AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ

MAGİSTRATURA MƏRKƏZİ

Əlyazma hüququnda

İBADULLAYEV YUNIS FAIQ OĞLU

“ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В УПРАВЛЕНИИ БИЗНЕСОМ” mövzusunda

MAGISTR DISSERTASIYASI

İqtisasın şifri və adı — 06 05 09 “İnformasiya sistemləri”

İxtisaslaşma — İqtisadi informasiya sistemləri

Elmi rəhbər:
dos. E.H.Hüseynov

Magistr programının rəhbəri:
dos. H.M. Bayramov

Kafedra müdiri — dos. H.M. Bayramov

BAKI - 2016

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы. Информация на сегодняшний день рассматривается как один из основных ресурсов развития общества, а информационные системы и технологии - как средство повышения производительности и эффективности работы людей.

Цель диссертации.Основная цель диссертации-выявление главной идеи, связанной с использованием информационных систем и технологий, на примере IP-телефонии, а также ее применение в бизнесе.

Научная новизна.Предложено получение финансовой выгоды приудобном разворачивания IP-телефонии в бизнесе, а также применение и построение правильных и надежных коммуникаций для получения качества речи.

Практическая ценность работы.

- сокращение затрат на междугороднюю и международную связь;

-снижение издержек на построение, эксплуатацию, модернизацию и техническую поддержку телекоммуникационной инфраструктуры;

-возможность построения единой, многофункциональной, отказоустойчивой телекоммуникационной платформы на базе корпоративной IP-сети;

-сокращение расходов на каналы связи за счет повышения возможности использования современных приложений, использующих преимущества интеграции голоса, видео и данных в рамках единой телекоммуникационной инфраструктуры;

- обеспечение максимально эффективного использования каналов связи для совместной передачи голосового трафика, трафика данных и трафика видео приложений.

Наиболее широко информационные системы и технологии используются в производственной, управленческой и финансовой деятельности, хотя начались подвижки в сознании людей, занятых и в других сферах, относительно необходимости их внедрения и активного применения. Это

определило угол зрения, под которым будут рассмотрены основные области их применения. Главное внимание уделяется рассмотрению информационных систем и технологий с позиций использования их возможностей для повышения эффективности труда работников информационной сферы производства и поддержки принятия решений в различных организациях. В современных условиях быстрое наращивание объемов бизнеса компании за счет расширения филиальной сети, слияний и поглощений приводит к тому, что телекоммуникационная инфраструктура предприятий представляет собой множество разнородных УАТС и телефонных систем. Это делает актуальной задачу по переходу на унифицированные коммуникации.

Внедрение IP-телефонии в компании, как неотъемлемой части унифицированных коммуникаций, повышает эффективность ведения бизнеса и позволяет осуществлять многие операции, невозможные в случае применения традиционной телефонии.

Диссертационная работа состоит из трех глав.

Впервая главе рассматриваются основные характеристики современных информационных систем.Вторая глава посвящена информационно-логическим моделям и архитектуре систем IP-0телефонии на примере банка. Третья глава включает техническую инфраструктуру IP-телефонии.Работа изложена на98 страницахкомпьютерного набора.

ГЛАВА I. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ СОВРЕМЕННЫ ИНФОРМАЦИОННЫХ СИСТЕМ

1.1.Понятие информационной системы

Понятие "информационная технология" тесно связано с понятием "информационная система".Существует множество определений понятия "система". Например, система рассматривается как совокупность взаимосвязанных элементов (объектов), объединённых для реализации общей цели, обособленная от окружающей среды, взаимодействующая с ней как целое и проявляющая при этом системные свойства. В более широком смысле толкование системы даёт терминологический словарь по автоматике, информатике и вычислительной технике: система – это совокупность взаимосвязанных объектов, подчинённых определённой единой цели с учётом условий окружающей среды . Упорядоченная совокупность элементов системы и их связей между собой представляет структуру системы.

Проанализировав понятие структуры и существующие определения системы, можно выделить следующие её основные составляющие: 1) система - это упорядоченная совокупность элементов; 2) элементы системы взаимосвязаны и взаимодействуют в рамках данной системы, являясь её подсистемами; 3) система как целое выполняет установленную ей функцию, которая не может быть сведена к функции отдельного элемента; 4) элементы системы могут взаимодействовать друг с другом в рамках системы, а также самостоятельно с внешней средой и изменять при этом своё содержание или внутреннее строение.

