МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет
имени К.И. Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра «Электроника, телекоммуникации и космические технологии»

Қасымхан Н.Е.

Анализ обеспечения безопасности в IP-телефонии

ДИПЛОМНАЯ РАБОТА

специальность 5В071900 – Радиотехника, электроника и телекоммуникация

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И. Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра «Электроника, телекоммуникации и космические технологии»

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой ЭТиКТ
канд.техн.наук
_____ Е. Ташгай
"13" 05 2019г

ДИПЛОМНАЯ РАБОТА

На тему: Анализ обеспечения безопасности в IP-телефонии

по специальности 5В071900 – Радиотехника, электроника и телекоммуникация

Выполнила Касымхан Н.Е.

Рецензент
канд.техн. наук, профессор АУЭС
_____ А.С. Байкенов
_____2019г.

Научный руководитель
маг-р техн. наук, лектор
_____ Г.М. Байкенова
"1" 05 2019г.

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И. Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра «Электроника, телекоммуникации и космические технологии»

5В071900 – Радиотехника, электроника и телекоммуникация

УТВЕРЖДАЮ
Заведующий кафедрой ЭТиКТ
канд.техн.наук
_____ Е. Таштай
"_08_" _____02_____ 2019г

ЗАДАНИЕ
на выполнение дипломной работы

Обучающемуся *Касымхан Назерке Ерканкызы*
Тема *Анализ обеспечения безопасности в IP-телефонии*
Утверждена *приказом Ректора Университета* № 1162-б от "16" 10 2018г
Срок сдачи законченной работы "16" мая 2019г.
Исходные данные к дипломной работе: *Стандарты IP-телефонии; Оборудование; Протоколы обеспечения безопасности IP-телефонии.*
Краткое содержание дипломной работы:
а) *Общие сведения об IP-телефонии*
б) *Анализ безопасного соединения в сетях IP – телефонии*
в) *Модель организации обеспечения безопасности в IP-телефонии на примере Site-to-site VPN*
Перечень графического материала (с точным указанием обязательных чертежей): *Структурная схема IP-телефонии, Сценарии IP-телефонии, Организация безопасности стандартов, Схема распределения ключей при симметричном и ассиметричном шифровании, Схема работы IP-телефонии через VPN-туннель, Схема Site-to-site VPN на Cisco ASA*
Рекомендуемая основная литература:
1 Б. С. Гольдштейн, А. В. Пинчук, А. Л. Суховицкий. IP-телефония. - СПб.: БХВ-Петербург, 2014. —336 с.
2 Баскаков И. В., Пролетарский А. В., Мельников С. А., Федотов Р. А., IP-телефония в компьютерных сетях: Учебное пособие. – Москва, 2008.
3 Смит Ричард Э. Аутентификация: от паролей до открытых ключей. - М.: издательский дом «Вильямс», 2002.

ГРАФИК

подготовки дипломной работы (проекта)

Наименования разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю и консультантам	Примечание
Принципы передачи голосовой информации в сетях с коммутацией пакетов	8.02.2019	Выполнено
Обеспечение безопасности в IP-телефонии	22.03.2019	Выполнено
Модель организации обеспечения безопасности в IP-телефонии на примере Site-to-site VPN	21.04.2019	Выполнено

Подписи

консультантов и нормоконтролера на законченную дипломную работу (проект) с указанием относящихся к ним разделов работы (проекта)

Наименования разделов	Консультанты, И.О.Ф. (уч. степень, звание)	Дата подписания	Подпись
Нормоконтролер	доктор PhD Тайсарлова Р.Н.	13.05.2019	

Научный руководитель _____ Г.М. Байкенова
(подпись)

Задание принял к исполнению обучающийся _____ Н.Е. Касымхан
(подпись)

Дата "_16___"___10_____2018г.

АННОТАЦИЯ

Данная дипломная работа посвящена вопросам анализа обеспечения безопасности в IP-телефонии – системы связи, которая предполагает отправку голосового сигнала по сетям IP. Во всех подробностях разбираются подходы в построении IP-телефонии, также ее защита, обеспечение безопасности для совершаемых атак на ее структуру.

Не менее 50% дипломной работы уделяется практическим материалам по анализу защиты данных и конфигурации структурных элементов VoIP-сети, исходя из требований малых предприятий, так и компаний с развитой филиальной сетью.

АҢДАТПА

Бұл дипломдық жұмыс IP-телефония қауіпсіздігін қамтамасыз етудегі талдау мәселелеріне арналған. IP-телефония дегеніміз IP желілері бойынша дауыстық сигналды жіберуді болжайтын байланыс жүйесі. Берілген мәліметтер бойынша IP-телефонияны құру тәсілдері, сондай-ақ оны қорғау, оның құрылымына жасалатын шабуылдар үшін қауіпсіздікті қамтамасыз ету қарастырылады.

Дипломдық жұмыстың 50%-нан астамы шағын кәсіпорындардың, сондай-ақ дамыған филиалдық желісі бар компаниялардың талаптарын негізге ала отырып, VoIP-желісінің құрылымдық элементтерінің конфигурациясы мен деректерді қорғауды талдау бойынша практикалық материалдарға бөлінеді.

ANNOTATION

This thesis is devoted to the analysis of security in IP-telephony - a communication system that involves sending a voice signal over IP networks. The approaches to building IP-telephony, as well as its protection, ensuring security for the attacks on its structure are described in details.

At least 50% of the thesis is given to practical materials on data protection analysis and configuration of the structural elements of a VoIP network, based on the requirements of small enterprises and companies with a developed branch network.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современное время стремительными темпами идет развитие сети Интернет, различных сетей на базе IP протокола, а также сетей IP-телефонии. Мировая сеть Интернет, предоставляя огромное количество услуг, верно входит в наши жизни.

На сегодня практически невозможно представить осуществление успешной работы какой-либо компании при отсутствии локальной сети. Большие компании организовывают свои сети, которые находятся в нескольких корпусах или даже в местностях.

На данном этапе нелегко переоценить важность информации и важность обеспечение ее защиты. Ведь для получения важных данных, злоумышленнику необязательно иметь физический доступ к ним, как раньше. Имея необходимые знания, умения и владея определенным комплексом программно-аппаратных средств, легко реализовать кражу или копирование ценной информации не покидая дом.

IP-телефония, являясь преемником двух технологий, – простой телефонии с коммутацией каналов и IP-сетей с коммутацией пакетов, – вобрала в себя и комплекс проблем, относящиеся к обеспечению безопасности. От простой телефонии она получила хищение сервисов, а различного рода атаки в компьютерном мире (от отказа в обслуживании до хищения пакетов с дальнейшим прослушиванием) досталась ей от IP-сетей.

Все разнообразие возможных опасностей для сетей IP-телефонии, можно поделить на два вида: угрозы, которые возникают в ходе неразрешенного доступа к ресурсам сети и угрозы, возникающие при передаче информации по каналам. Для предотвращения угроз первого вида необходим надежный механизм аутентификации, авторизации и учета. Остальные проблемы можно исключить с помощью правильно подобранного алгоритма шифрования или может даже построения некой системы всей сети IP-телефонии, которая была бы способна осуществить данный алгоритм шифрования.

В данной дипломной работе описываются построение современной безопасной сети VoIP, проводится анализ типов угроз и методы борьбы с ними. Как результат, производится выработка рекомендации по обеспечению безопасности в сетях IP-телефонии и дается сценарий безопасного VoIP-соединения.

1 Принципы передачи голосовой информации в сетях с коммутацией пакетов

1.1 Интеграция традиционной телефонии и сетей передачи данных

Самая первая передача голоса через интернет-протокол (voice over IP, VoIP) состоялась в 1973 году, в результате тестирования экспериментального протокола Network Voice, специально созданного для ARPANET. Но затем, до 1995 года, каких-либо значительных шагов предпринято не было. Однако без таких нескольких историй не было бы основной истории.

Основы для VoIP были положены в 1925-1928 годах, еще в то время, когда был изобретен вокодер (Vocoder) – электронный синтезатор речи на базе компании AT&T. Этот синтезатор воспроизводил подобие человеческой речи, изучая звуки издаваемые человеком. Данное устройство активно использовалось во времена Второй Мировой войны для передачи конфиденциальных информаций.

В 1988 году произошло еще одно событие, имевшее значение – появление первого знаменитого кодека G.722 (Wideband Audio Codec), качество которого сравнимо с речью, передаваемой по ТфОП. Данный широкополосный кодек, который имел битрейт, вдвое превосходящий битрейты предыдущего G.711, и издавал он отличный звук по тем временам.

В 1991 году Джон Уолкер, основатель Autodesk, собрал структуру для VoIP, которая требовала пропускную способность всего 32 кбит/с (64 кбит/с - норма по тому времени) и сделал публичный релиз программы NetFone (позднее его переименовали в Speak Freely), которая и стала первым в мире VoIP-телефоном. Но на самом деле, изначально для чего был использован и создан NetFone – осуществление связи внутри компании Уолкера.

В 1993 году возникла первая система для связи видеоконференций Telepresence System, которая была названа Телепорт (Teleport), но в дальнейшем переименованная в Tele Suite.

Наряду с этим, в исследовательских центрах и университетах параллельно проводились исследования по передаче речи при помощи пакетной коммутации данных.

После появления Интернета, для общения друг с другом, пользователям не хватало голосовой связи. Решением просьб и требований пользователей стало появление VoIP - протокола пакетной передачи голоса, в 1995 году. По данному протоколу, пакеты передавались от одного адреса к другому по Интернет-протоколу. Так и появилась IP-телефония.

Вообще, вначале IP-телефония считалась просто как дешёвое решение междугородной и международной связи. Но она очень быстро стала востребованной среди пользователей и бизнесменов.

1993 - 1994 года. Чарли Клэйн создал первую программу для ПК - Maven, которая могла передавать голос по сети. Примерно в это же время

популярность набрала программа для организации видеоконференций CU-See Me, для ПК на Macintosh, разработанная в Корнельском университете. Оба эти приложения обрели огромную популярность - с их помощью на Земле транслировался полёт космического челнока Endeavor. Maven мог передавать звук, а CU-See Me - изображение. Через некоторое время, эти две программы объединили в одну общую [1].

В 1995 году израильская компания Vocal Tec изобрела самый первый интернет-телефон, которого назвали просто Internet Phone, и он был доступен широким массам.

В 1996 году выпущена была самая начальная версия стандарта H.323, который был предназначен для голосовой и видеосвязи через Интернет, в это же время была начата работа над открытым стандартом IP-телефонии - стандартом SIP. Первоначально, SIP был создан и осуществлен для соединения нескольких человек в режиме конференции и ничего общего с VoIP-телефонией у этого стандарта не было. Первая разработка SIP знала только одну команду - сделать вызов, и только через три года было освоено, в общем, шесть команд. Но уже тогда было ясно, что по своему потенциалу и объему он обойдёт H.323.

1998 год был одним из кризисных и поворотных для IP-телефонии. Предприятия сумели осознать все достоинства данного типа связи и стали разрабатывать свои частные решения. В особенности, бизнесмены приступили к отказу от продуктов ПК-ПК и стали осуществлять решения ПК-телефон и телефон-телефон для VoIP. IP-телефония начала соединяться в коммутируемые телефонные сети общего пользования (public switched telephone network, PSTN, ТСОП, ТфОП).

В этом же году появились первые IP-коммутаторы – считавшиеся первым физическим оборудованием для IP-телефонии, отвечавшие за маршрутизацию вызовов. Вопреки таким техническим прорывам, VoIP-звонки по состоянию на 1998 год не дотягивали даже до 1% от всего голосового трафика. В 2000 году эта цифра едва дошла до 3%, а вот в 2003 произошёл резкий скачок — до 25%. Телефонные звонки по IP-протоколу быстро обрели образ бесплатных и очень дешёвых вызовов на все направления, независимо от расстояния. Одно время коммерческие компании по-своему эксплуатировали эту бесплатность и могли транслировать рекламные ролики в начале или середине разговора как «плату» за свободное соединение. Позже такая практика прекратилась.

В 1999 году появляется первая IP-PBX (виртуальная АТС именно для VoIP, потому что виртуальная АТС для PSTN была создана ранее) - Asterisk. Как это часто бывает, Asterisk вырос из потребности компании в продукте, который она не может купить или который её не устраивает. Таким образом, Марк Спенсер, имеющий собственную компанию по технической поддержке Linux, понял, что ему срочно нужна мощная АТС для call-центра, но по тем временам это оборудование стоило больших денег. Тогда, он создал свою IP-АТС с открытым исходным кодом. После того, как Asterisk набрал популярность, Спенсер поменял профиль компании на поддержку и разработку аппаратного обеспечения для Asterisk. До сих пор, Asterisk пользуется у

разработчиков и бизнеса большой популярностью. Так, например, когда мы интегрировали IP-телефонию со своей Region Soft CRM, выбрали основной виртуальной АТС именно Asterisk [2].

В 2000 году компания Cisco считалась одним из лидеров в области работы с технологиями. И в этом же году она осуществила переход на IP-телефонию всех своих штабов в Калифорнии, а именно в Сан-Хосе. Весь этот процесс занял около года и 55 зданий с 20 000 человек перешли на IP-телефонию. Данный проект считался одним из самых масштабных. Этот опыт не мог не сказаться на профиле компании, ведь на сегодняшний день Cisco дает исключительные возможности и решения в области IP-телефонии и управлении сетью.

2005 год. Предприятие Calypso Wireless представила на рынке телефон C1250i, самый первый мобильный телефон, который мог переключаться между вышкой сотовой связи GSM и доступной сетью Wi-Fi 802, при этом используя Cisco Aironet Access Point и собственную патентованную технологию Calypso Wireless ASNAP. При помощи этого пользователи могли организовывать видеоконференции и делать звонки по VoIP. Фактически данный телефон считался смартфоном на WindowsMobile.

В 2006 году было разработано первое мобильное приложение для IP-телефонии Truphone. С начала данное приложение было создано для сотовых телефонов модели Nokia, но затем оно было выпущено и для платформ iPhone, Android и BlackBerry. Truphone мог делать бесплатные звонки внутри своей сети, отправлять текст в другую сеть, в том числе на Skype и звонить на ТфОП. Приложение использовало стандарт SIP и звонило не через GSM, а через сеть Wi-Fi. Позже компания выпустила несколько softphone-ов, а в данный момент она занимается выгодными туристическими SIM-картами.

