передает подтверждение запроса ACF.

9) Вызываемый терминал передает сообщение ALERTING, которое привратник маршрутизирует к контроллеру шлюзов. При этом вызываемому пользователю подается визуальный или акустический сигнал о входящем вызове, а вызывающему пользователю подается индикация того, что вызываемый пользователь не занят и получает сигнал о вызове.

10) Контроллер преобразует сообщение ALERTING в сообщение ACM, которое немедленно пересылается к АТС-А.

11) После того как вызываемый пользователь примет входящий вызов, контроллер получит сообщение CONNECT.

12) Контроллер шлюзов меняет в шлюзе TGW1 режим «recvonly» на полнодуплексный режим.

13) Шлюз TGW1 выполняет и подтверждает изменение режима соединения.

14) Контроллер передает сообщение ANM к АТС-А, после чего начинается разговорная фаза соединения, в ходе которой оборудование вызвавшего пользователя передает речевую информацию, упакованную в пакеты RTP/UDP/IP, на транспортный адрес RTP-канала терминала вызванного абонента, а тот передает пакетированную речевую информацию

на транспортный адрес RTP-канала терминала вызвавшего абонента. При помощи канала RTCP ведется контроль передачи информации по RTP каналу.

15) После окончания разговорной фазы начинается фаза разрушения соединения. Оборудование пользователя, инициирующего разрушение соединения, должно прекратить передачу речевой информации, закрыть логические каналы и передать сообщение RELEASECOMPLETE, после чего сигнальный канал закрывается.

16) Контроллер шлюзов передает сообщение RELEASE к АТС-А с целью завершения соединения.

17) Кроме того, контроллер передает к шлюзу команду DLCX.

18) Шлюз подтверждает завершение соединения и передает к контролеру собранные за время соединения статистические данные.

19) После вышеописанных действий контроллер и оконечноеоборудова-ние извещают привратник об освобождении занимавшейся полосы пропускания. С этой целью каждый из участников соединения посылает привратнику по каналу RAS запрос выхода из соединения DRQ, на который привратник должен передать подтверждение DCF.

20) От АТС-А приходит подтверждение разъединения RLC, после чего соединение считается разрушенным [2].

Следует заметить, что алгоритм взаимодействия протоколов SIP и MGCP не сильно отличается от вышеописанного алгоритма.

Рабочая группа MEGACO комитета IETF продолжает работу по усовершенствованию протокола управления шлюзами, в рамках которой разработан более функциональный, чем MGCP, протокол MEGACO.

Международный союз электросвязи в проекте версии 4 рекомендации H.323 ввел принцип декомпозиции шлюзов. Управление функциональными блоками распределенного шлюза будет осуществляться контроллером шлюза

- MediaGatewayController - при помощи адаптированного к H.323 протокола MEGACO, который в рекомендации H.248 назван GatewayControlProtocol.

Сообщения протокола MEGACO отличаются от сообщений протокола MGCP, но процедуры установления и разрушения соединений с использованием обоих протоколов идентичны, поэтому описание процедуры установления соединения на базе протокола MEGACO здесь не приводится.

Выводы по главе-I

На основе научного анализа изучил проблемы IP-телефонии и рассмотрел ее использование в защищенном режиме.

Рассмотрел уровни архитектуры IP-телефонии, построение сетей на основе протоколов H.323, SIP и MGCP; сценарии систем «компьютер-компьютер», «компьютер-телефон», «телефон-телефон».

Глава II.ТИПЫ УГРОЗ В IP-ТЕЛЕФОНИИ И МЕТОДЫ БОРЬБЫ С НИМИ

2.1. Типы угроз в сетях IP-телефонии

Конфиденциальность и безопасность являются обязательными требованиями для любой телефонной сети. Со временем удалось обеспечить определенный, хотя и далекий от совершенства, уровень безопасности в традиционных сетях. Распространение IP-телефонии и ее претензии на то, чтобы стать основной технологией передачи голоса в недалеком будущем, порождают ряд проблем, с которыми традиционная телефония либо никогда не сталкивалась, либо давно о них забыла, либо уже научилась справляться.

В корпоративных кругах сегодня существуют как противники, так и сторонники внедрения IP-телефонии (IPT) в качестве альтернативной технологии передачи голоса. И если первые, как говорится, могут не беспокоиться, то вторые должны осознавать, что новые конвергентные сети и голосовые сервисы привносят также новые уязвимости для сетей.

Вопрос безопасности связи всегда был одним из важных в сетях телекоммуникаций. В настоящее время в связи с бурным развитием глобальных компьютерных сетей, и в том числе сетей Интернет-телефонии, обеспечение безопасности передачи информации становится еще более актуальным. Разработка мероприятий в области безопасности должна проводиться на основе анализа рисков, определения критически важных ресурсов системы и возможных угроз. Существует несколько основных типов угроз, представляющих наибольшую опасность в сетях IP-телефонии:

– Подмена данных о пользователе означает, что один пользователь сети выдает себя за другого. При этом возникает вероятность несанкционированного доступа к важным функциям системы. Использование механизмов аутентификации и авторизации в сети повышает уверенность в том, что пользователь, с которым устанавливается связь, не является

подставным лицом и что ему можно предоставить санкционированный доступ [15].

– Подслушивание. Во время передачи данных о пользователях (пользовательских идентификаторов и паролей) или частных конфиденциальных данных по незащищенным каналам эти данные можно подслушать и впоследствии злоупотреблять ими. Методы шифровки данных снижают вероятность этой угрозы.

– Манипулирование данными. Данные, которые передаются по каналам связи, в принципе можно изменить. Во многих методах шифрования используется технология защиты целостности данных, предотвращающая их несанкционированное изменение [14].

– Отказ от обслуживания (DenialofService — DoS) является разновидностью хакерской атаки, в результате которой важные системы становятся недоступными. Это достигается путем переполнения системы ненужным трафиком, на обработку которого уходят все ресурсы системной памяти и процессора. Система связи должна иметь средства для распознавания подобных атак и ограничения их воздействия на сеть.

– Наиболее развитой формой мошенничества в Интернет, без сомнения, является фишинг. Типичными инструментами фишинга являются mail (почтовые сообщения, использующие методы социальной инженерии), специально разработанные web-сайты.

Число фишинг-атак выросло вдвое за первые шесть месяцев 2008 года, сообщает Reuters со ссылкой на "Отчет по угрозам интернет-безопасности", подготовленный Symantec.

В первом полугодии 2009 года фишеры отправили 157 тысяч уникальных писем, что на 81 процент больше по сравнению со вторым полугодием 2008 года. По словам авторов исследования, каждое такое письмо может быть отправлено сотням тысяч интернет-пользователей [19].