Информационная система (ИС), это среда, составляющими элементами которой являются компьютеры, компьютерные сети, программные продукты, базы данных, люди и т.д. Основная цель информационной системы – организация хранения, обработки и передачи итоговой информации, необходимой для принятия решения. Информационная система представляет собой человеко-компьютерную систему обработки информации.

Информационная технология – это процесс работы с информацией, состоящий из чётко регламентированных правил выполнения операций. Основнаяцель информационной технологии – производство необходимой пользователю информации.Исполнение функций информационной системы невозможно без знанияориентированной на неё информационной технологии.Современная информационная система – это набор информационных технологий, направленных на поддержку жизненного цикла информации и включающих три основные составляющие процесса: обработку данных, управление, управление информацией и управление знаниями.

1.2.Основные задачи информационных систем

Современные информационные системы решают следующие основные задачи.

1. Осуществление поиска, обработки и хранения информации, которая накапливается в течение большого периода времени, имеет большую ценность.ИС предназначены для более быстрой и надёжной обработки информации, чтобы люди не тратили время, чтобы избежать свойственных человеку случайныхошибок, чтобы сэкономить расходы, чтобы сделать жизнь людей более комфортной.

2. Хранение данных разной структуры. Не существует развитой ИС, работающей с одним однородным файлом данных. Более того, разумным требованием к информационной системе является то, чтобы она могла развиваться.Могут появиться новые функции, для выполнения которых требуются дополнительные данные с новой структурой. При этом вся накопленная ранее информация должна остаться сохранной. Теоретически можно решить эту задачупутём использования нескольких файлов внешней памяти, каждый из которыххранит данные с фиксированной структурой. В зависимости от способа организации используемой системы управления файлами эта структура может быть структурой записи файла или поддерживаться отдельной библиотечной функцией, написанной специально

для данной ИС. Известны примеры реальнофункционирующих ИС, в которых хранилище данных планировалось основывать на файлах. В результате развития большинства таких систем в них выделился отдельный компонент, который представляет собой разновидность системы управления базами данных (СУБД).

3. Анализ и прогнозирование потоков информации различных видов и типов, перемещающихся в обществе. Изучаются потоки с целью их минимизации,стандартизации и приспособления для эффективной обработки на вычислительных машинах, а также особенности потоков информации, протекающей через различные каналы распространения информации.

4. Исследование способов представления и хранения информации, созданиеспециальных языков для формального описания информации различной природы, разработка специальных приёмов сжатия и кодирования информации, аннотирования объёмных документов и реферирования их. В рамках этого направления развиваются работы по созданию банков данных большого объёма,хранящих информацию из различных областей знаний в форме, доступной длявычислительных машин.

5. Построение процедур и технических средств для их реализации, с помощью которых можно автоматизировать процесс извлечения информации из документов, не предназначенных для вычислительных машин, а ориентированных на восприятие их человеком.

6. Создание информационно-поисковых систем, способных воспринимать запросы к информационным хранилищам, сформулированные на естественномязыке, а также специальных языках запросов для систем такого типа.

7. Создание сетей хранения, обработки и передачи информации, в составкоторых входят информационные банки данных, терминалы, обрабатывающиецентры и средства связи.Конкретные задачи, которые должны решаться информационной системойзависят от той прикладной области, для которой предназначена система. Области применения информационных

приложений разнообразны: банковское дело,управление производством, медицина, транспорт, образование, юриспруденцияи т.д.

Информационная система определяется следующими свойствами.

1. Структура ИС, её функциональное назначение должны соответствоватьпоставленным целям.

2. ИС предназначена для производства достоверной, надёжной, своевременной и систематизированной информации, основанной на использовании БД,экспертных систем и баз знаний. Так как любая ИС предназначена для сбора,хранения и обработки информации, то в основе любой ИС лежит среда хранения и доступа к данным. Среда должна обеспечивать уровень надёжности хранения и эффективность доступа, которые соответствуют области применения ИС.

3. ИС должна контролироваться людьми, ими пониматься и использоватьсяв соответствии с основными принципами, реализованными в виде стандарта организации на ИС. Интерфейс пользователя ИС должен быть легко понимаем наинтуитивном уровне.

4. Любая информационная система может быть подвергнута анализу, построена и управляема на основе общих принципов построения систем.

5. Любая ИС является динамичной и развивающейся.