Постепенно эти softphone-ы научились сотрудничать с телефонами ТфОП, мобильными, а также факсами и электронной почтой. Более того, до сих пор при тестировании средств IP-телефонии, в крупных компаниях, в тест-план обязательно входят тесты на отправку факсов с одного аппарата на другой аппарат, факса на почту и факса между протоколами SIP, H.323 и OKC7.

IP-телефония имеет огромные преимущества, которые сделали её очень популярной и оставили потенциал развития:

-она дешевая – каждый пользователь получает общий тариф, вне зависимости от расстояния;

-она имеет открытые стандарты;

-она сравнительно простая для разработчиков;

-её поддерживают многие устройства и платформы;

-она легко встраивается в сторонние приложения и т.д.

Сегодня, IP-телефония окружает нас везде, в том числе и дома, и в бизнесе. Она сделала прорыв в мире связи – телекоммуникационные гиганты были вынуждены понизить цены и искать оптимальные решения для своих клиентов. В истории IP-телефонии достаточно много интересных моментов: от

шифрования до работы СОРМ в VoIP, от протоколов до нестандартного оборудования. История продолжается и до сих пор, обещает быть интересной.

1.2 Общие сведения об IP-телефонии

1.2.1 Основные понятия об IP-телефонии

Под IP-телефонией принято понимать технологию, использующую сеть с пакетной коммутацией для ведения любых типов разговоров и передачи факсов в режиме реального времени на базе протокола IP. Наиболее распространенной такой сетью является – Интернет. Иногда можно встретить такой термин – VoIP (VoiceOver IP), по-другому «голос по IP», что означает передачу голосовой информации по линиям IP.

Долгое время сети с коммутацией каналов (т.е. телефонные сети) и сети с коммутацией пакетов (IP-сети) могли существовать независимо друг от друга. Одни каналы мы могли использовать для передачи голосовой информации, а другие – для передачи данных. IP-телефония позволила нам объединить обе сети с помощью так называемого шлюза - устройства, стоящего на стыке телефонной и IP-линий.

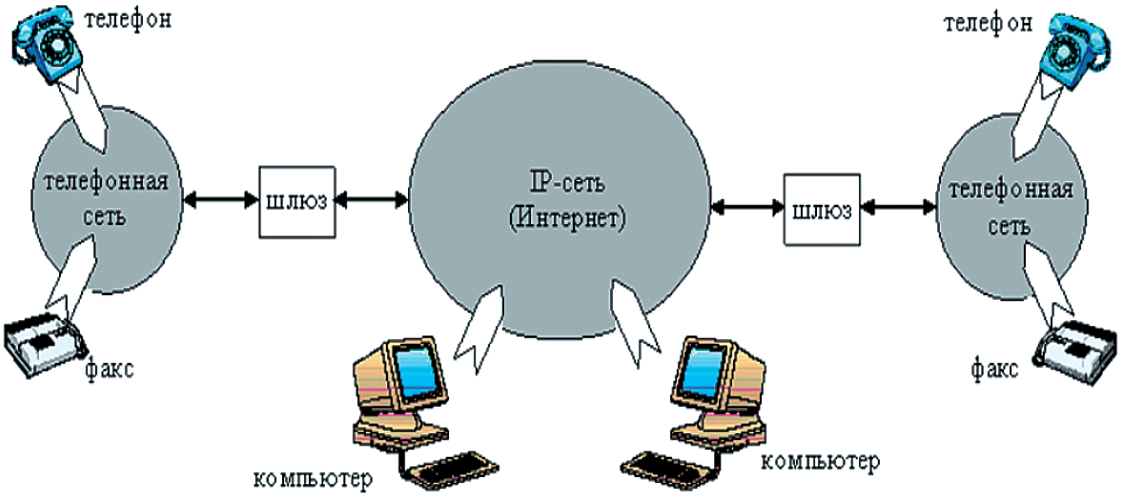


Рисунок 1.1– Пример простого построения IP-телефонии

Передача голоса в IP-сети происходит следующим образом. Входящий звонок и сигнальная информация из телефонной сети передаются на пограничное сетевое устройство, которое называется телефонным шлюзом, и обрабатываются специальной картой устройства голосового обслуживания. Шлюз, используя протоколы управления стандарта H.323, перенаправляет сигнальную информацию другому шлюзу, который находится на приемной стороне IP-сети. Принимающий шлюз осуществляет передачу сигнальной информации на приемное телефонное оборудование, при этом гарантируя

сквозное соединение. После того, как обеспечивается установка соединения, голос на входном сетевом устройстве оцифровывается (если он не был цифровым), кодируется в соответствии со стандартными алгоритмами ITU, такими как G.711 или G.729, затем сжимается, и в виде пакетов отправляется по назначению на удаленное устройство с использованием стека протоколов TCP/IP. Поступающие на приемный шлюз IP-пакеты преобразуются обратно в телефонный сигнал, и принимающий абонент получает вызов.

Протоколы – это то, из чего состоит сама IP-телефония, они осуществляют организацию телефонного разговора, управляют вызовами и передают трафик по сети. Существуют три крупных семейства стандартов, отличающиеся между собой подходами в построении сети: H.323, SIP и MGCP.

Стандарт IP-телефонии H.323 считается древнейшим и он необходим для осуществления VoIP-телефонии и видеоконференцсвязи. Это огромный набор протоколов и элементов, которые могут позволить передавать медиа по пакетным сетям с негарантированной пропускной способностью. Состав рекомендации H.323 предполагает разные возможности коммуникации – от простой телефонии до видеоконференцсвязи с дальнейшей передачей медиа [4].

Одним из достоинств стандарта H.323 является его связующая функция, которая обеспечивает различным устройствам производителей сотрудничать и взаимодействовать друг с другом.

Самыми основными элементами сети являются: терминал (Terminal), шлюз (Gateway), привратник (контроллер зоны, Gatekeeper) и устройство управления конференциями (MultipointControlUnit- MCU) [4].

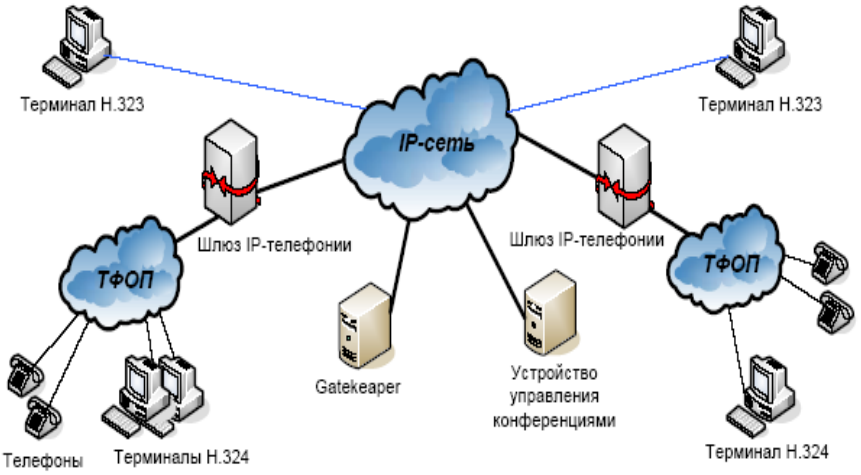


Рисунок 1.2– Архитектура сети IP-телефонии по стандарту H.323

Терминал (Terminal) – оконечное устройство пользователя сети IP-телефонии, обеспечивающее двухстороннюю мультимедийную связь с другими терминалами H.323, устройством управления конференциями или шлюзом.

Главное предназначение шлюза – преобразование речевой информации, которые поступают со стороны ТфОП, в такой вид, который был бы пригодный

для дальнейшей передачи по сетям с маршрутизацией пакетов IP. Кроме этого, шлюз преобразовывает сигнальные сообщения систем сигнализации ОКС7 и DSS1 в сигнальные сообщения H.323 и проводит обратное преобразование согласно с рекомендацией ITUH.246.

Шлюз позволяет сжимать информацию (голос), конвертировать её в IP пакеты и направляет в IP-сеть.

Сервер управления конференциями (MCU) осуществляет связь двух и более терминалов – H.323. Все H.323-терминалы, которые участвуют в конференции, могут устанавливать соединение с MCU [4].

В составе устройства управления конференциями должен быть один обязательный элемент контроллера конференций (MC), и он может включать в себя несколько процессоров для обработки пользовательской информации (MP). Элемент контроллера конференции может быть совмещён с контроллером зоны, шлюзом или устройством управления конференциями, а устройство управления конференциями, может быть совмещено со шлюзом или контроллером зоны.

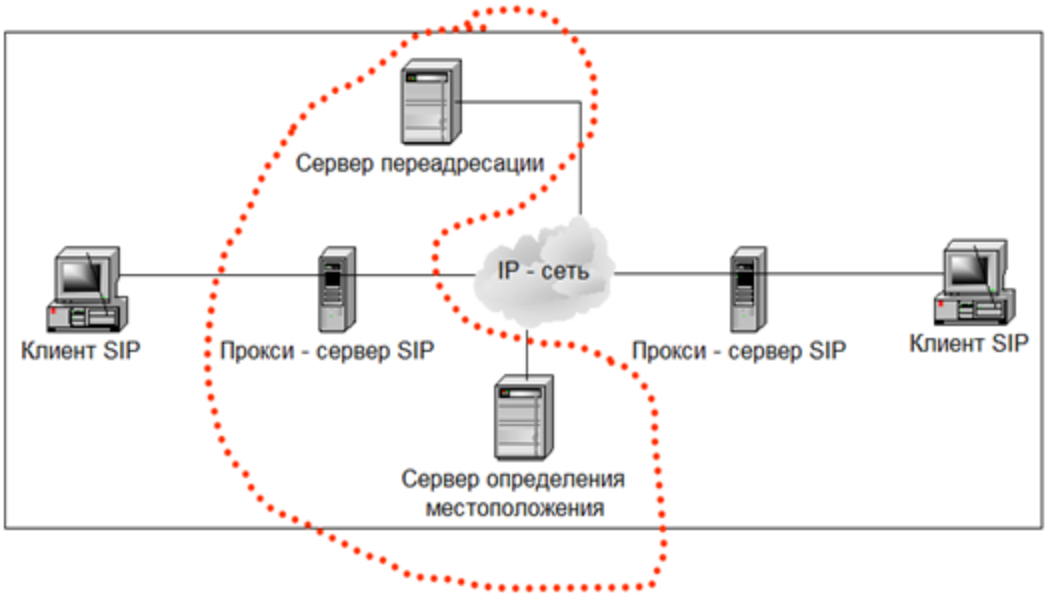
SIP представляет из себя текстово-ориентированный протокол, являющийся частью глобальной архитектуры мультимедиа, которая разработана комитетом IETF. Путь SIP в построении сетей IP-телефонии считается намного проще в реализации, по сравнению с H.323. Вообще, SIP основан на том же подходе, что и протокол передачи гипертекста HTTP: запрос – ответ (request – reply). Все сообщения SIP являются текстовыми, и их можно читать глазами, а коды возврата считаются такими же, как и в HTTP, поэтому некоторые из них могут показаться хорошо знакомыми не только сетевым администраторам, но и многим другим продвинутым пользователям интернета (404 - абонент не найден, 200 - OK). И из-за этого протокол SIP можно считать более подходящим поставщикам услуг Интернет в предоставлении услуги IP-телефонии, и при этом, эта услуга будет являться всего лишь малой частью пакета услуг.

Протокол SIP умело поддерживает услуги интеллектуальной сети, такие как преобразование имён, переадресация и маршрутизация, что и является существенным для использования SIP в качестве протокола сигнализации в сетях общего пользования, где преимущественной задачей оператора является оказание широкого спектра телефонных услуг. Также еще одной важной особенностью протокола SIP считается поддержка мобильности пользователя. Это свойство SIP не является уникальным, потому что, протокол H.323 тоже в какой-то степени поддерживает такую возможность.

Сеть протокола SIP состоит из основных элементов трех видов: агенты пользователя, прокси-серверы и серверы переадресации.

Агенты пользователя (User Agent или SIP client) являются приложениями терминального оборудования и они могут включать в себя два элемента: агент пользователя – клиент (User Agent Client – UAC) и агент пользователя – сервер (User Agent Server – UAS). Клиент UAC активизирует SIP-запросы, т. е. выполняет роль в качестве вызывающей стороны. Сервер UAS является

принимающей стороной запросов и возвращает ответы, т.е. выступает в качестве вызываемой стороны. Агент пользователя умеет хранить состояние сеанса или диалога.



- Может быть реализовано в одном физическом устройстве

Рисунок 1.3 – Сеть, построенная на базе протокола SIP

1.2.2 Виды соединений

Структура IP-телефонии представляет из себя комплекс терминального оборудования, каналов связи и узлов коммутации. Они формируются по таким же принципам, что и сети Интернет.

Существуют три самые часто используемые сценария в сетях IP-телефонии:

– "компьютер – компьютер";

– "компьютер – телефон";

– "телефон – телефон".

Составляющие элементы IP-телефонии по сценарию «компьютер-компьютер» показаны на рисунке 1.4.

По этому сценарию аналоговые голосовые сигналы от микрофона узла А модифицируются в цифровой вид с помощью аналого-цифрового преобразователя (АЦП). Отсчеты речевой информации в цифровом виде потом сжимаются кодирующим оборудованием в отношении 4:1, 8:1 или 10:1. Конечные данные, после того как сжались, объединяются в пакеты, к которым после прибавляются заголовки протоколов и только затем эти пакеты отправляются по IP-сети в систему IP-телефонии, который и обслуживает абонента Б. После того, как пакеты принимаются системой абонента Б,

заголовки протокола устраняются, а сжавшиеся речевые информации принимаются в устройство, который их развертывает в начальную форму. Затем данные обратно преобразуются в аналоговый вид с помощью цифро-аналогового преобразователя (ЦАП) и поступают в телефон абонента Б.