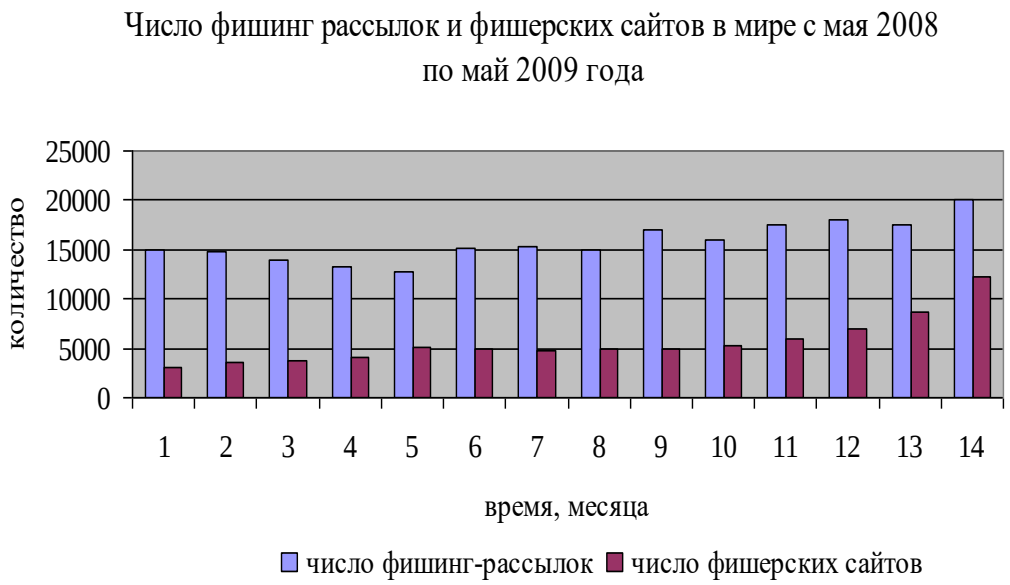

Рис.2.1. Число фишинг рассылок и фишерских сайтов в мире с мая 2008 по май 2009 год

Базовыми элементами в области безопасности являются аутентификация, целостность и активная проверка. Аутентификация призвана предотвратить угрозу обезличивания и несанкционированного доступа к ресурсам и данным. Хотя авторизация не всегда включает в свой состав аутентификацию, но чаще всего одно обязательно подразумевает другое. Целостность обеспечивает защиту от подслушивания и манипулирования данными, поддерживая конфиденциальность и неизменность передаваемой информации. И, наконец, активная проверка означает проверку правильности реализации элементов технологии безопасности и помогает обнаруживать несанкционированное проникновение в сеть и атаки типа DoS [16].

2.2. Методы криптографической защиты информации

Основой любой защищенной связи является криптография. Криптографией называется технология составления и расшифровки закодированных сообщений. Кроме того, криптография является важной

составляющей для механизмов аутентификации, целостности и конфиденциальности. Аутентификация является средством подтверждения личности отправителя или получателя информации. Целостность означает, что данные не были изменены, а конфиденциальность создает ситуацию, при которой данные не может понять никто, кроме их отправителя и получателя. Обычно криптографические механизмы существуют в виде алгоритма (математической функции) и секретной величины (ключа). Алгоритмы широко известны, в секрете необходимо держать только криптографическиеключи. Причем чем больше битов в таком ключе, тем менее он уязвим [15].

В системах обеспечения безопасности используются три основных криптографических метода:

- симметричное шифрование;
- асимметричное шифрование;
- односторонние хэш-функции.

Все существующие технологии аутентификации, целостности и конфиденциальности созданы на основе именно этих трех методов. Например, цифровые подписи можно представить в виде сочетания асимметричного шифрования с алгоритмом односторонней хэш-функции для поддержки аутентификации и целостности данных.

Симметричное шифрование, которое часто называют шифрованием с помощью секретных ключей, в основном используется для обеспечения конфиденциальности данных. При этом два пользователя должны совместно выбрать единый математический алгоритм, который будет использоваться для шифрования и расшифровки данных. Кроме того, им нужно выбрать общий ключ (секретный ключ), который будет использоваться с принятым ими алгоритмом шифрования/расшифровки [14].

В настоящее время широко используются алгоритмы секретных ключей типа DataEncryptionStandard (DES), 3DES (или «тройной DES») и InternationalDataEncryptionAlgorithm (IDEA). Эти алгоритмы шифруют

сообщения блоками по 64 бита. Если объем сообщения превышает 64 бита (как это обычно и бывает), необходимо разбить его на блоки по 64 бита в каждом, а затем каким-то образом свести их воедино. Такое объединение, как правило, происходит одним из следующих четырех методов: электронной кодовой книги (ECB), цепочки зашифрованных блоков (CBC), x-битовой зашифрованной обратной связи (CFB-x) или выходной обратной связи (OFB).

Шифрование с помощью секретного ключа чаще всего используется для поддержки конфиденциальности данных и очень эффективно реализуется с помощью неизменяемых «вшитых» программ (firmware). Этот метод можно использовать для аутентификации и поддержания целостности данных, но метод цифровой подписи является более эффективным.

Метод секретных ключей имеет следующие недостатки:

– необходимо часто менять секретные ключи, поскольку всегда существует риск их случайного раскрытия;

– трудно обеспечить безопасное генерирование и распространение секретных ключей.

Асимметричное шифрование часто называют шифрованием с помощью общего ключа, при котором используются разные, но взаимно дополняющие друг друга ключи и алгоритмы шифрования и расшифровки. Этот механизм полагается на два взаимосвязанных ключа: общего ключа и частного ключа. Наиболее типичные примеры использования алгоритмов общих ключей:

– обеспечение конфиденциальности данных;

– аутентификация отправителя;

– безопасное получение общих ключей для совместного использования.

Важным аспектом асимметричного шифрования является то, что частный ключ должен храниться в тайне. Если частный ключ будет раскрыт, то человек, знающий этот ключ, сможет выступать от имени клиента, получать сообщения данного клиента и отправлять сообщения так, будто это сделал этот клиент [15].

Механизмы генерирования пар общих/частных ключей являются достаточно сложными, но в результате получаются пары очень больших случайных чисел, одно из которых становится общим ключом, а другое — частным. Генерирование таких чисел требует больших процессорных мощностей, поскольку эти числа, а также их произведения должны отвечать строгим математическим критериям. Однако этот процесс генерирования абсолютно необходим для обеспечения уникальности каждой пары общих/частных ключей. Алгоритмы шифрования с помощью общих ключей редко используются для поддержки конфиденциальности данных из-за ограничений производительности. Вместо этого их часто используют в приложениях, где аутентификация проводится с помощью цифровой подписи и управления ключами.

Среди наиболее известных алгоритмов общих ключей можно назвать RSA и ElGamal.

Безопасной хэш-функцией называется функция, которую легко рассчитать, но обратное восстановление которой требует непропорционально больших усилий. Входящее сообщение пропускается через математическую функцию (хэш-функцию), и в результате на выходе получают некую последовательность битов. Эта последовательность называется «хэш» (или «результат обработки сообщения»). Этот процесс невозможно восстановить [13].

Хэш-функция принимает сообщение любой длины и выдает на выходе хэш фиксированной длины.

Обычные хэш-функции включают:

– алгоритм MessageDigest 4 (MD4);
– алгоритм MessageDigest 5 (MD5);
– алгоритм безопасногохэша (SecureHashAlgorithm — SHA).

Технология шифрования часто используется в приложениях, связанных с управлением ключами и аутентификацией. Например, алгоритм Диффи-Хеллмана позволяет двум сторонам создать общий для них секретный ключ,

известный только им двоим, несмотря на то, что связь между ними осуществляется по незащищенному каналу. Затем этот секретный ключ используется для шифрования данных с помощью алгоритма секретного ключа. Важно отметить, что на сегодня пока не создано средств для определения автора такого ключа, поэтому обмен сообщениями, зашифрованными этим способом, может подвергаться хакерским атакам. Алгоритм Диффи-Хеллмана используется для поддержки конфиденциальности данных, но не используется для аутентификации. Аутентификация в данном случае достигается с помощью цифровой подписи [18].