1.3.Структура информационной системы

Структуру ИС составляет совокупность отдельных её частей, называемыхподсистемами. Подсистема – это часть системы, выделенная по какому-либопризнаку. Если общую структуру ИС рассматривать как совокупность подсистем независимо от сферы применения, то в этом случае подсистемы называютобеспечивающими.

Среди основных подсистем ИС обычно выделяют информационное, техническое, математическое, программное, лингвистическое, организационное иправовое обеспечение.Назначение подсистемы информационного обеспечения

состоит в своевременном формировании и выдаче достоверной информации для принятия управленческих решений.

Информационное обеспечение – это совокупность единой системы классификации и кодирования информации, унифицированных систем документации,схем информационных потоков, циркулирующих в организации, а также методология построения БД.Система классификации позволяет сгруппировать объекты в определённыеклассы, которые будут характеризоваться рядом общих свойств.Классификаторы представляют собой систематический свод, перечень каких-либо объектов, позволяющий находить каждому их них своё место, и имеют определённое (обычно числовое) обозначение.Классификация объектов – это процедура группировки на качественномуровне, направленная на выделение однородных свойств. Применительно к информации как к объекту классификации выделенные классы называют информационными объектами.

В любой стране разработаны и применяются государственные, отраслевые,региональные классификаторы. Например, классифицированы: отрасли промышленности, оборудование, профессии, единицы измерения, статьи затрат ит.д.Классификатор – это систематизированный свод наименований и кодовклассификационных группировок.

Назначение классификатора:

– систематизация наименований кодируемых объектов;

– однозначная интерпретация одних и тех же объектов в различных задачах;

– возможность обобщения информации по заданной совокупности признаков;

– возможность сопоставления одних и тех же показателей, содержащихся вформах статистической отчётности;

– возможность поиска информации и обмена ею между различными внутрифирменными подразделениями и внешними информационными системами;

– рациональное использование памяти компьютера при размещении кодируемой информации.

Разработаны три метода классификации объектов, которые различаютсяразной стратегией применения классификационных признаков.

1. Иерархический метод классификации.

Учитывая достаточно жёсткую процедуру построения структуры классификации, необходимо перед началом работы определить её цель, т.е. какими свойствами должны обладать объединяемые в классы объекты. Эти свойства принимаются в дальнейшем за признаки классификации.В иерархической системе классификации каждый объект на любом уровнедолжен быть отнесён к одному классу, который характеризуется конкретнымзначением выбранного классификационного признака. Для последующей группировки в каждом новом классе необходимо задать свои классификационныепризнаки и их значения. Таким образом, выбор классификационных признаковбудет зависеть от семантического содержания того класса, для которого необходима группировка на последующем уровне иерархии. Количество уровнейклассификации, соответствующее числу признаков, выбранных в качестве основания деления, характеризует глубину классификации.Достоинства иерархической системы классификации: простота построенияи использование независимых классификационных признаков в различных ветвях иерархической структуры.Недостатки иерархической системы классификации: жёсткая структура, которая приводит к сложности внесения изменений, так как приходится перераспределять все классификационные группировки; невозможность группироватьобъекты по заранее не предусмотренным сочетаниям признаков.

2. Фасетный метод классификации.

В отличие от иерархического позволяет выбирать признаки классификациинезависимо как друг от друга, так и от семантического содержания классифицируемого объекта. Признаки классификации называются

фасетами (facet –рамка). Каждый фасет содержит совокупность однородных значений данногоклассификационного признака. Причём значения в фасете могут располагатьсяв произвольном порядке, хотя предпочтительнее их упорядочение. Схема построения фасетной системы классификации представляется в виде таблицы. Названия столбцов соответствуют выделенным классификационным признакам(фасетам). В каждой клетке таблицы хранится конкретное значение фасета.Процедура классификации состоит в присвоении каждому объекту соответствующих значений из фасетов.Достоинства фасетной системы классификации: возможность созданиябольшой ёмкости классификации, т.е. использования большого числа признаков классификации и их значений для создания группировок; возможность простой модификации всей системы классификации без изменения структуры существующих группировок. Недостатком фасетной системы классификации является сложность её построения, так как необходимо учитывать всё многообразие классификационных признаков.

3. Дескрипторный метод классификации.