Рисунок 1.4 – Сценарий IP-телефонии "компьютер – компьютер"

Другой сценарий «телефон – компьютер» – применяются в разных видах справочно-информационных службах Интернет, в Call-центрах а также может в службах технической поддержки. Интернет-пользователь, который подключился к серверу WWW какой-то компании, получает возможность обращаться к оператору справочно-информационной службы.

Рассмотрим две разновидности сценария «телефон – компьютер» IP-телефонии:

–от компьютера (пользователя IP-сети) к телефону (абоненту ТфОП) - предполагается, что установку соединения запрашивает сам пользователь IP-сети. Шлюз для содействия сетей ТфОП и IP может реализоваться в отдельном оборудовании или соединятся в устройство ТфОП или IP-сети, которое уже существует;

–от абонента ТфОП к пользователю IP-сети с распознаванием принимаемой линии на базе нумерации по Е.164 или IP-адресации. В данном примере, установку связи между пользователем сети и абонентом ТфОП начинает абонент ТфОП.

При попытке осуществить вызов справочной службы, с помощью услуги пакетной телефонии и обычного телефона, абонент А вызовет ближайший шлюз IP-телефонии. От шлюза к абоненту А запрашивается ввести номер, к которому хочет отправить вызов (например, номер службы), и свой личный идентификационный номер (PIN) для распознавания и дальнейшего начисления платы. Анализируя вызываемый номер, шлюз находит самый удобный и доступный путь к этой службе. Также, шлюз может активизировать свои задачи для кодирования и сбора речи в пакеты, осуществляет контакт со службой, наблюдает за процессом обслуживания вызова, а также осуществляет прием информации о состояниях данного процесса (например, занятость, посылка вызова, разъединение и т.п.) от исходящей стороны по протоколу сигнализации и управления. Прерывание с каждой другой стороны передается второй стороне по протоколу сигнализации и просит завершения уже установленных соединений и высвобождения ресурсов шлюза для обслуживания дальнейшего вызова. Для осуществления соединений от службы к абонентам применяется такой же способ.

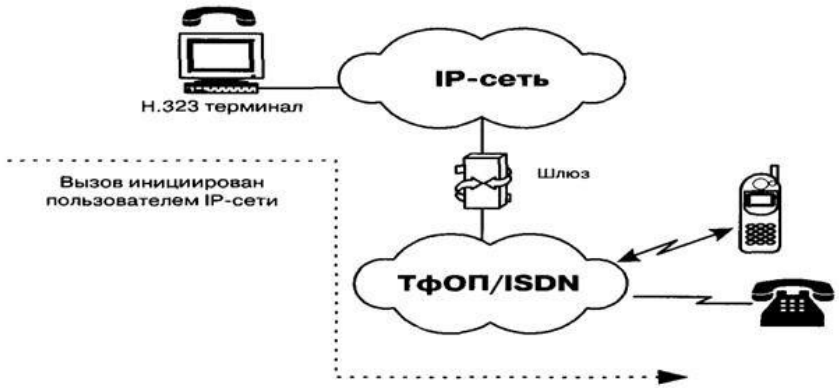


Рисунок 1.5 - Сценарий IP-телефонии "компьютер – телефон"

Успешность соединения услуг передачи речи и информации считается главным стимулом применения IP-телефонии по сценариям «компьютер-компьютер» и «компьютер-телефон», не причиняя никаких ущербов пользе операторов классических телефонных сетей.

Отличие сценария IP-телефонии «телефон – телефон» заключается в том что, он предполагает возможность предоставления международной и междугородной связи простым абонентам.

Как показано на рисунке 1.6, импортеры IP-услуг оказывают услуги «телефон – телефон» при помощи установления шлюзов IP-телефонии на входе и выходе IP-линий. Абоненты подключаются к шлюзу поставщика через ТфОП, набирая специальный номер доступа. Клиенту предоставляется доступ к шлюзу, если тот использует персональный идентификационный номер (PIN) или услугу идентификации номера вызывающего абонента (Calling Line Identification). Затем шлюз попросит ввести номер телефона вызываемого клиентом абонента, анализируя данный номер он определит какой шлюз имеет хороший доступ к необходимому телефону. После того, как между входным и выходными шлюзами установится контакт, дальнейшая установка соединения к нужному абоненту происходит выходным шлюзом по его местной телефонной сети [3].

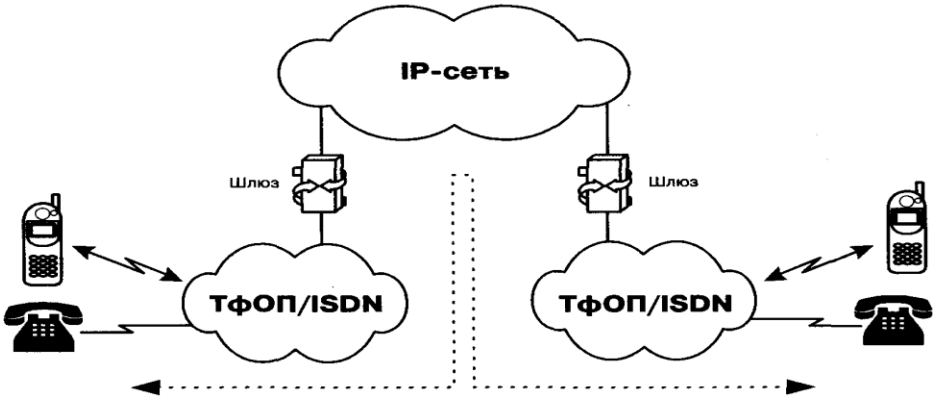


Рисунок 1.5 – Соединение абонентов ТфОП через транзитную IP-сеть по сценарию "телефон – телефон"

1.3 Виды угроз для системы голосовой связи

При выборе метода для постройки системы голосовой связи большое внимание уделяется соображениям безопасности. При введении в компании классической АТС на основе технологии TDM или новой системы IP-телефонии специалисты, и администраторы структуры голосовой связи должны выбрать соответственные меры для того, чтобы предотвратить реализацию угроз как, мошенничество при проведении междугородного общения и прослушание телефонных разговоров.

Понятие безопасности всегда предусматривается при исследовании и введении систем голосовой связи. Это началось еще тогда, когда появились частные телефонные линии, когда прослушивание линии считалось постоянной и огромной угрозой. Самые первые случаи хакерской атаки системы голосовых связей были предприняты в 1970-х годах, когда злоумышленники подделывали сигналы управления вызовами при помощи специальных оборудований и реализовывали бесплатные телефонные звонки. На сегодняшний день среди самых частых нападений на телефонные системы TDM, а также на системы IP-телефонии, считаются атаки: "отказ в обслуживании", афера при реализации междугородных переговоров и прослушивание телефонных переговоров.

Классификация угроз для сетей VoIP представлена ниже.

Vishing (VoIP- phishing). Эти угрозы предполагают изменение работы механизмов аутентификации злоумышленником, для того чтобы заменить личность или его данные. Обычно злоумышленник пользуясь доверием пользователя может получить необходимые данные для аутентификации.

Toll Faud. Правонарушитель получая доступ к сети, может произвести неодобренные действия, он может удалять данные, изменять счета и все это с целью злонамеренного использования услуг VoIP.

Spam Over IP telephony (SPIT) – предполагает использование заранее подготовленные сообщения, поступающие в виде звонков, что может вызвать перегрузку сети или может отказ в обслуживании.

Отказ в обслуживании. При осуществлении атаки "отказ в обслуживании" хакеры применяют программные возможности, отправляющие огромное количество пакетов без смысла на IP-телефоны, бизнес-серверы или части сетевой инфраструктуры. Целью злоумышленников является загруженность сетевых резервов для того, чтобы вызовы прервались или же, чтобы обработка вызовов была невозможной. Простой причиной атаки является отвлечение ИТ-специалистов, чтобы они не обратили внимания на другие атаки.

Прослушивание телефонных разговоров или атака вида "человек в середине". При осуществлении атак вида "человек в середине" пользователь, который внутри может присвоить себе IP-адрес маршрутизатора или компьютера для прослушивания голосового потока и информаций, которые вводятся с клавиатуры IP-телефона, например, пин-кодов.

Перехват и модификация. В данном виде угрозы, злоумышленник совершает более активные действия в сетевом трафике, что может привести к сбросу вызовов, подмене вызовов и изменению его данных.

Подмена абонента. При реализации атаки вида "подмена абонента" хакер подделывает данные доступа законного пользователя с тем, чтобы вызовы, производящиеся с телефона злоумышленника, были похожи на исходящие вызовы с телефона другого пользователя. Злоумышленник может сымитировать IP-адрес собственного узла или создать свой DHCP-сервер, который отвечает за распределение IP-адресов.

Безопасность инфраструктуры. Для осуществления защиты системы голосовой связи применяются те же проверенные целостные решения Cisco, которые обеспечивают безопасность передачи данных. Объединения, включившие сеть Cisco (SDN) уже имеют фундамент для построения безопасной системы голосовой связи.

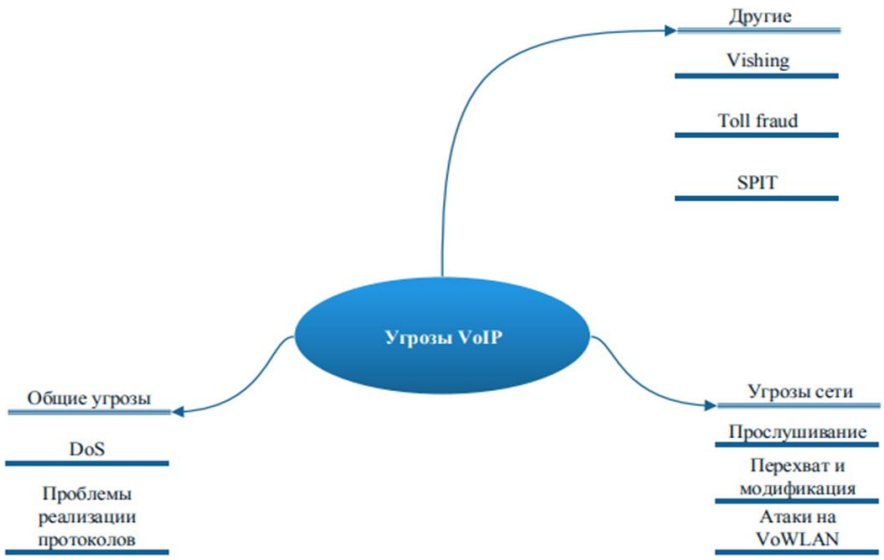


Рисунок 1.6 – Угрозы для VoIP

1.4 Постановка задачи

В представленной дипломной работе будут рассмотрены отличительные особенности пакетной передачи речи, архитектура сети IP-телефонии, виды соединений в сети IP – телефонии, типы угроз в IP-сетях, а также методы их предотвращения. Одним из главных и важных вопросов развития IP–телефонии считается ее защита и безопасность, так как, являясь прямым последователем простой, обычной телефонии и IP-технологии, она отобрала в себя не только их преимущества, но и их недостатки. Поэтому, в данной работе я буду проводить анализ и сравнение защищенного соединения в сетях IP – телефонии.

Цель дипломной работы – провести анализ обеспечения безопасности в IP-телефонии. Для этого необходимо решить следующие задачи:

-анализ существующих видов угроз для IP-телефонии и способы их предотвращения;

-изучить протоколы обеспечения безопасности и их возможности;

-рассмотреть методы криптографической защиты информации;

-показать на примере организацию защиты информации в канале.

2 Обеспечение безопасности в IP-телефонии

2.1 Слабые места IP-телефонии

Технология VoIP – это настоящее и будущее наших телефонных коммуникаций. Но в то же время, мы не можем пренебрегать теми угрозами, которые она несет в себе, для их безопасности. VoIP имеет свои недостатки присущие любой IP-службе, учитывая ее сложную структуру и требования обслуживания в режиме реального времени. Большинство этих проблем устраняются при помощи защищенных IP-УАТС и телефонов, развертывания VoIP-оптимизированных межсетевых экранов (МЭ), модернизации инфраструктуры с учетом требований безопасности, а также средств безопасности общего назначения. Но перед тем, как прибегнуть к рекомендациям по обеспечению безопасности, нам следует выявить существующие уязвимости и угрозы.

IP-телефония являясь последователем IP-сети, наследует от нее как достоинства, так и недостатки обеспечения безопасности. IP-телефония считается в своем роде уникальной службой, но защищена она не лучше чем любая другая IP-служба, к примеру, как электронная почта. Эти службы часто являются мишенью для атак, так как имеют свои изъяны и уязвимости.

Для VoIP-сети необходимо большее количество элементов и программ, по сравнению с другими классическими сетями с коммутацией каналов. К таким элементам относятся: серверы поддержки, коммутаторы, маршрутизаторы, МЭ, IP-УАТС, кабельные системы, программные телефоны. Уязвимость высока, если много компонентов.

На сегодня существуют очень много стандартов IP-телефонии, такие как Session Initiation Protocol (SIP), H.323, Media Gateaway Control Protocol (MGCP), H.248, а также другие фирменные протоколы.

Недостатками при реализации протоколов могут быть программные ошибки. К примеру, атаки осуществляемые злоумышленником при попытке проверки размера запроса протокола:

-удаленный доступ - злоумышленник может получить удаленный доступ к системе под правами администратора;

-отказ в обслуживании - в результате неправильно сформированного запроса происходит отказ службы;

-отказ в обслуживании из-за огромной нагрузки – большое количество запросов могут «парализовать» уязвимую систему.

Пользователи сети всегда полагаются на конфиденциальность телефонных разговоров, по сравнению со службами электронной почты или же мгновенных сообщений, от которых конфиденциальности никто не ждет. Хоть и не большинство, но какая-то часть VoIP-вызовов шифруются. Наряду с этим, шифрование без строгой аутентификации не является гарантией

конфиденциальности, так как это не исключает применение злоумышленником атаки вида «человек по середине» и получения доступа к среде передачи.