Цифровая подпись представляет собой зашифрованныйхэш, который добавляется к документу. Она может использоваться для аутентификации отправителя и целостности документа. Цифровые подписи можно создавать с помощью сочетания хэш-функций и криптографии общих ключей.

Сообщение, которое отправляется по каналу связи, состоит из документа и цифровой подписи. На другом конце канала связи сообщение делится на оригинальный документ и цифровую подпись. Так как цифровая подпись была зашифрована частным ключом, то на приемном конце можно провести ее расшифровку с помощью общего ключа. Таким образом, на приемном конце получается расшифрованныйхэш. Далее подается текст документа на вход той же функции, которую использовала передающая сторона. Если на выходе получится тот же хэш, который был получен в сообщении, целостность документа и личность отправителя можно считать доказанными.

Цифровым сертификатом называется сообщение с цифровой подписью, которое в настоящее время обычно используется для подтверждения действительности общего ключа. Цифровой сертификат в стандартном формате X.509 включает следующие элементы:

- номер версии;
- серийный номер сертификата;

– эмитент информации об алгоритме;
– эмитент сертификата;
– даты начала и окончания действия сертификата;
– информация об алгоритме общего ключа субъекта сертификата;
– подпись эмитирующей организации [19].

На практике часто используют совместно шифрование и цифровые сертификаты. Например, маршрутизатор и межсетевой экран имеют по одной паре общих/частных ключей (рис.2.2). Предположим, что эмитирующей организации (CA) удалось получить сертификаты X.509 для маршрутизатора и межсетевого экрана по защищенным каналам. Далее предположим, что маршрутизатор и межсетевой экран тоже получили копии общего ключа CA по защищенным каналам. Теперь, если на маршрутизаторе имеется трафик, предназначенный для межсетевого экрана, и если маршрутизатор хочет обеспечить аутентификацию и конфиденциальность данных, необходимо предпринять следующие шаги [14].

Маршрутизатор отправляет в эмитирующую организацию CA запрос на получение общего ключа межсетевого экрана.

CA отправляет ему сертификат межсетевого экрана, зашифрованный частным ключом CA.

Маршрутизатор расшифровывает сертификат общим ключом CA и получает общий ключ межсетевого экрана.

Межсетевой экран направляет CA запрос на получение общего ключа маршрутизатора.

CA отправляет ему сертификат маршрутизатора, зашифрованный частным ключом CA.

Межсетевой экран расшифровывает сертификат общим ключом CA и получает общий ключ маршрутизатора.

Маршрутизатор и межсетевой экран используют алгоритм Диффи-Хеллмана и шифрование с помощью общих ключей для аутентификации.

С помощью секретного ключа, полученного в результате использования алгоритма Диффи-Хеллмана, маршрутизатор и межсетевой экран проводят обмен конфиденциальными данными.

Общий вид криптографической системы можно представить следующимобразом (рис.2.2.).

Рис.2.2. Общий вид криптографической системы

ДляиспользованиятакойсистемыдляопределенногосообщенияMi выбирается некоторый ключ Ki из множества возможных ключей K. После чего припомощиключаKiформируетсякриптограммаEi.Этакриптограмма, полученная при помощи преобразования TKi, по каналу передачи передается в точкуприема.НаприемномконцеспомощьюотображенияTK^{-1}i1,обратного выбранному, из криптограммы Ei восстанавливается исходное сообщение Mi.

Еслипротивникперехватиткриптограмму,тооннесможетее расшифровать,еслинезнаетключаKi.Поэтому,чембольшемощность множестваK,темменьшевероятностьтого,чтокриптограммабудет расшифрована. Эта вероятность называется апостериорной вероятностью. Вычислениеапостериорныхвероятностей – естьобщаязадача дешифрования [16].

Рис.2.3. Произведение двух секретных систем

Образованиепроизведениядвухсекретныхсистем (рис.2.4) осуществляется следующим образом: S = RT,причем RS = SR, а RS ≠ RS.

То есть сначала применяется система T, а затем система R к результатам первой операции.

КлючсистемыSсостоиткакизключасистемыT,такиизключа системы R.

Рис.2.4. Классификация современных криптосистем

По характеру использования ключа все криптосистемы можно разделить насимметричные (одноключевыессекретнымключом)иасимметричные (несимметричные, с открытым ключом). В первом случае как для шифрования, такидлядешифрованияприменяетсяодинитотжеключ.Онявляется

секретнымипередаетсяотправителемполучателюпоканалусвязи, исключающемперехват.Васимметричныхсистемахдляшифрованияи дешифрования используются разные ключи, связанные между собой некоторой математическойзависимостью.Причемзависимостьявляетсятакой,чтоиз одногоключавычислитьдругойключоченьтруднозаприемлемый промежуток времени [15].

Функции шифрования и дешифрования в зависимости от алгоритма могут бытьодинаковымиили,чточащевсего,разными,причемпроцесс дешифрования является инверсией процесса шифрования.

Всемногообразиесимметричныхкриптографическихсистем (рис.2.5.) основывается на следующих базовых классах:

– Блочные шифры. Представляютсобойсемействообратимыхпреобразованийблоков (частей фиксированной длины) исходного текста. Фактически блочный шифр – это система подстановки блоков. После разбиения текста на блоки каждый блок шифруетсяотдельнонезависимоотегоположенияивходной последовательности.

Одним из наиболее распространенных способов задания блочных шифров является использование так называемых сетей Фейстела [13]. Сеть Фейстела представляетсобойобщийметодпреобразованияпроизвольнойфункциив перестановку на множестве блоков.

Калгоритмам блочного шифрования относятся:американскийстандарт шифрования DES и его модификации, российский стандарт шифрования ГОСТ 28147–89, Rijndael, RC6, SAFFER+ и многие другие.

– Шифры замены (подстановки). Шифрызамены (подстановки) – этонаиболеепростойвид преобразований,заключающийсявзаменесимволовисходноготекстана другие

(того же алфавита) по более или менее сложному правилу. Подстановки различаютмоноалфавитныеимногоалфавитные.Впервомслучаекаждый символисходноготекстапреобразуетсявсимволшифрованноготекстапо одному и тому же закону. При многоалфавитной одстановке закон меняется от символаксимволу.Кэтомуклассуотноситсятакназываемаясистемас одноразовым ключом.

– Шифры перестановки. Перестановки – методкриптографическогопреобразования, заключающийсявперестановкеместамисимволовисходноготекстапонекоторо му правилу. Шифры перестановки в настоящее время не используются в чистом виде, так как их криптостойкостьнедостаточна.

– Гаммирование. Гаммирование – представляетсобойпреобразование,прикотором символыисходноготекстаскладываютсяпомодулю,равномумощности алфавита, с символами псевдослучайной последовательности, вырабатываемой понекоторомуправилу.Впринципе,гаммированиенельзявыделитьв отдельныйклассшифровпреобразований,таккакэтапсевдослучайная последовательность можетвырабатываться,например,припомощиблочного шифра [12].

– Потоковые шифры. Потоковые шифры представляют собой разновидность гаммированияи преобразуютоткрытыйтекствшифрованныйпоследовательно,поодному биту.Генераторключевойпоследовательности,иногданазываемый генератором бегущего ключа, выдает последовательность бит k1,k2,...,ki ,.... Эта ключеваяпоследовательностьскладываетсяпомодулю2с последовательностьюбитисходноготекстар1, р2,..., pi ,...дляполучения шифрованного текстаci = pi*ki . На приемной стороне текст складывается по модулю2сидентичнойключевойпоследовательностьюдляполучения исходноготекста.Такоепреобразованиеназываетсягаммированиемс помощью

операции XOR.Однако при потоковом шифровании для повышения криптостойкостигенераторключевойпоследовательности «завязывается»на текущеесостояниекодируемогосимвола.Тоестьзначения,выдаваемые генератором, зависят не только от ключа, но и от номера шифруемого бита и входной последовательности.

2.3. Защита от прослушивания

Виртуальные ЛВС снижают в известной степени риск прослушивания телефонных разговоров, однако в случае перехвата речевых пакетов анализатором восстановление записи разговора для специалиста дело нехитрое. Главным образом, виртуальные ЛВС способны обеспечить защиту от внешних вторжений, но защитить от атаки, инициированной изнутри сети, могут быть не способны. Человек, находящийся внутри периметра сети, может подключить компьютер прямо к разъему настенной розетки, сконфигурировать его как элемент виртуальной ЛВС системы IP-телефонии и начать атаку [10].

Наиболее совершенный способ противодействия подобным манипуляциям — использование IP-телефонов со встроенными средствами шифрования. Кроме того, дополнительную защиту обеспечивает шифрование трафика между телефонами и шлюзами. На сегодняшний день практически все производители, такие как Avaya, Nortel и Cisco, предлагают встроенные средства шифрования для информационных потоков и сигнализации. Шифрование трафика является наиболее логичным решением для защиты от прослушивания разговоров, но такая функциональность несет и ряд трудностей, которые необходимо учитывать при построении защищенной связи. Основной проблемой может быть задержка, добавляемая процессом зашифровывания и расшифровывания трафика. При работе в локальной сети подобная проблема, как правило, не дает о себе знать, но при связи через территориально-распределенную сеть способна доставлять неудобства. К тому же шифрование сигнализации, происходящее на прикладном уровне,

может затруднить работу межсетевых экранов. В случае применения потокового шифрования задержки гораздо ниже, чем при использовании блочных шифров, хотя полностью от них избавиться не удастся. Вариантом решения проблемы могут служить более быстрые алгоритмы или включение механизмов QoS в модуль шифрования.

2.4 Защищенность сети доступа

Среди всего многообразия способов несанкционированного перехвата информации особое место занимает анализ трафика в сети доступа, поскольку сеть доступа - самый первый и самый удобный источник связи между абонентами в реальном масштабе времени, и при этом самый незащищенный.

Сеть доступа имеет еще один недостаток с точки зрения безопасности - возможность перехвата речевой информации из помещений, по которым проходит телефонная линия, и где подключен телефонный аппарат (далее оконечное оборудование (ОО)), даже тогда, когда не ведутся телефонные переговоры. Для такого перехвата существует специальное оборудование, которое подключается к телефонной линии внутри контролируемого помещения или даже за его пределами. Требования к оборудованию противодействия данных угрозам описывают НД ТЗІ 2.3-002-2001, НД ТЗІ 2.3-003-2001, НД ТЗІ 4.7-001-2001 и некоторые другие нормативные документы [11].

Я провела краткий анализ вариантов угроз информации в канале связи. Для удобства анализа провела классификацию канала связи по степени защищенности (защиты) передаваемой информации.

Структурная схема передачи данных в открытом канале показана на рис.2.6.

Рис.2.6. Передача данных в открытом канале данных

Рис.2.7. Передача данных в полузакрытом канале данных

Основная проблема, с которой сталкиваются пользователи сетей, где применяется сквозное шифрование, связана с тем, что служебная информация.используемая для установления соединения, передается по сети в незашифрованном виде. Опытный криптоаналитик может извлечь для себя массу полезной информации, зная кто с кем, как долго и в какие часы общается через сеть доступа. Для этого ему даже не потребуется быть в курсе предмета общения.

По сравнению с канальным, сквозное шифрование характеризуется более сложной работой с ключами, поскольку каждая пара пользователей должна быть снабжена одинаковыми ключами, прежде чем они смогут связаться друг с другом. А поскольку криптографический алгоритм реализуется на верхних уровнях модели OSI, приходится также сталкиваться со многими существенными различиями в коммуникационных протоколах и интерфейсах сети доступа (для примера: отправитель - канал ТЧ, получатель

- 2B+D). Все это затрудняет практическое применение сквозного шифрования.

Приведенные выше методы защиты информации уже не удовлетворяют современных требованиям. При использовании этих методов злоумышленник может перехватывать адресную информацию, вести мониторинг передаваемых данных, несанкционированно подключаться к линии, искажать передаваемую информацию.

Единственным возможным методом, удовлетворяющим всем современны требованиям, является использования комбинации канального и сквозного шифрования. При этом может закрывается вся передаваемая по каналу связи информация.

Комбинация канального и сквозного шифрования данных в сети доступа обходится значительно дороже, чем каждое из них по отдельности. Однако именно такой подход позволяет наилучшим образом защитить данные, передаваемые по сети. Шифрование в каждом канале связи не позволяет злоумышленнику анализировать служебную информацию, используемую для маршрутизации. А сквозное шифрование уменьшает вероятность доступа к незашифрованным данным в узлах сети.

При этом злоумышленник может проводить анализ только открыто передаваемых данных, но не может нелегально использовать линию связи.

Структурная схема передачи данных в закрытом канале показана на рисунке.

При занятии линии (получении сигнала вызова от АТС) происходит автоматический переход в закрытый режим связи (А1, К1). После перехода в закрытый режим, абонентский комплект (АК) или криптографический модуль перед АК АТС аутентифицирует КСЗИ. Данный шаг необходим для устранения возможности несанкционированного использования линии. После проведения аутентификации возможен выход из закрытого режима.