2.2 Протоколы обеспечения безопасности IP-телефонии

2.2.1 Обеспечение безопасности протокола H.323

В системах IP-телефонии, построенных на основе Рекомендации ITU-T H.323, вопросами защиты и безопасности занимаются на базе Рекомендации H.235. Данная Рекомендация объясняет некоторые технические требования, наряду с вопросами безопасности: аутентификация пользователей и шифрование данных. Для того, чтобы обеспечить гарантированную связь в настоящем времени по опасным сетям, нужно учитывать две главные области обеспечения безопасности – аутентификация и шифрование.

Соответственно с Рекомендацией H.235 в системе должно быть реализовано четыре главные функции безопасности:

-аутентификация;

-целостность данных;

-шифрование;

-проверка отсутствия долгов.

Аутентификация пользователя обеспечивается управлением доступа в конечной точке сети и выполняется привратником, являющимся администратором зоны H.323 [11]. Аутентификация берет основу на использовании совместных ключей с цифровым сертификатом. Идентификаторы провайдера услуг включаются, чтобы авторизовать сертификаты.

Целостность данных и шифрование достигается криптографической защитой. Отказ в обслуживании вызова на выходе достигается проверкой отсутствия долгов. По Рекомендации H.235 для обеспечения безопасности используются такие стандарта, как: IP Security и безопасность транспортного уровня Transport Layer Security (TLS).

На рисунке 1.2 была показана архитектура H323, где одним из элементов являются терминалы – оборудование конечных точек сети, которое позволяет пользователям общаться друг с другом в реальном времени. Для работы VOIP обязательно терминалы должны поддерживать следующие протоколы:

– H.245, которые устанавливают возможности терминалов и создания канала обмена аудиоинформацией;

– H.225 используется для сигнализации вызова и установки параметров связи. Сигнализация H.225.0 основана на процедурах установления вызова ISDN и рекомендации Q.931;

– RAS используется для регистрации терминала пользователя и установки дополнительных параметров управления контроллером зоны (не используется, если нет привратника);

– RTP/RTCP для упорядочивания звуковых и видеопакетов.

<table>
<tr><td colspan="3">Гарантированная доставка информации по протоколу TCP</td><td colspan="3">Негарантированная доставка информации по протоколу UDP</td></tr>
<tr><td rowspan="2">H.245</td><td colspan="2">H.225</td><td colspan="2">Потоки речи и видеоинформации</td></tr>
<tr><td>Управление соединением (Q.931)</td><td>RAS</td><td>RTCP</td><td>RTP</td></tr>
<tr><td colspan="3">TCP</td><td colspan="3">UDP</td></tr>
<tr><td colspan="6">IP</td></tr>
<tr><td colspan="6">Канальный уровень</td></tr>
<tr><td colspan="6">Физический уровень</td></tr>
</table>

Рисунок 2.1 –Семейство протоколов H.323

Согласно рекомендации H.323, для обеспечения безопасной связи в системе необходимо использовать механизмы защиты данных канала управления Q.931, данные канала управления для коммуникаций H.245, а также данные канала передачи мультимедиа. Каналы управления вызовами H.225 и каналы сигнализации H.245 начиная с начальной станции, в обязательном порядке, должны работать в защищенных или незащищенных режимах одновременно. Обычно для канала управления вызовами защита делается предварительно. В канале сигнализации режим защиты включается после получения информации, которая была передана при помощи протокола начальной установки и подключения терминалов стандарта H.323.

2.2.2 Организация безопасности протоколов SIP и MGCP

Протокол SIP, ориентированный на применение решений третьих лиц, не имеет серьезную защиту и используется абонентскими пунктами для установки соединения. В качестве механизма аутентификации предлагаются такие варианты, как базовая аутентификация, как в HTTP, и аутентификация на основе PGP. Майкл Томас из компании Cisco Systems, чтобы устранить слабую защищенность, создал стандарт IETF, который был назван «SIP security framework». Этот протокол объясняет внутренние и внешние опасности для протокола SIP и описывает методы защиты от них. Одним из способов является защита на транспортном уровне с использованием TLS или IPSec. На рисунках 2.2 и 2.3 изображены архитектуры сетей на базе протоколов SIP и MGCP.

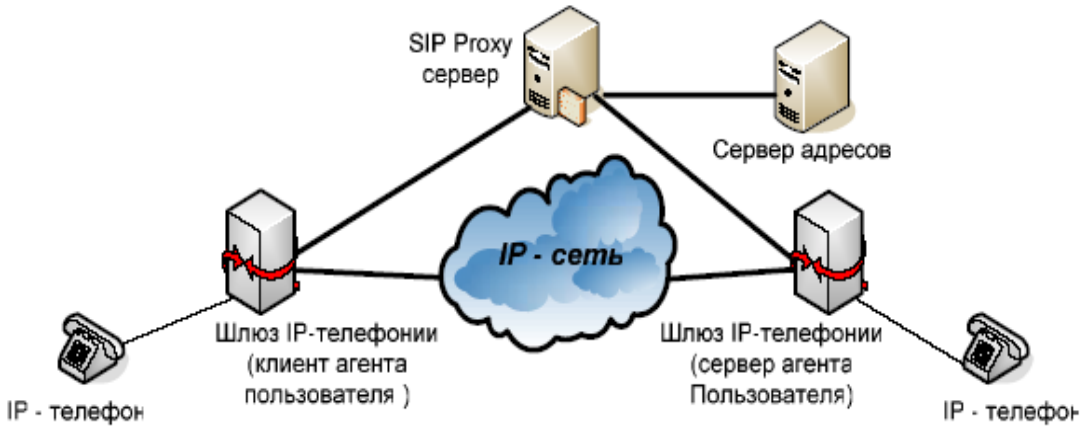


Рисунок 2.2- Архитектура сети на базе протокола SIP

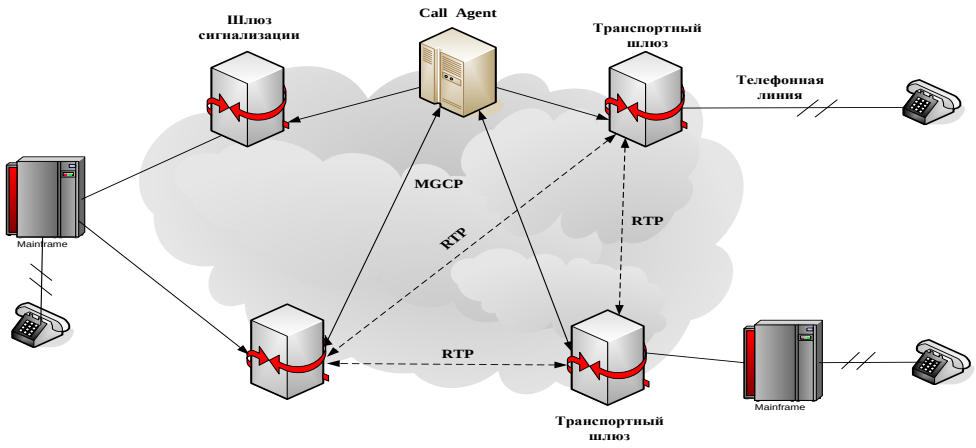


Рисунок 2.3 - Архитектура сети на базе протокола MGCP

Стандарт MGCP, использующий для защиты речевых данных - протокол ESP спецификации IPSec, определен в механизме аутентификации RFC 2705 и не применяется в оконечных устройствах. Шлюзы стандарта MGCP поддерживают работу как с элементами, поддерживающими H.323, так и с элементами, поддерживающими SIP. Защиту передаваемой информации от повторений осуществляет протокол AH, наряду с обеспечением аутентификации и целостности данных. Но в то же время, данным протоколом не достигается конфиденциальность данных, она достигается применением ESP.

2.3 Угрозы, атаки и способы их отражения в VoIP

Проблема безопасности присуща IP-телефонии, несмотря на ее несомненные достоинства, и о ней нельзя забывать. Специалистам в области IT

и защите информации, необходимо знать о возможных угрозах на элементы структуры IP-телефонии и о методах защиты от них. Также не стоит забывать о существовании стандартов VoIP и возможностях, которые они предоставляют.

Основная проблема безопасности IP-телефонии заключается в том, что она относительно проста и открыта, что позволяет злоумышленникам совершать атаки на ее элементы. Обычно случаи атаки неизвестны, но если захотеть, то их можно реализовать, так как нападения на простые IP-системы без изменений могут быть осуществлены относительно сетей передачи с цифровым голосом.

У IP-телефонии наряду с преимуществами, есть и недостатки, так как она считается прямым потомком простой телефонии и IP-технологии. Примеры атак, которые могут быть использованы:

-подслушивание;
-отказ в обслуживании;
-подмена номеров;
-кража систем;
-вызовы без предупреждения;
-неразрешенное изменение настроек.

Рисунок 2.4 – Методы защиты от угроз в VoIP

Подслушивание считается огромной проблемой, которая относится и к обычной телефонии и к IP-телефонии. Но в IP-телефонии эта опасность еще выше, так как для совершения атаки злоумышленнику не требуется иметь физический доступ к телефонной линии. В случае, если злоумышленнику удалось перехватить голосовой трафик, то восстановление исходных переговоров ему не составит труда. Для таких случаев имеются специальные автоматизированные средства. К примеру, утилита vomit (Voice Over Misconfigured Internet Telephones), конвертирующая информацию, полученной посредством перехвата телефонного трафика при помощи анализатора

протоколов tcpdump в простой файл, дающая возможность прослушивания с любого плейера компьютера. Данная утилита дает возможность преобразовывать голосовой трафик, отправленный из IP-телефонов Cisco и который был сжат кодеком G.711.

Несмотря на частые случаи, атаку типа перехват данных не так легко реализовать. Атакующий должен располагаться данными об адресах шлюзов, абонентских пунктов и алгоритмах сжатия, используемых в VoIP-телефонии. В случае отсутствия такой информации, ему сложно будет настроить свое программное обеспечение для перехвата данных, или время анализа об объеме перехваченной информации превысит все пределы.

Отказ в обслуживании. При высокой загруженности сети, по которой отправляются оцифрованные информации, случаются искажения или даже пропажа части передаваемой голосовых сообщений. Поэтому, в случае если на сервер отправляются огромное количество «шумовых» пакетов, то это может привести к выходу из строя компонентов IP-телефонии, то есть приведет к атаке типа «отказ в обслуживании». Одним из методов предотвращения такой атаки является использование резервирования полосы пропускания, посредством применения современных протоколов, к примеру, как RSVP.

Подмена номера. В простой телефонии для связи с абонентом необходимо знать его номер, а в IP-телефонии в качестве телефонного номера абонента выступает его IP-адрес. И поэтому, могут быть ситуации, когда злоумышленник посредством подмены адреса, может выдать себя за требуемого вами абонента. Или же он может подделать адрес, выдавая себя за узел у которого есть доступ ко всем приложениям и сервисам, осуществляющие аутентификацию требований на основе проверки адресов. Для подделки используется IP-адрес из числа адресов применяемых внутри сети, или же одобренный внешний, к которому есть доверие и доступ к ресурсам системы. Так как аутентификация основывается на проверке адресов, указание любого адреса источника является решением проблемы для хакера. Указание в качестве адреса, адрес внутреннего узла, который находится за маршрутизатором или брандмауэром, приведет к наиболее хорошему эффекту. При недостаточно хорошей реализации механизмов аутентификации, есть возможность разрушения фильтров на фильтрующих маршрутизаторах.

Именно из-за этого обеспечение хорошей аутентификации крайне необходимо. Фильтрация пакетов, поступающих извне, считается необходимой мерой защиты. Атаки обнаруживаются системой Cisco Secure IDS, а сами фильтры устанавливаются в маршрутизаторах периметра.

Обеспечение безопасности

Выбор правильной топологии. Для инфраструктуры VoIP не стоит применять такие устройства как концентраторы, так как они намного облегчают атакующим перехват данных. Также, необходимо как следует разграничить информационное течение между оцифрованным голосом и обычными данными, поскольку они проходят по одной кабельной системе и сетевому оборудованию. Данная операция может быть выполнена при помощи

VLAN. Серверы, которые участвуют при построении IP-телефонии следует устанавливать в отдельных сетевых сегментах, защищенные при помощи дополнительно встроенных средств (межсетевых экранов, систем обнаружения атак, систем аутентификации и так далее).

Физическая безопасность. Хорошо было бы запретить несанкционированный доступ пользователей к сетевым устройствам, и по мере возможности оборудования не предназначенные для абонентов установить в специальных серверных комнатах. Такие действия позволят предотвратить неразрешенное подключение ПК атакующего. Также необходимо временами проверять наличие неразрешенно подключенных к сети оборудований. Такие устройства определяются по-разному, к примеру наличием сканеров (Internet Scanner, Nessus), которые распознают есть ли в сети «чужие» устройства.

Контроль доступа. Данный метод считается простым способом защиты инфраструктуры и контроля MAC-адресов. Запретите доступ к шлюзам и другим устройствам для IP-телефонов с неизвестными MAC-адресами. Это даст возможность исключить неразрешенный доступ «чужих» телефонов, которые могли бы прослушать ваши разговоры или совершать звонки за ваш счет. Узлы сети нужно настроить так, чтобы они могли предотвратить попытки неразрешенного подключения к ним.

VLAN. Технология виртуальных локальных сетей (VLAN) позволяет безопасное разграничение физической сети на несколько отдельных участков, которые работают независимо друг от друга. В IP-телефонии данная технология применяется для разделения друг от друга передачи голоса и передачи обычных данных.

Шифрование. Шифрование необходимо применять и между IP-телефоном и шлюзом. Это даст возможность обеспечить безопасность всего пути, по которой двигаются голосовые данные из одного конца в другой.

Межсетевой экран. Для защиты корпоративной сети обычно применяют МЭ, которые могут использоваться и для инфраструктуры VoIP. Для этого необходимо просто добавить некоторые правила, которые учитывают топологию сети, месторасположение установленных элементов и так далее.

Для обеспечения безопасности элементов IP-телефонии можно применить два вида межсетевых экранов. Первый тип – корпоративный, который устанавливается на выходе корпоративной сети и осуществляет защиту всех ее ресурсов. Второй тип – персональный, который защищает только один отдельный узел, на котором может быть установлен абонентский пункт, шлюз или диспетчер. Также некоторые ОС (Linux или Windows 2000) имеют в своем составе встроенные персональные МЭ, что дает возможность применять их для повышения уровня защиты инфраструктуры VoIP.