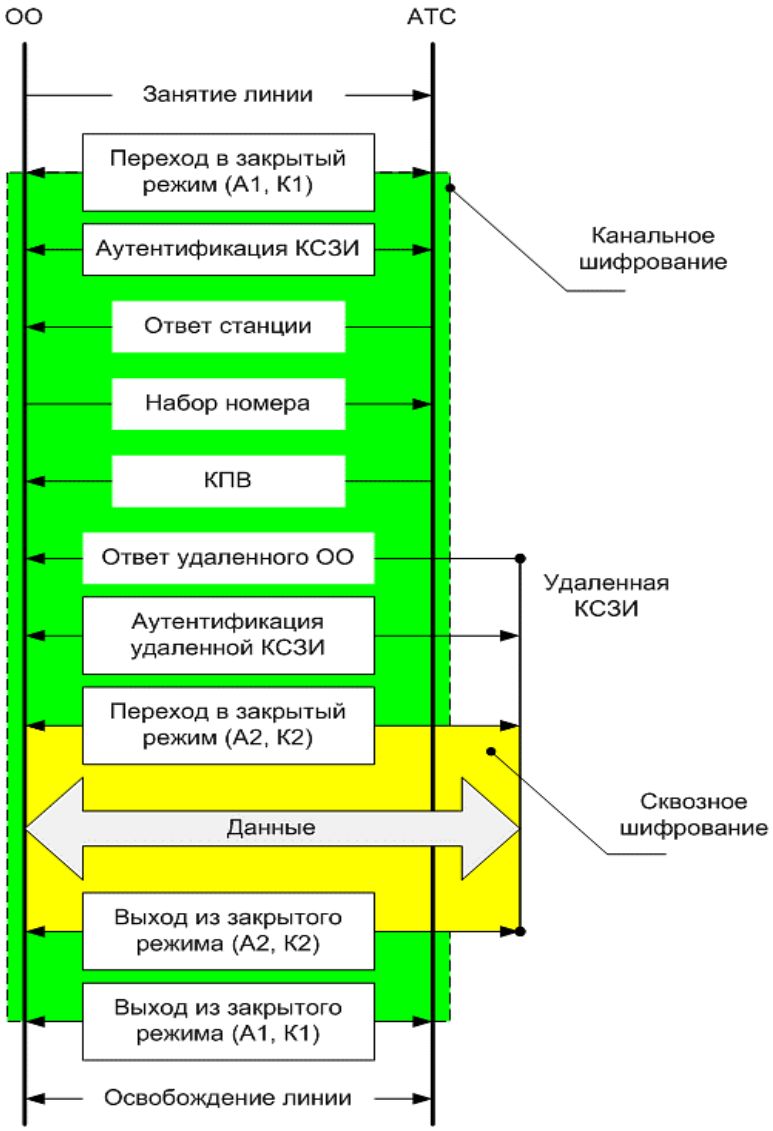

Рис.2.8. Передача данных в закрытом канале данных

При вызове со стороны вызывающего абонента, АТС принимает адресную информацию, устанавливает соединение. При ответе удаленной КСЗИ возможны два варианта: аутентификации удаленной КСЗИ и переход в закрытый режим (А2, К2) либо переход в закрытый режим (А2, К2) и аутентификация удаленной КСЗИ [10].

Аутентификация удаленной КСЗИ необходима для противодействия атаке, при которой удаленная КСЗИ злоумышленника при помощи перекоммутации выдает себя за КСЗИ легального пользователя.

После удачной аутентификации удаленной КСЗИ также возможен выход из защищенного режима (отказ от вхождение в защищенный режим).

Также при передаче данных необходимо проводить т.н. проверку обратного кода. Проверка обратного кода - представляет собой процедуру защиты, осуществляемую в процессе передачи данных. Заключается в том, что у удаленной КСЗИ периодически запрашивается идентифицирующая информация, которая и называется обратным кодом. Эта информация сравнивается с эталонной, сохраненной при аутентификации в начале сеанса связи. При несовпадении кодов передача блокируется. Проверкой обратного кода можно обнаружить факт изменения (перекоммутации) направлений выдачи данных или злоумышленного использования приемного устройства зарегистрированного (законного) корреспондента [13].

Выводы по главе-II

Рассмотрел виды угроз IP-телефонии, такие как регистрацию чужого терминала, позволяющую делать звонки за чужой счет, подмену абонента, внесение изменений в голосовой или сигнальный трафик, снижение качества голосового трафика, перенаправление голосового или сигнального трафика, перехват голосового или сигнального трафика, подделка голосовых сообщений, завершение сеанса связи, отказ в обслуживании иудаленный несанкционированный доступ к компонентам инфраструктуры IP-телефонии.Эти проблемы предлагаю решать разными способами: криптографии, защищенности канала, технологии AAA.

Глава III. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ С ТОЧКИ ЗРЕНИЯ ПРОВЕРКИ ПРАВ ДОСТУПА К РЕСУРСАМ (AAA)

3.1. Непрямая аутентификация

Сеть IP-телефонии любого провайдера, как правило, имеет несколько точек доступакуслуге;притакойсхемеорганизацииреализовыватьпроцесс аутентификации пользователей для каждой точки доступа в отдельности (на месте)нецелесообразно.Гораздоразумнеецентрализоватьпроцесс аутентификации, используя для этого отдельный сервер и общую базу данных, ккоторымбудутобращатьсясерверыдоступа (такоерешениеполучило названиенепрямойаутентификации).Объясняетсяэтоглавнымобразомс точкизренияпроблемадминистрирования,возникающихвслучае организации аутентификации на месте [18].

Непрямая аутентификация – модель, в которой механизм аутентификации

размещается в стороне от других серверов сети, при этом они связываются с ним каждый раз, когда пользователь запрашивает доступ.

Решениянаосновенепрямойаутентификациипозволяютсправлятьсяс проблемой масштабируемостинавычислительныхцентрах,укоторыходна группапользователей,нонесколькоточекобслуживания.Даженатой

площадке,гдевсегодвасервера,будетзатруднительноподдерживать совместимостьдвухотдельныхбазданныхаутентификации.Еслидругие проектныешаблонырedусматриваютобъединениемеханизмов аутентификации и управления доступом, то шаблон непрямой аутентификации перемещает механизмаутентификацииизточкиобслуживаниявотдельный аутентификационныйсервер.Вседругиекомпонентысетипредоставляют услугиилиуправляютдоступомкресурсам,нонепринимаютрешенийоб аутентификации.Вместоэтогоониаутентифицируютпользователей непрямым

способом, связываясь с аутентификационным сервером всякий раз, когда кто-то пытается зарегистрироваться в системе [20].

Сточкизренияобеспечения безопасностисоединения каквсетях IP-телефониив частности,так ив IP-сетяхвообще,проблемуможноусловноразделитьнадвесоставляющих.

Первое – это проблемаобеспечения правомерного ибезопасногодоступак сетевымресурсамиуслугам,авторое – этообеспечениебезопасности информации уже непосредственно в каналах. Именно первой части проблемы обеспечения безопасности в сетях IP-телефонии и посвящена эта дипломная работа.

Совершенноочевидно,чтоосновнаярольприрешенииподобныхзадач будетпринадлежатьпроцессуаутентификациипользователей.Всилу структуры мультисервисной сети, на базе которой предоставляются услуги IP-телефонии нас будет интересовать непрямая аутентификация, ее протоколы, а также слабые и сильные места.

Многиеширокоизвестныесегоднясистемыобеспечиваютнепрямую аутентификациюспомощьюспециальноразработанныхпротоколов [19].

Открытымстандартомдляреализациинепрямойаутентификацииявляется протокол RADIUS. Вобщемслучаепротоколнепрямойаутентификации начинает свою работу, когда кто-нибудь пытается зарегистрироваться в точке обслуживания с удаленного места, которым может быть, например, рабочая станция. Когдаточкаобслуживанияпринимаетзапроснарегистрацию,она пересылает имя пользователя и пароль аутентификационному серверу. Часто для пересылки данныхтакихсообщений используется внутренний протокол типа RADIUS илипротокол,разработанныйизготовителем.Еслисервер подтверждаетаутентификацию,тоонпосылаетвточкуобслуживания подтверждение,сформатированноевсоответствиисэтимвнутренним протоколом.Получивего,точкаобслуживанияпринимаеткисполнению попыткупользователязарегистрироваться.Еслисерверпосылаетотказ,то точкаобслуживанияотвергаетзапрос.Посколькуаутентификационные запросы

перенаправляются аутентификационному серверу, имеется риск, что взломщик будет подделывать сообщение «Доступ разрешен», чтобы обмануть точку доступа; поэтому для аутентификации двусторонних сообщений между точкойобслуживанияиаутентификационнымсерверомдолжно использоваться шифрование.

Некоторыесистемы,использующиенепрямуюаутентификацию,могут иметьвысокийуровеньустойчивостикотказам,поддерживаяфункцию перенаправления. Есликакой-либо изсерверовтеряетработоспособность (в томчислеипри DOS-атаке),тозапросынааутентификациюмогут перенаправлятьсянаальтернативныйсервер,содержащийкопиювсей аутентификационнойбазыданных.Этопозволяетпровайдеру IP-телефонии реплицироватьсвоислужбынанесколькохост-машинереализовать аутентификацию на нескольких аутентификационных серверах, исключаятем самым появление точки критического отказа [18].

3.2. Технологии AAA на основе протокола TACACS+

3.2.1. Протокол TACACS+

TACACS+ – этопростойпротоколуправлениядоступом,основанныйна стандартах UDP и разработанных компанией Bolt, BeranekandNewman, Inc. (BBN). TACACS+ представляет собой приложение сервера защиты, позволяющее наосновесоответствующегопротоколареализоватьцентрализованное управлениедоступомпользователейкуслугам.Информацияосервисах TACACS+ и пользователях хранится в базе данных, обычно размещенной на компьютере под управлением UNIX или Windows NT. TACACS+позволяет с помощью одного сервера управления приложениями реализовать независимую поддержку сервисов AAA.

Протокол TACACS+ работаетпотехнологииклиент-сервер.

Фундаментальным структурным компонентом протокола TACACSявляется разделение аутентификации, авторизации и учета. Это позволяет обмениваться идентификационнымисообщениямилюбойдлиныисодержания,и, следовательно,использоватьдляклиентов TACACS+ любой идентификационный механизм, в том числе PPP PAP, PPP CHAP, аппаратные карты и т.д.

3.2.2. Свойства протокола TACACS+

TACACS+ поддерживает следующие возможности сервера защиты:

– Пакеты TCP длянадежнойпередачиданных.Использование TCP в качествепротоколасвязидлясоединений TACACS+ междусервером доступа и сервером защиты. Для TACACS+ резервируется TCP-порт 49.

– Архитектура AAA. Каждыйсервиспредоставляетсяотдельноиимеет собственную базу данных, но, тем не менее, они работают вместе, как один сервер защиты.

– Канальноешифрование.Часть TCP-пакета,содержащаяданные протокола TACACS+, шифруетсясцельюзащитытрафикамежду сервером доступа и сервером защиты.

– Каждый пакет TACACS+ имеет 12-байтовый заголовок, пересылаемый ввидеоткрытоготекста,ителопеременнойдлины,содержащеепараметры TACACS+. Тело пакета шифруется с помощью алгоритма, использующегопсевдослучайныйзаполнитель,получаемый посредством MD5. Пакеты TACACS+ передаютсяпосетиихранятся сервером TACACS+ в шифрованном виде. Когда это необходимо, пакет

дешифруетсясерверомдоступаиприложением TACACS+ путем обращения алгоритма шифрования.

– Аутентификация PAP и CHAP.Обеспечиваетполныйконтроль аутентификации с помощью средств вызова/ответа PAP и CHAP, а также посредствомиспользованиядиалоговыхоконвводапаролядоступаи поддержки сообщений интерактивной процедуры начала сеанса.

– Защиталокальныхиглобальныхсетей.ПоддержкасредствААА удаленногоилокальногосетевогодоступадлясерверовдоступа, маршрутизаторов и другогосетевого оборудования, поддерживающего TACACS+.Даетвозможностьосуществлятьцентрализованное управление сетевым оборудованием.

– Функцияобратноговызова.Даннаяфункциявозвращаеттелефонные вызовы,заставляясервердоступазвонитьсоответствующему пользователю, что может дать дополнительные гарантии защиты.

– Индивидуальные списки доступа пользователей. База данных TACACS+ может дать указаниесерверусетевого доступаконтролировать доступ данного пользователяксетевымслужбамиресурсамвтечении фазы авторизации на основе списка доступа [19].

Аутентификация не является обязательной. Она рассматривается как опция, котораяконфигурируетсянаместе.Внекоторыхместахонавообщене требуется, в других местах она может применяться лишь для ограниченного набора услуг.

Заголовок пакета TACACS+ содержит полетипа,являющееся признаком того,чтопакетпредставляетсобойчастьпроцессаААА.Аутентификация TACACS+различаеттритипапакетов: START (начало), CONTINUE (продолжение) и REPLY (ответ).

Взапросенаавторизациюможноуказать,чтоаутентификация пользователянепроведена (личностьнедоказана).Вэтомслучаелицо,

отвечающее за авторизацию должно самостоятельно решить, допускать такого пользователякзапрашиваемымуслугамилинет.Протокол TACACS+допускаеттолькоположительнуюилиотрицательнуюавторизацию,о днако этотрезультатдопускаетнастройкунапотребностиконкретногозаказчика.

Авторизацияможетпроводитьсянаразныхэтапах,например,когда пользователь впервые входит в сеть и хочет открыть графический интерфейс иликогда пользовательзапускает PPP и пытается использовать поверх PPP протокол IP сконкретнымадресом IP. Вэтихслучаяхдемонсервера TACACS может разрешить предоставление услуг, но наложить ограничения по времени или потребовать список доступа IP для канала PPP.

Впроцессеавторизации TACACS+ используетсядватипапакетов: REQUEST (запрос)и RESPONSE (ответ).Данныйпроцессавторизации пользователя контролируется посредством обмена парами «атрибут/значение» между сервером защиты TACACS+ и сервером доступа [20].

Аудит (или учет) обычно следует за аутентификацией и авторизацией. Учет представляет собой запись действий пользователя. В системе TACACS+ учет может выполнять две задачи. Во-первых, он может использоваться для учета использованныхуслуг (например,длявыставлениясчетов).Во-вторых,его можно использовать в целях безопасности. Для этого TACACS+ поддерживает три типа учетных записей. Записи «старт» указывают, что услуга должна быть запущена.Записи «стоп»говорятотом,чтоуслугатолькочтоокончилась. Записи «обновление» (update) являются промежуточными и указывают на то, что услуга все еще предоставляется. Учетные записи TACACS+ содержат всю информацию,котораяиспользуетсявходеавторизации,атакжедругие данные:времяначалаиокончания (еслиэтонеобходимо)иданныеоб использовании ресурсов. Транзакции между клиентом TACACS+ и сервером TACACS+ идентифицируются с помощью общего «секрета», который никогда непередаетсяпоканаламсвязи.Обычноэтот «секрет»вручную

устанавливаетсянасервереинаклиенте. TACACS+ можнонастроитьна шифрование всего трафика, который передается между клиентом и демоном сервера TACACS+ [18].