Разносторонность и обширность темы все-таки не дают возможности подробнее изучить обеспечение безопасности IP-телефонии. Те моменты, которые мне удалось описать, показывают что VoIP уязвима и по отношению к ней могут быть использованы такие же методы атаки, которые известны для обычной телефонии и IP-сетей.

2.4 Методы криптографической защиты информации

Началом для любой системы защиты является криптография. Криптографией называется набор способов защиты информационной взаимосвязи, вызванными злоумышленником таких действий как отклонение от нормального штатного протекания взаимодействий, основанных на алгоритмах преобразования данных. Также, криптография считается важным моментом в механизмах аутентификации, целостности и конфиденциальности. Под аутентификацией понимается способ подтверждения личности получателя или отправителя сообщений. Целостность предполагает сохранение данных в начальном виде, а при конфиденциальности никто кроме отправителя или получателя не смогут понять зашифрованную информацию. Криптографическая конструкция представляется в виде алгоритма (математической функции) и секретной величины (ключа). При этом если в ключе больше битов, то он считается менее уязвимым.

В системах обеспечения защиты информации используются три главных метода криптографической защиты:

-симметричное шифрование;

-ассиметричное шифрование;

-односторонние хэш-функции.

На базе этих трех видов шифрования построены все методы технологии аутентификации, целостности и конфиденциальности информации.

При симметричном алгоритме шифрования требуется, чтобы оба участника секретной переписки имели доступ к одинаковому ключу. Необходимость этого заключается в том, что тот, кто отправляет зашифровывает информацию этим ключом, а получатель может расшифровать только данным ключом. Следовательно, создается проблема отправки ключа безопасно. В симметричном алгоритме шифрования применяются ключи не самой большой длины и шифруются огромные размеры информации. Системы с симметричными ключами используются в следующем порядке:

С защитой формируется, осуществляется распространение и сохраняется шифрованный ключ. Для получения секретного текста, отправитель применяет симметричный алгоритм шифрования вместе с секретным ключом. Дальше процесс передачи зашифрованного текста. Симметричный секретный ключ передается только по защищенным каналам. Имеющимся у себя алгоритмом симметричного шифрования и секретным ключом, получатель восстанавливает исходный текст.

DES (Data Encryption Standard) – наиболее широко известный шифр симметричного алгоритма шифрования.

Работа стандарта DES заключается в следующем. Цифровые данные делятся на блоки с длиной 64 бита, и после по блокам шифруются. Блоки делятся на правую часть и левую. Первый этап шифрования заключается в том, что правая часть записывается вместо левой части, а сумма по модулю 2 правой

и левой частей записываются вместо правой. Второй этап представляет собой схему, где происходят замены по битам и перестановки. Ключ DES состоит из 64 бита (длина), 56 битов, из которых являются случайными, 8 битов служебные, которые применяются для контроля ключа.

Рисунок 2.5 – Схема распределения ключей при симметричном шифровании

У шифра DES имеется два режима работы: Electronic Code Book (ECB) и Cipher Block Chaining (CBC). Режим CBC не похож на другие обычные режимы, так в нем перед каждым шифрованием нового блока, к нему используется операция «исключающее ИЛИ» с передним блоком. Модификация Triple DES применяется в тех случаях когда надежность алгоритма DES недостаточна. Выбирая три независимых друг от друга ключа, можно осуществить простое перешифрование: доступный текст в начале шифруется первым ключом, далее шифрованный текст – на втором, и только потом данные выделенные после второго шага зашифровывается на третьем ключе.

International Data Encryption Algorithm (IDEA) – шифр, имеющий 128 бит длину ключа. Данный стандарт, выпущенный в 1990 году, не уступает DES ни по скорости, ни по стойкости к анализу.

Шифры RC2 и RC4 созданы основателем предприятия RSA Data Security – Роном Рейвестом. Данные шифры применяют ключи разнообразной длины, в продуктах для экспорта они заменяют DES. RC2 – 64-битовый блочный шифр, а RC4 – поточный шифр. Эффективность этих шифров не должна быть ниже чем у блочного шифра Data Encryption Standard, по задумке разработчиков.

У всех систем с открытым шифрованием имеются свои недостатки. В первую очередь, к надежности канала уделяется огромное внимание, так как по нему передается ключ от отправителя ко второму участнику зашифрованных переговоров [8].

Для того чтобы решить проблему симметричного шифрования применяются системы с ассиметричным шифрованием. Алгоритм ассиметричного шифрования разработан Диффи и Хеллманом и основан на открытых ключах.

Данные системы отличаются присутствием у каждого пользователя двух ключей: открытого и секретного. Открытый ключ может передаваться всем абонентам, участвующим в секретном переговоре. В результате этого, находим решения двух проблем: необходимость секретной доставки ключа отпадает; квадратичная зависимость количества ключей от количества пользователей тоже не является обязательным – для n-го числа пользователей необходимо 2n число ключей.

Шифр RSA – первый шифр, который был осуществлен на основе ассиметричного шифрования. Шифр RSA считается популярным и самым известным среди других ассиметричных шифров. Математическое утверждение RSA: нахождение делителей огромного натурального числа, которые являются произведением двух простых – очень сложная процедура. По известному открытому ключу нелегко найти личный ключ, парный ему. Изученный со всех сторон, шифр RSA, определен как самый устойчивый при необходимой длине ключей.

DSS – шифр, использующий ассиметричное шифрование. Стандарт Digital Signature Standard был признан правительством США, применяется длина ключа от 512 до 1024 битов. Данный стандарт используется для создания цифровой подписи, но не для закрытия данных. DSS не так широко распространен, так как в нем найдены некоторые уязвимости в защите.

Рисунок 2.6 – Схема распределения ключей при ассиметричном шифровании

В структуре симметричного шифрования ключи шифрования и дешифрования одинаковы. В ассиметричном шифровании ключи не совпадают: ключ шифрования – открытый, ключ дешифрования – засекреченный, собственный. На рисунках 2.5 и 2.6 показаны схемы распределения ключей для симметричного и ассиметричного систем шифрования. Секретные ключи доставляются только по засекреченным каналам, а по открытым каналам доставляются открытые ключи.

Безопасная хэш-функция – это функция, которая является легко рассчитываемой, но ее обратное восстановление сложно реализуемо. Входящие

данные проходят через хэш-функцию (математическую функцию) и на выходе мы получаем определенную последовательность битов. Данная последовательность битов называется «хэш» - результат обработки информации и этот процесс не подлежит восстановлению.

Хэш-функция может принимать сообщения любого объема и на выходе реализует сообщения хэш фиксированной длины.

В приложениях, которые связаны с аутентификацией и управлением ключами, применяются технологии шифрования. К примеру, алгоритм шифрования Диффи-Хеллмана дает возможность создать один общий секретный ключ обоим сторонам, при том, что данные доставляются по незащищенному каналу, и этот ключ будет известен только им двум. После данный ключ будет применяться для шифрования сообщений с использованием алгоритма секретного ключа. Алгоритм Диффи-Хеллмана применяется для сохранения конфиденциальности информации, но для аутентификации не применяется. Для аутентификации используется цифровая подпись.

Электронная цифровая подпись (ЭЦП) – последовательность символов, которая была выделена в итоге криптографической защиты электронной информации. Электронная цифровая подпись прибавляется к блоку данных и дает возможность принимающей стороне проверить адресата, целость материала и защититься от фальшивости. ЭЦП используется в роли собственноручной подписи.

Сообщение, передающееся по каналу передачи, состоит из документа и цифровой подписи. Цифровая подпись расшифровывается получателем с помощью общего ключа, так как она шифруется частным ключом. Затем, на приемной стороне получаем расшифрованный хэш. На вход функции, которая применялась передающей стороной, отправляется текст сообщения. Целость материала и личность адресата считается доказанной, в том случае, если на выходе получится хэш, полученный в сообщении.

Сертификат – документ, подтверждающий согласование открытого ключа с информацией, который распознает владельца ключа. Сертификат содержит в себе всю информацию о владельце, об открытом ключе.

2.5 Технология аутентификации

Определение пользователя и оконечных устройств, их местоположения с дальнейшей авторизацией называется аутентификацией. Самым простым видом аутентификации является применение паролей, но их приходится часто применять чтобы поддержать безопасность. Способы применения одноразовых паролей используются очень широко. Отдельно можно выделить способы аутентификации по протоколу S/Key или с помощью специализированных аппаратов (token password authentication).

Система одноразовых паролей S/Key – это система формирования одноразовых паролей на основе стандартов MD4 и MD5. Данная система предназначена для предотвращения атаки, когда злоумышленник распознает идентификатор пользователя, подслушивает канал и использует данные для неразрешенного доступа.

Система S/Key базируется на технологии клиент-сервер, где клиентом выступает ПК, а сервером – сервер аутентификации. Для начала, систему небходимо настроить на общую парольную фазу. Клиент приступает к обмену S/Key, далее серверу передается пакет активации, в свою очередь, сервер передает порядковый номер и случайное число, называемое «зерном» (seed). Затем, клиент формирует одноразовые пароли.

После формирования, пароль необходимо проверить. Чтобы осуществить проверку, клиент отправляет одноразовый пароль серверу, который его проверяет. Для проверки, система через хэш-функцию одноразово пропускает полученный пароль. Если в результате осуществленных процессов, пароль одинаков с предыдущим, хранящимся в документе, то аутентификацию можно считать положительным.

Две схемы осуществления аутентификации с помощью устройств:

-схема запрос-ответ;

-схема аутентификации с синхронизацией по времени.

Схема запрос-ответ предполагает подключение пользователя к серверу аутентификации, который запрашивает ввод персонального идентификационного номера (PIN) или пользовательского идентификатора (user ID). После того, как пользователь отправит PIN или user ID, сервер делает «запрос» (передает «зерно»). Данное число пользователем вводится в аппаратное средство, представляющее из себя некую карточку, в котором количество запроса шифруется при помощи ключа. Результат осуществленной операции показывается на экране. Пользователь передает его на сервер аутентификации. На сервере аутентификации происходит подсчет этих результатов самостоятельно, с применением пользовательских баз данных, в котором хранятся ключи. Клиент сам подсчитывает этот результат. После получения ответа от клиента, сервер сравнивает его со своими вычислениями. Пользователь получает доступ к сети только в том случае, если результат окажется положительным. В ином случае, доступ не предоставляется.

При применении второй схемы, с синхронизацией по времени, на устройстве пользователя и на сервере используется засекреченный алгоритм, он распознает пароли и заменяет их на новые через синхронизированные промежутки времени. Подключение к серверу аутентификации пользователем происходит после ввода кода доступа. Затем пользователь вводит в карточное устройство свой персональный идентификационный номер, в результате чего на экране отображается одноразовый пароль. Данный пароль и передается на сервер. Результат сравнения паролей сервером, решит получение доступа к сети или его непредоставление.

2.5.1 Протокол PPP

PPP (Point-to-Point Protocol) – стандарт, который осуществляет отправку пакетов по последовательным каналам.

Аутентификация, базирующаяся на стандарте PPP – это известный инструмент упаковки, многократно используемое в глобальных сетях. Он состоит из трех основных элементов:

-способ упаковки дейтаграмм в последовательных линиях;

-протокол Link Control Protocol (LCP), применяемый для установки, конфигурации и проверки связи;

-семейство протоколов Network Control Protocols (NCP), которые используются для установления и конфигурации разных стандартов в сетевом уровне.

В протоколе PPP имеются два способа аутентификации: протоколами EAP и CHAP. Протокол EAP – единый протокол аутентификации PPP, поддерживающий различные идентификационные конструкции. Аутентификация осуществляется после соответствия с LCP и до соответствия с IP Control Protocol, посредством которых выполняется обмен IP-адресами. Данный вид аутентификации происходит в автоматизированном режиме и нет необходимости какого-либо вмешательства пользователя. Протокол CHAP предполагает наивысший уровень обеспечения безопасности, так как не отправляет пароль по каналу связи PPP.

2.5.2 Протокол TACACS

TACACS (Terminal Access Controller Access Control System) – базирующийся на стандартах UDP, обычный протокол регулирования доступом. Данный протокол основан на технологии «клиент-сервер», в которой клиентом является NAS, а сервером TACACS+ является «демон» (операция, осуществляемая на аппарате UNIX или NT). Основным и главным элементом TACACS+ считается AAA (Authentication, Authorization, Accounting) – разделение аутентификации, авторизации и учета. Данный процесс дает возможности обмена идентификационными данными различной длины и состава, а также применять для клиентов любые идентификационные конструкции, такие как PPP PAP, PPP CHAP, карты устройств и Kerberos (рисунок 2.6).

По умолчанию аутентификация не считается обязательной. Она остается в роли опции, конфигурация которой происходит при необходимости.

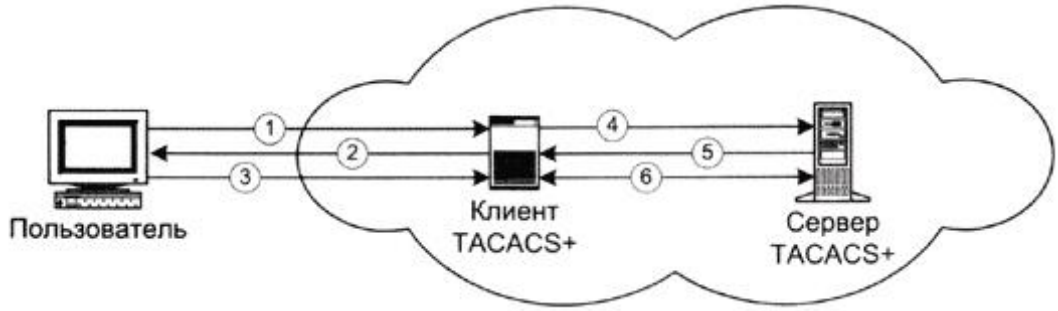


Рисунок 2.7 - Взаимодействие между пользователем и системой TACACS+

Авторизация – способ выделения действий, разрешенные данному пользователю. Обычно процесс аутентификации происходит раньше, но это необязательно. При осуществлении запроса авторизации разрешается указание о невыполнении процесса аутентификации (то есть, личность пользователя не доказана). В таком случае, ответственный за авторизацию личность, должен сам решить, пропускать этого пользователя или нет. Процесс авторизации может осуществляться на разных уровнях, к примеру, когда пользователь только вошел в сеть и пытается открыть интерфейс изображений или при попытке применения протокола IP поверх протокола PPP. В таких ситуациях, демон сервера может предоставить услуги, но в течении ограниченного времени.