Впроцессеаудита TACACS+ используетдватипапакетов – REQUEST (запрос) иRESPONSE (ответ). Данный процесс во многом подобен процессу авторизации.Впроцессеаудитасоздаютсязаписисинформациейоб активностипользователявотношениизаданныхсервисов.Записи, регистрирующиевыполненныесетевымоборудованиемдействия,могут сохраняться в некоторомстандартном формате, насерверезащитыс целью дальнейшего анализа.

В рамках TACACS+ аудит AAA не является средством надежной защиты и обычно используетсятолько дляучета илиуправления. Однакос помощью аудита AAA можно контролировать действия пользователя, чтобы, например, вовремязаметитьегонеобычноеповедениеприработессетевым оборудованием [20].

3.3. Технологии AAA на базе протокола RADIUS

3.3.1 Протокол RADIUS

Протокол RADIUS былразработанкомпанией LivingstonEnterprises, Inc. (теперьнаходящейсявсоставе LucentTechnologies) вкачествепротокола аутентификациисерверногодоступаиучета.Внастоящеевремяпротокол RADIUS описывается в документе RFC 2865, а аудит RADIUS – в RFC 2866.

RADIUS (RemoteAccessDial-InUserService – сервисидентификации удаленныхабонентов)представляетсобойраспределенныйпротокол, используемый в рамках технологии клиент/сервер и обеспечивающий защиту сетиотнесанкционированногодоступа.Такнапримеркомпания Cisco поддерживает RADIUS какоднуизсоставляющихсистемызащитыAAA.

Рассматриваемыйпротоколскорееобъединяетаутентификациюи авторизацию, чем трактует их отдельно, как это делается в отношении аудита [17].

Протокол RADIUS можетиспользоватьсясдругимипротоколамизащиты AAA, например с TACACS+, Kerberos и локальными базами данных защиты. Протокол RADIUS реализованвомногихсетевыхсредах,требующих высокогоуровнязащитыприусловииподдержкисетевогодоступадля удаленныхпользователей.Онпредставляетсобойполностьюоткрытый протокол,поставляемыйвформатеисходноготекста,которыйможно изменить длятого,чтобы он мог работатьс любой доступной в настоящий моментсистемойзащиты.Широкуюпопулярность RADIUS обеспечивает возможность добавлять новые пары «атрибут/значение» в дополнение к тем, которые описанывдокументе RFC 2865. Протокол RADIUS имеетатрибут поставщика , позволяющий поставщику осуществлять поддержку своихсобственныхрасширенныхнабороватрибутов,включающих нестандартныеатрибуты. Вследствие использования пар «атрибут/значение» конкретныхпоставщиковмогутвозникатьтрудностиприинтеграции серверныхпродуктовзащиты RADIUS вдругиесистемызащиты.Серверы защиты RADIUS исоответствующиеклиентыдолжныигнорировать нестандартныепары «атрибут/значение»,созданныеконкретными поставщиками.

Связьмежду NAS исервером RADIUS основананапротоколе UDP. В целом считается, что протокол RADIUS не имеет отношения к подключению. Все вопросы, связанные с доступностью сервера, повторной передачей данных иотключениямипоистечениивремениожидания,контролируются устройствами,работающимиподуправлениемпротокола RADIUS, ноне самимпротоколомпередачи.Протокол RADIUS основаннатехнологииклиент-сервер. Клиентом RADIUS обычно является NAS, а сервером RADIUS считается «демон», работающий на машине UNIX или NT. Клиент передает пользовательскуюинформациюнаопределенныесерверы RADIUS, азатем

действует в соответствии с полученными от сервера инструкциями. Серверы RADIUSпринимаютзапросыпользователейнаподключение,проводят идентификациюпользователей,азатемотправляютвсюконфигурационную информацию,котораянеобходимаклиентудляобслуживанияпользователя.

Для других серверов RADIUS или идентификационных серверов других типов сервер RADIUS может выступать в роли клинта-посредника (proxy) [19].

3.3.2. Свойства и возможности протокола RADIUS

RADIUS поддерживает следующие возможности сервера защиты:

– Пакеты UDP.Длясвязи RADIUS междусерверомдоступаи серверомзащитыиспользуетсяпротокол UDP и UDP-порт 1812, официально назначенный для этого. Некоторые реализации RADIUS используют UDP-порт 1645. Использование UDP упрощает реализацию клиента и сервера RADIUS.

– Объединениеаутентификацииавторизацииивыделениеаудита. Сервер RADIUS получаетзапросыпользователя,выполняет аутентификациюиобеспечиваетклиентуинформациюо конфигурации. Аудит выполняется сервером аудита RADIUS.

– Шифрованиепаролейпользователей.Пароли,содержащиесяв пакетах RADIUS (а это только пользовательские пароли), шифруются посредством хэширования MD5.

– Аутентификация PAP и CHAP.Обеспечиваетуправление аутентификацией с помощью средств вызова/ответа PAP и CHAP, а также посредством диалога начала сеанса и ввода пароля наподобие входа в систему UNIX.

– Защитаглобальнойсети.ОбеспечиваетподдержкусредствAAA удаленногодоступадлясерверовдоступамногихпоставщиков, поддерживающихклиентов RADIUS. Даетвозможность централизовать управление удаленным доступом.

– Поддержкарядапротоколов,обеспечивающихтерминальный доступ к серверу защиты RADIUS.

– Функция обратного вызова. Данная функция возвращает телефонные вызовы,заставляясервердоступазвонитьсоответствующему пользователю,чтоможетдатьдополнительныегарантиизащиты пользователям, использующим доступ по телефонным линиям.

– Расширяемость.Всетранзакцииипредполагаютиспользованиепар «атрибут/значение» переменной длины. Новые атрибуты могут быть добавлены в существующие реализации протокола.

– Гарантированнаясетеваязащита.Аутентификациятранзакций междуклиентомисерверомзащиты RADIUS предполагает использование общего секретного значения [20].

3.3.3. Процесс аутентификации и авторизации в протоколе RADIUS

Клиент RADIUS и сервер защиты RADIUS обмениваются пакетами Access-Request (доступ-запрос), Access-Accept (доступ-подтверждение), Access-Reject (доступ-отказ)и Access-Challenge (доступ-вызов). Какпоказанонарис.3.1, припопыткеподключитьсяксерверусетевогодоступа,имеющему конфигурацию клиента RADIUS, выполняются следующие шаги:

– Пользовательинициализируетзапросаутентификации PPP ксерверу сетевого доступа.

– У пользователя запрашивается имя пользователя и пароль

– Серверсетевогодоступапосылаетсерверузащиты RADIUS пакет Access-Request, содержащий имя пользователя, шифрованный пароль и другие атрибуты.

Рис.3.1. Процесс аутентификации и авторизации RADIUS

Серверзащиты RADIUS идентифицируетклиента-инициатора, выполняетаутентификациюпользователя,проверяетпараметры авторизации пользователя и возвращает один из следующих ответов:

Access-Accept – пользователь аутентифицирован.

Access-Reject – пользователь не аутентифицирован, и сервер сетевого доступалибопредлагаетввестиимяпользователяипарольснова, либо запрещает доступ.

Access-Challenge – вызовявляетсядополнительнойвозможностью сервера защиты RADIUS.

– Серверсетевогодоступаобращаетсякпараметрамаутентификации, разрешающим использование конкретных служб.

– Ответ Access-Accept или Access-Reject связывается с дополнительными данными (парами «атрибут/значение»),используемымидлясеансов EXECиавторизации. Процессаутентификации RADIUS долженбыть завершен до начала процесса авторизации [17].

– Сервер защиты RADIUS может периодически посылать пакеты Access-Challengeсерверусетевогодоступа,чтобыпотребоватьповторного введения имени пользователя и пароля пользователем, информировать о состоянииисерверасетевогодоступаиливыполнитькакие-тодругие действия,предусмотренныеразработчикамисервера RADIUS. Клиент RADIUS не может посылать пакеты Access-Challenge.

Авторизация — это процесс определения действий, которые позволены данному пользователю. Обычно аутентификация предшествует авторизации, однако это не обязательно. В запросе на авторизацию можно указать, что аутентификация пользователя не проведена (личность пользователя не доказана). В этом случае лицо, отвечающее за авторизацию, должно самостоятельно решить, допускать такого пользователя к запрашиваемым услугам или нет. Протокол TACACS+ допускает только положительную или отрицательную авторизацию, однако этот результат допускает настройку на

потребности конкретного заказчика. Авторизация может проводиться на разных этапах, например, когда пользователь впервые входит в сеть и хочет открыть графический интерфейс иди когда пользователь запускает PPP и пытается использовать поверх PPP протокол IP с конкретным адресом IP. В этих случаях демон сервера TACACS+ может разрешить предоставление услуг, но наложить ограничения по времени или потребовать список доступа IP для канала PPP [16].

Выводы по главе-III

На основе технологии AAA сравнил протоколы аутентификации TACACS+ и RADIUS. После исследования протоколов аутентификации, одной из основных составляющих защищенности, сделал вывод, что в административных сетях для защиты информации лучше использовать протокол TACACS+, учитывая особенности каждой сети. Для сети более крупного масштаба лучше использовать протокол RADIUS.

Заключение

В данной магистерской диссертационной работена основе научного анализа изучил проблемы IP-телефонии и рассмотрел ее использование в защищенном режиме.

Рассмотрел уровни архитектуры IP-телефонии, построение сетей на основе протоколов H.323, SIP и MGCP; сценарии систем «компьютер-компьютер», «компьютер-телефон», «телефон-телефон».

Рассмотрел виды угроз IP-телефонии, такие как регистрацию чужого терминала, позволяющую делать звонки за чужой счет, подмену абонента, внесение изменений в голосовой или сигнальный трафик, снижение качества голосового трафика, перенаправление голосового или сигнального трафика, перехват голосового или сигнального трафика, подделка голосовых сообщений, завершение сеанса связи, отказ в обслуживании иудаленный несанкционированный доступ к компонентам инфраструктуры IP-телефонии.Эти проблемы предлагаю решать разными способами: криптографии, защищенности канала, технологии AAA.

На основе технологии AAA сравнил протоколы аутентификации TACACS+ и RADIUS. После исследования протоколов аутентификации, одной из основных составляющих защищенности, сделал вывод, что в административных сетях для защиты информации лучше использовать протокол TACACS+, учитывая особенности каждой сети. Для сети более крупного масштаба лучше использовать протокол RADIUS.

Литература

1 http://2018.strategy.uz/ru

2 Мирманов А.Б., Наурыз К.Ж., Кенебаева Д.Б., Клюева П.Ю. Методические указания для выполнения дипломной работы (проекта) по специальности 050719 – «Радиотехника, электроника и телекоммуникации»: Астана 2009.

3 Гольдштейн Б. С., Пинчук А. В., Суховицкий А. Л. IP-телефония: Радио и связь, 2008.

4 Стив Мак-Квери, Келли Мак-Грю, Стивен Фой. Передача голосовых данных по сетям CiscoFrameRelay, ATM и IP; Киев, 2007.

5 Росляков А.В. IP-телефония; Москва, 2008.

6 Джонатан Дэвидсон, Джеймс Питерс, МаножБхатия, СатишКалидинди, Судипто М. Основы передачи голосовых данных по сетям IP (IP Voiceover IP Fundamentals); Вильямс, 2007.

7 НопинС. В., ШаховВ. Г. Анализ защищенности абонентских систем IP-телефонии от несанкционированного доступа // Информационные технологии. 2008. № 11. С. 67-74.

8 Блоги по технологиям и оборудованию cisco от инструкторов – Режим доступа: http://www.anticisco.ru/blogs. Дата обращения: 03.03.2010.

9 Форум тех.поддержки – Режим доступа: http://voip.jalita.com/literature. Дата обращения: 29.04.2010.

10 Ciscosystems – Режимдоступа: http://www.cisco.com/russian_win /warp/public/3/ru/solutions/sec/mer_tech_ident-tacacs.html. Датаобращения: 6.02.2010.

11 OpenNET – Режим доступа: http://www.opennet.ru/base/cisco/radius.txt Дата обращения: 7.03.2010.

12 Computerclub - Режим доступа: http://www.ccm.kz/article/default.Дата обращения: 6.02.2010.

13 Сайт об IP-телефонии- Режим доступа: http://ukash.idhost.kz. Дата обращения: 8.04.2010.

14 Price zone. IP-телефонии. Обзор технологии -Режим доступа: http://www.price.od.ua/articles.phtml_id=71. Дата обращения: 8.05.2010.

15 Исследования - Режим доступа: http://www.comcon-2.kz/ consultation/konsl_000023.php. Дата обращения: 10.05.2010.

16 Компьютерная документация и софт - Режим доступа: http://www.winsov.ru/net036.php. Дата обращения: 10.05.2010.

17 Стоп вирус -Режим доступа: http://www.stopvirus.kz/index.php. Дата обращения: 11.05.2010.

18 Проект объединения независимых сетей VoIP - Режим доступа: http://voipx.ru/cgi-bin/loscont.cgi?ID=08. Дата обращения: 12.05.2010.

19 Интернет решения - Режим доступа: http://www.gelios.biz/articles/ip-telefoniya-nastoyashhee-i-budushhee.html. Дата обращения: 6.05.2010.

20 IP-телефония - Режим доступа: http://www.ctspi.ru/TechSupp/ IPTEL/Obzor.htm. Дата обращения: 13.05.2010.

21 Современные технологии - Режим доступа: http://www.telda.ru/ connection.html.Дата обращения: 16.05.2010.

22 Официальный сайт Президента Р.К. – Режим доступа: http:// www.akorda.kz. Дата обращения: 01.06.2010.

23 Мирманов А.Б., Наурыз К.Ж., Кенебаева Д.Б., Клюева П.Ю. Методические указания для выполнения дипломной работы (проекта) по специальности 050719 – «Радиотехника, электроника и телекоммуникации»: Астана 2009.

24 Гольдштейн Б. С., Пинчук А. В., Суховицкий А. Л. IP-телефония: Радио и связь, 2008.

25 Стив Мак-Квери, Келли Мак-Грю, Стивен Фой. Передача голосовых данных по сетям CiscoFrameRelay, ATM и IP; Киев, 2007.

26 Росляков А.В. IP-телефония; Москва, 2008.

27 Джонатан Дэвидсон, Джеймс Питерс, МаножБхатия, СатишКалидинди, Судипто М. Основы передачи голосовых данных по сетям IP (IP Voiceover IP Fundamentals); Вильямс, 2007.

ПРИЛОЖЕНИЕ