Учет – процесс, осуществляющийся самым последним. Он предполагает запись всех действий пользователя. Учет в системе TACACS+ может выполнять две функции: применяется для выставления счетов и он может служить в роли аппарата по обеспечению безопасности. У системы TACACS+ есть три типа учетных записей:

-запись «старт» показывает начало запуска услуги;

-запись «стоп» указывает на окончание услуги;

-запись «обновление» считается промежуточным и говорит о том, что предоставление услуги все еще продолжается.

Учетные записи TACACS+ включают в себя все данные, необходимые в процессе авторизации, а также данные о начале и завершении, информацию о применении средств.

Транзакции осуществляемые между клиентом и сервером распознаются только по известному им «секрету», которые не отправляются по каналу связи. Данный секрет внедряется вручную на сервере и на клиенте. TACACS+ можно расположить к шифрованию всего трафика, передаваемому между клиентом и демоном сервера.

2.5.3 Протокол RADIUS

Протокол RADIUS (Remote Authentication in Dial-In User Service) – протокол аутентификации серверного доступа и учета.

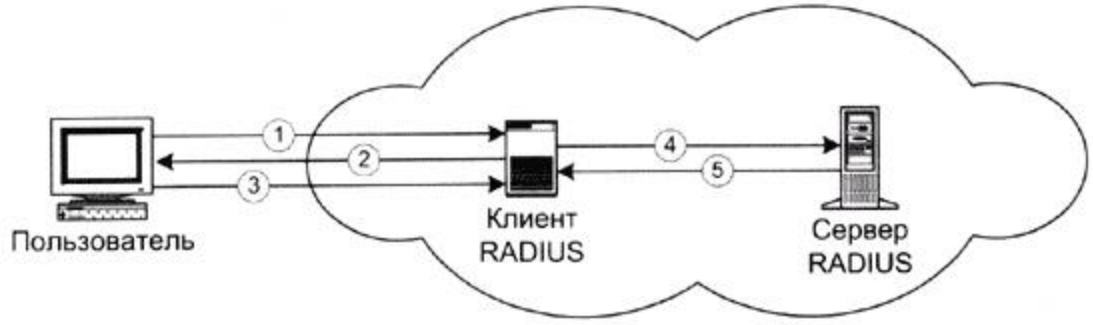


Рисунок 2.8 - Взаимодействие между пользователем и системой RADIUS

Осуществление связи между NAS и сервером RADIUS основывается на базе протокола UDP. Можно утверждать, что данный протокол никак не относится к подключению. Все операции, связанные с доступом, передачей данных осуществляются аппаратными оборудованиями, работающими под протоколом RADIUS, но не самим протоколом.

В протоколе RADIUS также работает технология «клиент-сервер», где клиентом является NAS, а сервером является «демон». Клиент отправляет серверам пользовательские данные и в дальнейшем действует по их указаниям. Серверы принимают запросы полученные от пользователей, осуществляют распознавание пользователей, а после передают их клиенту, для дальнейшего обслуживания пользователей. Сервер RADIUS выступает в роли клиента-посредника для распознающих серверов другого типа.

2.6 Построение Site-to-site VPN на Cisco ASA

VPN (Virtual Private Network) – частная виртуальная сеть. Технология VPN предполагает подключение удаленных пользователей через общедоступные сети к локальным сетям по защищенным каналам связи.

В качестве удаленных пользователей выступают:

-работники, которые работают в предприятиях с разделенной инфраструктурой, то есть компании, у которых может быть несколько точек, магазинов, офисов; которые расположены в разных районах города или области;

-работники, у которых работа напрямую связана с командировками, но им необходимо иметь доступ к локальной сети компании.

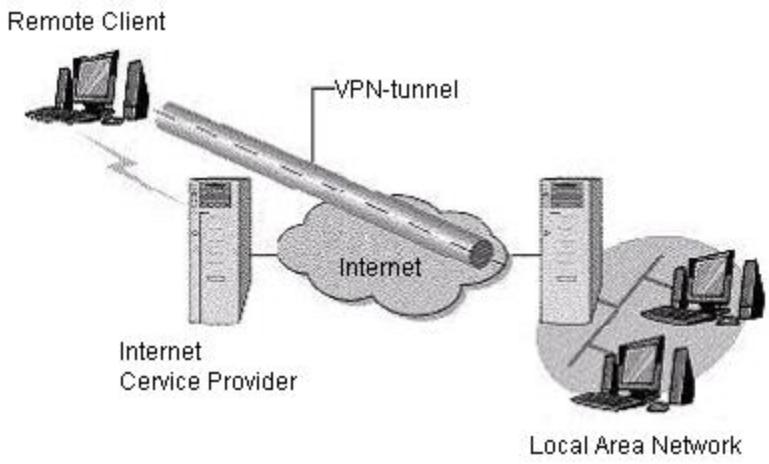


Рисунок 2.9 - Структурная схема VPN для удаленных пользователей

Технология VPN обеспечивает безопасность передачи данных по общедоступным сетям с помощью их шифрования.

Для организации сети VPN нужно:

-канал доступа для центрального офиса, каждого подразделения или пользователя. Это может быть как выделенная, так и коммутируемая линия;

-оборудование узла доступа в центральном офисе (VPN-сервер), оборудование доступа для каждого подразделения или пользователя (VPN-клиент).

Основной функцией VPN является защита трафика. Такая задача очень сложна на криптографическом уровне защиты. Для этого, во-первых, необходимо иметь надежную криптографию, которая бы гарантировала защиту от прослушания, обладать надежной системой защиты управления ключами, защита от атак, а также проверка работоспособности пользователя на данный момент. Во-вторых, нужно обеспечить масштабируемость конкретной VPN. Самыми успешно применяемыми в этом являются VPN-агенты, которые осуществляют защиту трафика на всех видах оборудования – рабочих станциях, серверах, или шлюзах.

У VPN есть отличительная черта, она обычно может различать отдельные компьютеры, но не самих пользователей. Но иногда, необходимо чтобы она могла отличить отдельных приложений и пользователей. Пользователь обязан воспринять одинаковую совокупность настроек программы вне зависимости от того, за каким компьютером он сидит. Необходимые для этого все данные содержатся в пользовательском электронном устройстве, дискете, на флешке и так далее. Если предприятие применяет специальные серверы доступа, то VPN должна уметь работать совместно с такой системой, и она не должна подключать к системе пользователей, которые не прошли авторизацию.

VPN образовывает непроницаемые каналы сверх открытых сетей. В обычной жизни предприятиям необходимо, чтобы работники имели доступ из VPN в открытую сеть и Интернет. Межсетевой экран (МЭ) осуществляет контроль в критичных точках контакта с открытой сетью. Формулировка: сетью VPN обеспечиваются функции МЭ в каждой области, где присутствует

ее агент. Межсетевой экран, который контролируется из центра безопасности, и VPN считаются взаимодополняемыми системами, они решают две связанные задачи:

-использует открытые сети в качестве канала дешевой связи (VPN);

-обеспечивает защиту от атак, при работе с открытой информацией содержащихся в открытых сетях (межсетевой экран).

VPN гарантирует защиту информации, которая передается, но не может осуществить ее защиту на отправном конечном компьютере. Такая задача решается специальными средствами:

-системами криптозащиты данных;

-системами защиты от неразрешенного доступа к оборудованию;

-антивирусных систем и тому подобное.

Туннелирование (tunneling), или инкапсуляция (encapsulation) – метод передачи полезных данных посредством промежуточной сети. В качестве информации могут быть пакеты другого протокола. При способе инкапсуляции кадр отправляется не в виде сгенерированной узлом отправителя, а ему присваивается дополнительный заголовок, в котором содержится информация о маршруте, адресе терминатора туннеля и инициатора туннеля, которые позволяют проходить через Интернет инкапсулированным пакетам. Передача пакетов осуществляется терминатором туннеля, на конце пути после деинкапсуляции. Данный процесс, который включает в себя инкапсуляцию и дальнейшую передачу пакетов, и называется туннелированием. Туннелем называется путь передвижения передаваемых инкапсулированных пакетов.

Работа VPN основана на протоколе Point-to-Point Protocol (PPP). Этот протокол создан для передачи данных по телефонным сетям и выделенным соединениям «точка-точка» - xDSL, он также может работать с многоканальными соединениями – ISDN, X.25 и Frame Relay. Расширение пропускной способности в PPP достигается посредством подключения нескольких параллельных каналов MultiLink Protocol (MP). Протокол PPP проводит инкапсуляцию пакетов IP, IPX и NetBIOS в кадры PPP и осуществляет их передачу по выделенным каналам «точка-точка». Используется данный протокол маршрутизаторами, которые соединены посредством выделенных каналов, или клиентом, соединенным удаленным подключением.

Одним из методов защиты данных в сетях IP-телефонии является применение шифрованных туннелей VPN. Организация соединения в виртуальной частной сети (VPN) происходит по каналу типа точка-точка, которая по-другому называется туннелем. Туннель обычно создается в общедоступной сети Интернет, где сеть незащищена. Связь типа точка-точка говорит о том, что соединение устанавливается между двумя компьютерами, называемыми peers.

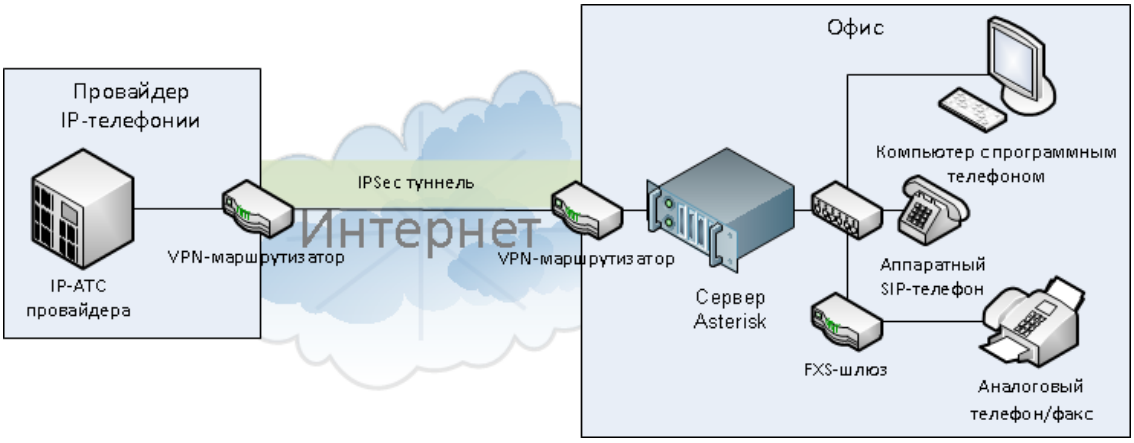


Рисунок 2.10 - Схема работы IP-телефонии через VPN-туннель

Виртуальная частная сеть по сравнению с другими способами удаленного доступа имеет некоторые экономические преимущества. Надобность в применении модемов исключается, так как у пользователя есть возможность без коммутируемого соединения обратиться к корпоративной сети. Организация удаленного доступа без выделенных линий тоже является одним из преимуществ.

Пример построения сети между двумя офисами – центрального и филиала с помощью логического соединения (туннеля) можно рассмотреть в многофункциональной программе – Cisco Packet Tracer.

В качестве примера рассмотрела организацию сети между двумя офисами и мне необходимо организовать удаленный доступ из локальной сети центрального офиса на филиал. Необходимость осуществить защиту трафика по сети Интернет является одним из главных моих задач.

Мы будем настраивать наши два межсетевых экрана для организации постоянного безопасного туннеля VPN с применением набора протоколов IPSecurity (IPSec). Они передаются по межсетевому протоколу IP. Организация VPN типа Site-to-site предполагает объеденение двух сторон.

Процесс построения сети можно разделить на две фазы. Первая фаза – две стороны по протоколу IKE согласовывают параметры технологического соединения; если они аутентифицируются, то поднимается защищенный ISAKMP Tunnel, по которому обе стороны будут договариваться об основном IPSec туннеле. Вторая фаза предполагает заключение соглашения о параметрах IPSec туннеля. После поднимается сам туннель, по которому будут двигаться пользовательские данные в зашифрованном виде.

Более подробно данный пример будет описан в третьей главе.

3 Модель организации обеспечения безопасности в IP-телефонии на примере Site-to-site VPN

Как уже было упомянуто во второй главе, одним из методов защиты данных в сетях IP-телефонии является применение шифрованных туннелей VPN. Организация соединения в виртуальной частной сети (VPN) происходит по каналу типа точка-точка, которая по-другому называется туннелем. Туннель обычно создается в общедоступной сети Интернет, где сеть незащищена. Связь типа точка-точка говорит о том, что соединение устанавливается между двумя компьютерами, называемыми peers.

В качестве примера организации соединения в виртуальной частной сети я рассмотрела организацию сети между двумя офисами и мне необходимо осуществить удаленный доступ из локальной сети центрального офиса на филиал. Необходимость обеспечения защиты трафика по сети Интернет является одним из главных моих задач.

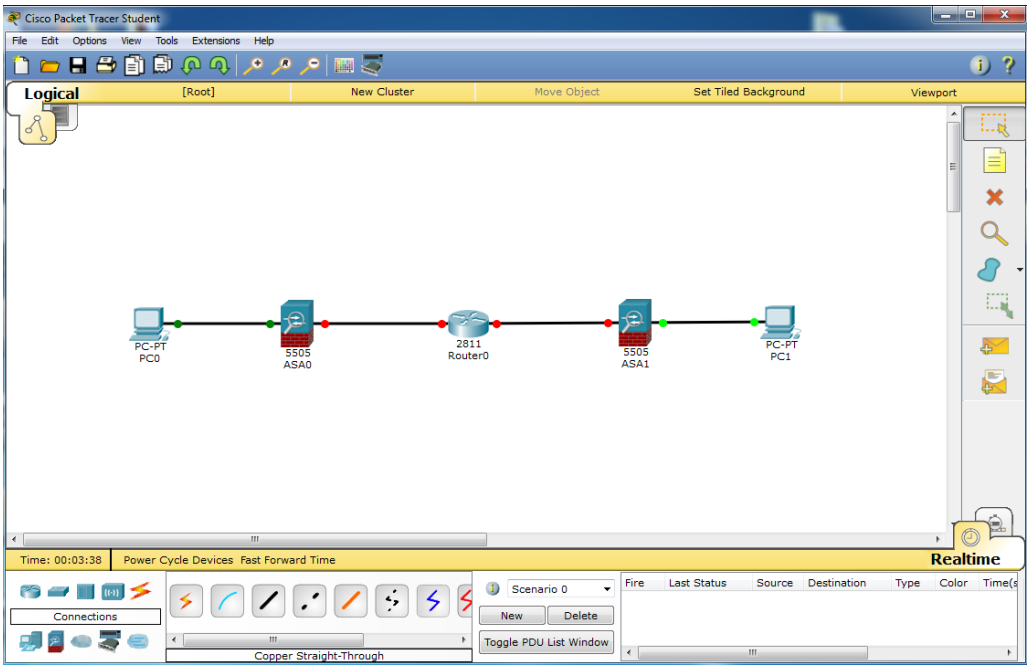


Рисунок 3.1 – Схема Site-to-site VPN на Cisco ASA

Мы будем настраивать наши два межсетевых экрана для организации постоянного безопасного туннеля VPN с применением набора протоколов IPSecurity (IPSec). Организация VPN типа Site-to-site предполагает объеденение двух сторон.

Cisco ASA является аппаратным межсетевым экраном с инспектированием сессий с сохранением состояния (stateful inspection). ASA умеет работать в двух режимах: routed (режим маршрутизатора, по умолчанию) и transparent (прозрачный межсетевой экран, когда ASA работает как бридж с фильтрацией) [9].

Прежде чем приступить к работе, с помощью команды show run, проверяем настройки конфигурации Cisco ASA 1 (рисунок 3.2) и видим, что fastEthernet 0/0 настроен на Vlan 2, которой является outside интерфейсом.

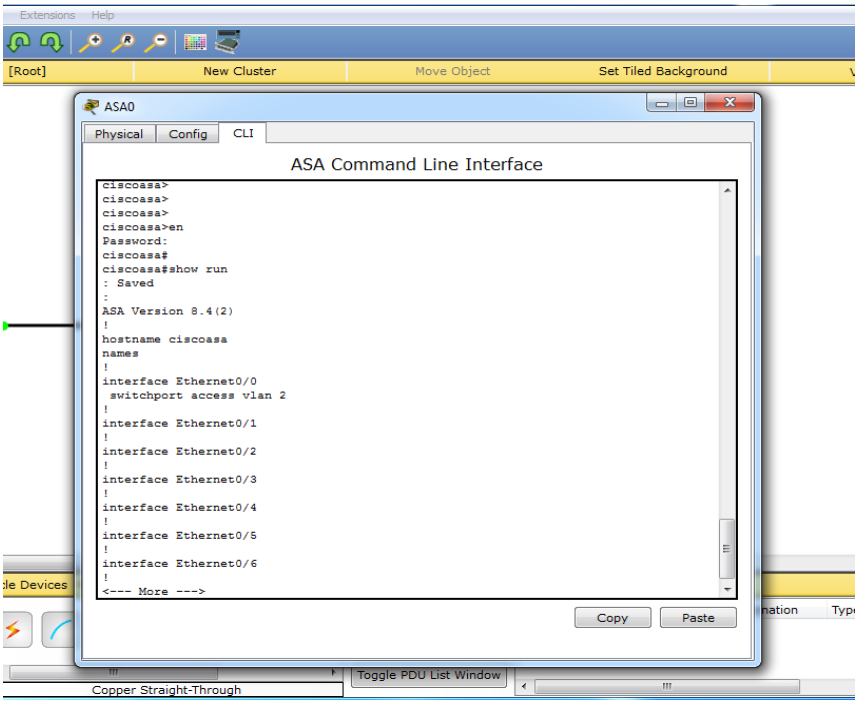


Рисунок 3.2 – Настройки конфигурации Cisco ASA 1

Проведем следующие операции в настройках Cisco ASA 1. Задаем IP-адрес 210.210.1.2 на outside интерфейс, с маской 255.255.255.252. Далее добавляем default маршрут на Cisco ASA 1, через outside интерфейс с помощью IP-адреса интернет провайдера 210.210.210.1.1. Проведение инспектирования трафика (stateful inspection) является обязательным моментом и она производится определением класса map, далее создаем policy map и с указанием созданным нами map, инспектируем icmp трафик. Такую же работу проделываем на Cisco ASA 2.

Затем настраиваем роутер провайдера (рисунок 3.3). На интерфейсе fastEthernet 0/0 настроим IP-адрес 210.210.1.1 с маской 255.255.255.252, а на интерфейсе fastEthernet 0/1 IP-адрес будет 210.210.2.1 с маской 255.255.255.252.

Далее организуем VPN. Данный процесс можно разделить на две фазы. Первая фаза – две стороны по протоколу IKE согласовывают параметры технологического соединения; если они аутентифицируются, то поднимается защищенный ISAKMP Tunnel, по которому обе стороны будут договариваться об основном IPSec туннеле. Вторая фаза предполагает заключение соглашения о параметрах IPSec туннеля. После поднимается сам туннель, по которому будут двигаться пользовательские данные в зашифрованном виде.

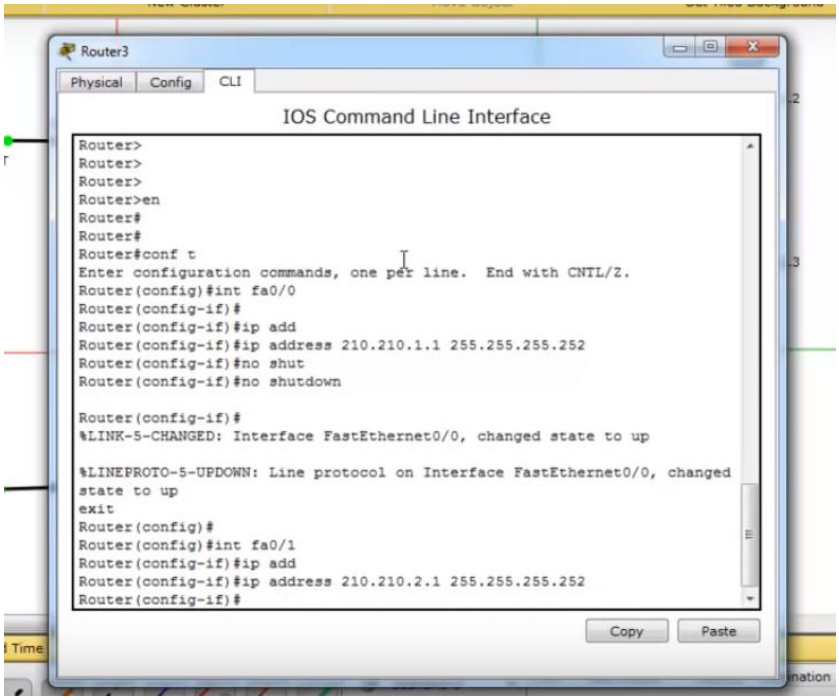


Рисунок 3.3 – Настройка роутера провайдера

Как уже знаем, сначала выполняем все операции на Cisco ASA 1, затем выполняем эту же работу на Cisco ASA 2.

Настройка первой фазы. Включаем на outside интерфейсе протокол IKE, с помощью команды crypto ikev1 enable outside. Затем настраиваем политику crypto ikev1 policy 1 и прописываем следующие параметры: encr 3des, hash md5. Далее проводим аутентификацию командой authentication pre-share key и определяем алгоритм Диффи-Хеллмана group 2. После команда exit и приступаем к следующему уровню (рисунок 3.4).

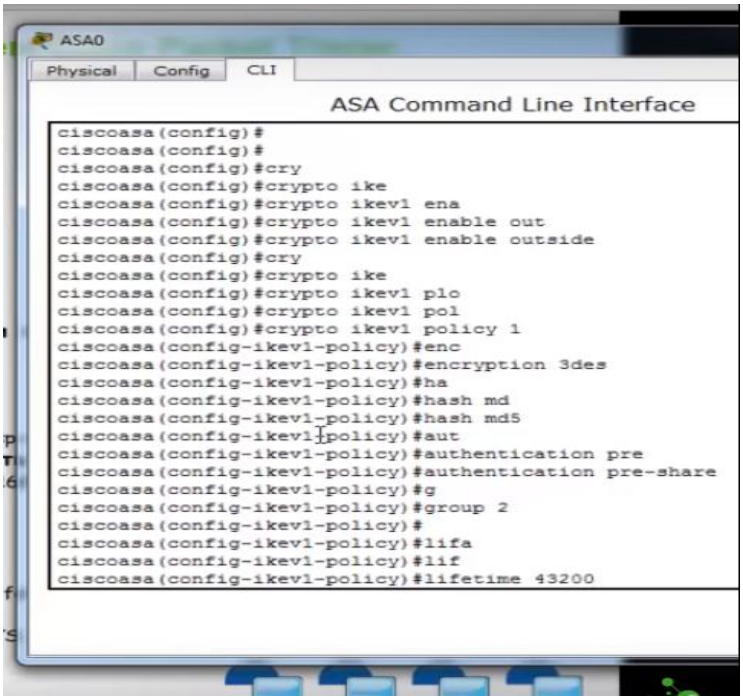


Рисунок 3.4 – Настройка первой фазы

Настройка ключа аутентификации и пира. Она осуществляется посредством tunnel-group (на нем пишутся параметры для аутентификации на первой фазе IPsec) с указанием IP-адреса Cisco ASA 2 210.210.2.2, в качестве типа аутентификации применяем type ipsec-l2l. Зададим атрибуты IPSec tunnel-group 210.210.2.2 ipsec-attributes, а именно ikev1 pre-shared-key cisco.

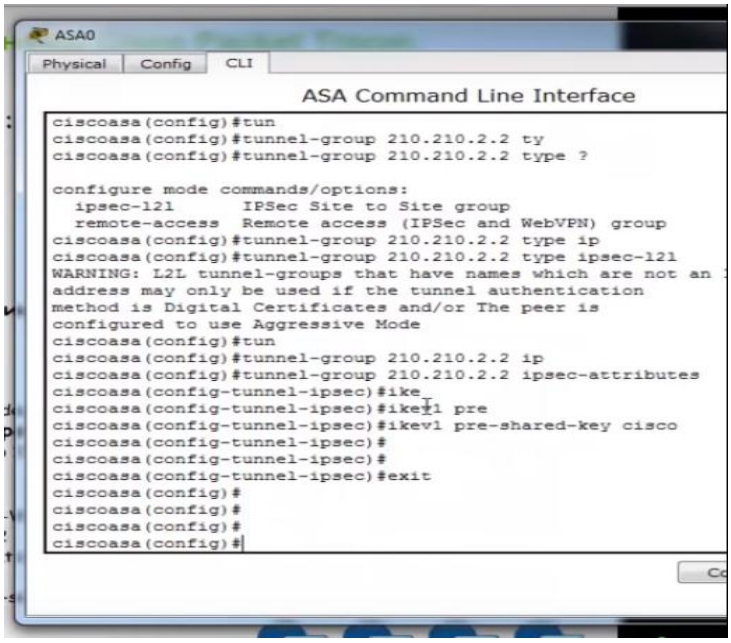


Рисунок 3.5 - Настройка ключа аутентификации и пира

Вторая фаза. Задаем параметры для второй фазы crypto ipsec ikev1 transform-set TS (набор преобразований, необходимый для защиты наших данных) esp-3des (метод шифрования) esp-md5-hmac (алгоритм хэширования).

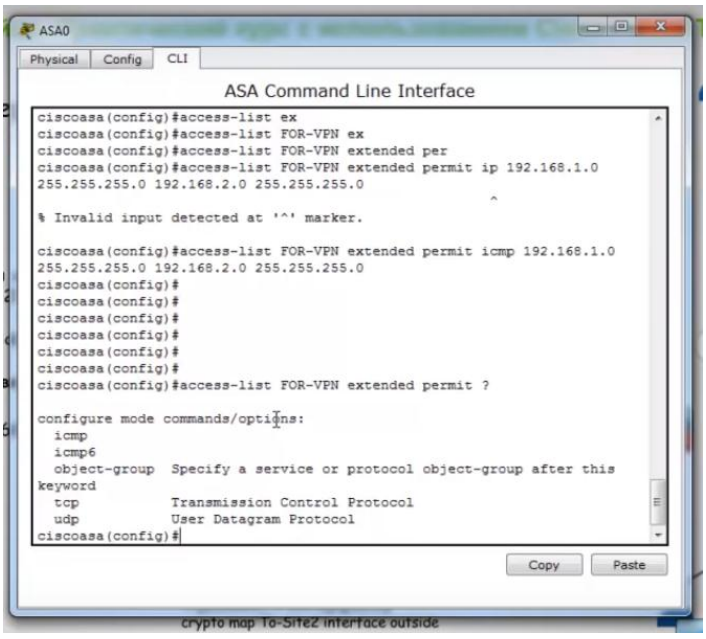


Рисунок 3.6 – Определение трафика, необходимого для шифрования

Определяем, какой трафик хотим пропускать через VPN-туннель, для этого создаем Access List командой access-list FOR-VPN extended permit icmp 192.168.1.0 255.255.255.0 (source – источник) 192.168.2.0 255.255.255.0 (destination – место назначения).

Создание криптокарты. Оно совмещает ранее заданные конфигурации ISAKMP и IPSec. Пишем crypto map, задаем имя To-Site2 даем номер 1, указываем что надо использовать трафик Access List-a FOR-VPN. Далее указываем пир peer 210.210.2.2 – IP-адрес Cisco ASA 2 (филиала). И указываем в секундах lifetime туннеля по умолчанию 86400 (время жизни ключа).

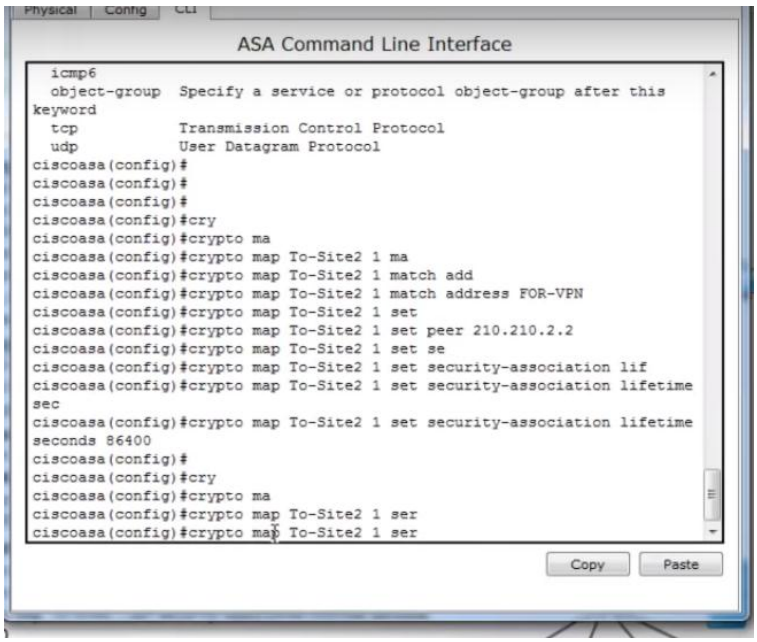


Рисунок 3.7 – Создание криптокарты

Привязка криптокарты к outside интерфейсу. Осуществляем данную операцию с помощью команды crypto map To-Site2 interface outside.

После выполненных всех манипуляций выполняем проверку командой ping (рисунок 3.8). К примеру, IP-адрес ПК 192.168.2.5, находящейся за вторым Cisco ASA.

Из данного ниже рисунка 3.8, мы видим что проверка прошла успешно и организация Site-to-site VPN между двумя Cisco ASA положительна.

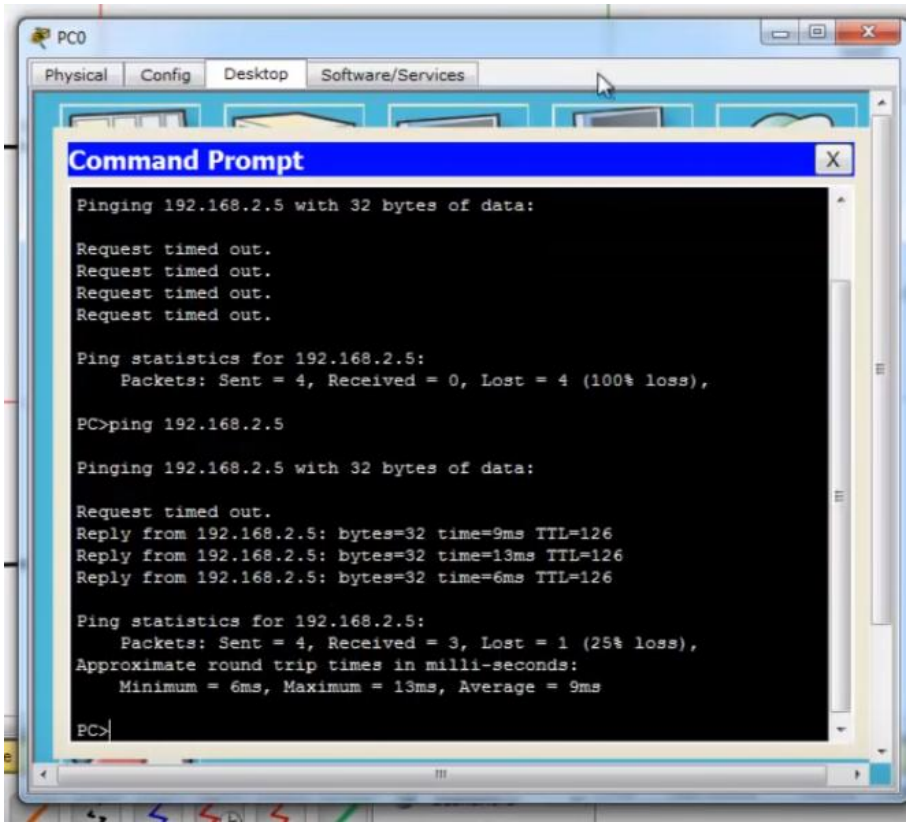


Рисунок 3.8 – Проверка сети при помощи команды ping

ЗАКЛЮЧЕНИЕ

В дипломной работе был дан анализ обеспечения безопасности соединения в сетях IP-телефонии. Были проанализированы возможности протоколов IP-телефонии с точки зрения обеспечения безопасности, проанализирован вариант защиты информации в канале за счет использования технологии виртуальных частных сетей на базе протокола IPSec. Как результат, была выработана рекомендация по обеспечению безопасности соединения в сетях IP- телефонии и представлен сценарий установления безопасного VoIP-соединения. В работе были смоделированы и рассмотрены различные атаки на сеть IP-телефонии и предложены варианты защиты. Выработанные алгоритмы в целом удовлетворяют защите от смоделированных ситуаций.

Приведенный анализ указывает на необходимость внедрения эффективных механизмов защиты соединений в сетях IP-телефонии для того, чтобы провайдер оставался конкурентоспособным на растущем рынке телематических услуг. Для чего в рамках обеспечения безопасности с точки зрения несанкционированного доступа рекомендуется использование протокола RADIUS, а с точки зрения обеспечения конфиденциальности и целостности информации, передаваемой в каналах сети IP-телефонии технологии IPSec.

Перечень принятых сокращений, терминов

IP - протокол межсетевого взаимодействия
VoIP - Voice over Internet Protocol
ПК – персональный компьютер
SIP - Session Initiation Protocol (протокол установления сеанса)
ТфОП - Телефонная сеть Общего Пользования
АТС - *Автоматическая Телефонная Станция*
PSTN - Public switched telephone network (телефонная сеть общего пользования)
GSM - Global System for Mobile Communications (глобальный стандарт цифровой мобильной сотовой связи с разделением каналов по времени и частоте)
ITU - *International Telecommunication Union (*Международный союз электросвязи)
MGCP - Media Gateway Control Protocol (протокол, предназначенный для управления шлюзами между системами традиционной телефонии (PSTN) и VoIP-системами)
MCU - Multipoint Control Unit
HTTP – HyperText Transfer Protocol (протокол передачи гипертекста)
АЦП – аналогово-цифровой преобразователь
ЦАП – цифро-аналоговый преобразователь
PIN - Personal Identification Number (персональный идентификационный номер)
TDM - Time Division Multiplexing (технология аналогового или цифрового мультиплексирования)
DHCP - Dynamic Host Configuration Protocol (протокол динамической настройки узла)
УАТС - *учрежденческая автоматическая телефонная станция*
МЭ – межсетевые экраны
ISDN - Integrated Services Digital Network (цифровая сеть с интеграцией служб)
RTCP - Real-Time Transport Control Protocol (протокол управления передачей в реальном времени)
PGP - *Pretty Good Privacy (*компьютерная программа, также библиотека функций, позволяющая выполнять операции шифрования и цифровой подписи сообщений)
IETF - *Internet Engineering Task Force (*Инженерный совет Интернета)
IPSec - IP Security
VLAN - Virtual Local Area Network (виртуальная локальная сеть)
ОС – операционная система
DES - Data Encryption Standard (алгоритм для симметричного шифрования)
RSA - аббревиатура от фамилий Rivest, Shamir и Adleman (криптографический алгоритм с открытым ключом)
LCP - *Link Control Protocol*
PPP - Point-to-Point Protocol

EAP - Extensible Authentication Protocol (расширяемый протокол аутентификации)
CHAP - Challenge Handshake Authentication Protocol (протокол аутентификации с косвенным согласованием)
TACACS - Terminal Access Controller Access Control System (сеансовый протокол, использовавшийся на серверах доступа ARPANET)
AAA - Authentication, Authorization, Accounting
RADIUS - Remote Authentication in Dial-In User Service (протокол для реализации аутентификации, авторизации и сбора сведений)
VPN - *Virtual Private Network* (виртуальная частная сеть)
ISAKMP Tunnel - Ассоциация Безопасности Интернета и Протокол Управления Ключами
IKE - Internet Key Exchange

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Б. С. Гольдштейн, А. В. Пинчук, А. Л. Суховицкий. IP-телефония. - СПб.: БХВ-Петербург, 2014. —336 с.

2 Баскаков И. В., Пролетарский А. В., Мельников С. А., Федотов Р. А., IP-телефония в компьютерных сетях: Учебное пособие. – Москва, 2008.

3 http://lib.kstu.kz:8300/tb/books/Korporativn@ie_seti_svyazi/plain/teory/2.1.html

4 https://www.intuit.ru/studies/courses/8/8/lecture/253

5 Амато Вито. Основы организации сетей Cisco, том 1. - М.: Издательский дом "Вильяме", 2004. – 512 с.

6 http://lib.kstu.kz:8300/tb/books/Korporativn@ie_seti_svyazi/plain/teory/7.1.html

7 Смит Ричард Э. Аутентификация: от паролей до открытых ключей. - М.: издательский дом «Вильямс», 2002.

8 https://helpiks.org/9-29992.html https://www.intuit.ru/studies/professional_skill_improvements/1216/courses/8/lecture/253?page=4

9 https://habr.com/ru/post/80414/

10 http://88.204.198.13.metro.online.kz/index.php/2015-05-20-06-43-19/poleznye-instruktsii-i-nastrojki/item/11-obespechenie-bezopasnosti-ip-telefonii

11 http://portal.kazntu.kz/files/publicate/2015-10-22-elbib_60.pdf

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

РЕЦЕНЗИЯ

на дипломную работу

Касымхан Назерке Ерханкызы

5В071900 – Радиотехника, электроника и телекоммуникации

На тему: Анализ обеспечения безопасности в IP-телефонии

Выполнено:
а) графическая часть на _____ листах
б) пояснительная записка на _____ страницах

ЗАМЕЧАНИЯ К РАБОТЕ

В современное время стремительными темпами идет развитие сети Интернет, различных сетей на базе IP протокола, а также сетей IP-телефонии. IP-телефония, являясь преемником двух технологий, – простой телефонии с коммутацией каналов и IP-сетей с коммутацией пакетов, – вобрала в себя и комплекс проблем, относящиеся к обеспечению безопасности. Проблема обеспечения безопасности при передаче любой информации всегда является актуальной.

Дипломная работа Касымхан Н. посвящена анализу обеспечения безопасности в IP-телефонии. В первой главе рассматриваются общие вопросы, связанные с интеграцией традиционной телефонии и сетей передачи данных, с основными понятиями об IP-телефонии, стандартами и видами угроз для системы голосовой связи.

Во второй главе дается анализ угроз, слабые места в IP-телефонии, методы обеспечения безопасности для различных стандартов: H323, SIP и MGCP; способы отражения этих угроз, а также методы криптографической защиты информации. Анализируются протоколы авторизации и аутентификации, протокол частной виртуальной сети, которые обеспечивают безопасность передачи данных по общедоступным сетям.

Третья глава посвящена моделированию организации обеспечения безопасности в IP-телефонии на примере Site-to-site VPN с помощью программы Cisco Packet Tracer.

Оценка работы

Считаю, что дипломная работа выполнена на 95/A/«отлично», а дипломант, Касымхан Назерке Ерханкызы, заслуживает присвоения академической степени бакалавра техники и технологии по специальности 5В071900-Радиотехника, электроника и телекоммуникации.

Рецензент
канд. техн. наук, проф. профессор АУЭС
_____ А.С. Байкенов
_____ 2019г.

Ф КазНИТУ 706-17. Рецензия

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

ОТЗЫВ

НАУЧНОГО РУКОВОДИТЕЛЯ

на дипломную работу

Касымхан Назерке Ерханкызы

5В071900 – Радиотехника, электроника и телекоммуникации

Тема: Анализ обеспечения безопасности в IP-телефонии

В данной дипломной работе рассматриваются вопросы обеспечения безопасности в IP-телефонии, которые всегда будут актуальными в связи с тем, что передача голосовой информации идет через ненадежные IP-сети.

Первая глава посвящена общим вопросам, связанным с появлением IP-телефонии, ее стандартам, методам передачи голосовой информации, а также угрозам, которые возникают при передаче голоса по публичным сетям.

Вторая глава непосредственно дает анализ всем угрозам передачи информации в IP-телефонии и методам обеспечения безопасности.

В третьей главе в программе Cisco Packet Tracer показана модель организации сети между двумя офисами, где в качестве примера рассматривается технология обеспечения безопасности –Site-to-site VPN.

Считаю, что дипломная работа выполнена на 95/A/«отлично», а дипломант, Касымхан Назерке Ерханкызы, заслуживает присвоения академической степени бакалавра техники и технологии по специальности 5В071900-Радиотехника, электроника и телекоммуникации.

Научный руководитель
маг-р техн. наук, лектор
_____ Г.М. Байкенова
"6" 05 2019г.

Ф КазНИТУ 706-16. Отзыв научного руководителя

Протокол анализа Отчета подобия

заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Касымхан Назерке

Название: Анализ обеспечения безопасности в IP-телефонии

Координатор: Гулжан Байкенова

Коэффициент подобия 1:10,5

Коэффициент подобия 2:0,4

Тревога:4

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

 обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;
 обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;
 обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

....
....
....
....
....

13.05.2019 .... Зав. каф. Б.-КТ

Дата   Подпись заведующего кафедрой / начальника структурного подразделения

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Касымхан Назерке

Название: Анализ обеспечения безопасности в IP-телефонии

Координатор:Гулжан Байкенова

Коэффициент подобия 1:10,5

Коэффициент подобия 2:0,4

Тревога:4

После анализа Отчета подобия констатирую следующее:

☐ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.