Для организации поиска информации, для ведения тезаурусов (словарей)эффективно используется дескрипторная (описательная) система классификации, язык которой приближается к естественному языку описания информационных объектов. Особенно широко она используется в библиотечной системепоиска.Суть дескрипторного метода классификации заключается в следующем:

– отбирается совокупность ключевых слов или словосочетаний, описывающих определённую предметную область или совокупность однородных объектов. Причём среди ключевых слов могут находиться синонимы;

– выбранные ключевые слова и словосочетания подвергаются нормализации, т.е. из совокупности синонимов выбирается один или несколько наиболееупотребимых;

– создаётся словарь дескрипторов, т.е. словарь ключевых слов и словосочетаний, отобранных в результате процедуры нормализации.

– между дескрипторами устанавливаются связи, которые позволяют расширить область поиска информации.

Связи могут быть трёх видов:

– синонимические, указывающие некоторую совокупность ключевых словкак синонимы;

– родовидовые, отражающие включение некоторого класса объектов в более представительный класс;

– ассоциативные, соединяющие дескрипторы, обладающие общими свойствами.

Система кодирования – совокупность правил кодового обозначения объектов.Система кодирования применяется для замены названия объекта на условное обозначение (код) в целях обеспечения удобной и более эффективной обработки информации.Код строится на базе алфавита, состоящего из букв, цифр и других символов. Код характеризуется: длиной – числом позиций в коде и структурой – порядком расположения в коде символов, используемых для обозначения классификационного признака.Процедура присвоения объекту кодового обозначения называется кодированием. Можно выделить две группы методов, используемых в системе кодирования, которые образуют:

– классификационную систему кодирования, ориентированную на проведение предварительной классификации объектов либо на основе иерархическойсистемы, либо на основе фасетной системы;

– регистрационную систему кодирования, не требующую предварительнойклассификации объектов.Классификационное кодирование применяется после проведения классификации объектов. Различают последовательное и параллельное кодирование.Последовательное кодирование используется для иерархической классификационной структуры. Суть метода заключается в следующем: сначала записывается код старшей группировки 1-го уровня, затем код группировки.Параллельное кодирование используется для фасетной системы классификации. Суть метода заключается в следующем: все фасеты кодируются независимо друг от друга; для значений каждого фасета

выделяется определённое количество разрядов кода. Параллельная система кодирования обладает теми жедостоинствами и недостатками, что и фасетная система классификации.Регистрационное кодирование используется для однозначной идентификации объектов и не требует предварительной классификации объектов. Различают порядковую и серийно-порядковую систему.Порядковая система кодирования предполагает последовательную нумерацию объектов числами натурального ряда. Этот порядок может быть случайным или определяться после предварительного упорядочения объектов, например по алфавиту. Этот метод применяется в том случае, когда количество объектов невелико, например кодирование названий факультетов университета,кодирование студентов в учебной группе.Серийно-порядковая система кодирования предусматривает предварительное выделение групп объектов, которые составляют серию, а затем в каждойсерии производится порядковая нумерация объектов. Каждая серия также будетиметь порядковую нумерацию. По своей сути серийно-порядковая система является смешанной: классифицирующей и идентифицирующей. Применяетсятогда, когда количество групп невелико.Унифицированные системы документации создаются на государственном,республиканском, отраслевом и региональном уровнях. Главная цель – этообеспечение сопоставимости показателей различных сфер жизнедеятельностиобщества. Разработаны стандарты, где устанавливаются требования:

– к унифицированным системам документации;

– к унифицированным формам документов различных уровней управления;

– к составу и структуре реквизитов и показателей;

– к порядку внедрения, ведения и регистрации унифицированных форм документов.

Однако, несмотря на существование унифицированной системы документации, при обследовании большинства организаций постоянно выявляется целыйкомплекс типичных недостатков:

– чрезвычайно большой объём документов для ручной обработки;

– одни и те же показатели часто дублируются в разных документах;

– работа с большим количеством документов отвлекает специалистов отрешения непосредственных задач;

– имеются показатели, которые создаются, но не используются, и др.

Поэтому устранение указанных недостатков является одной из задач, стоящих при создании информационного обеспечения.Схемы информационных потоков отражают маршруты движения информации и её объёмы, места возникновения первичной информации и использованиярезультатной информации. За счёт анализа структуры подобных схем можновыработать меры по совершенствованию всей системы управления.Построение схем информационных потоков, позволяющих выявить объёмыинформации и провести её детальный анализ, обеспечивает:

– исключение дублирующей и неиспользуемой информации;

– классификацию и рациональное представление информации.

При этом подробно должны рассматриваться вопросы взаимосвязи движения информации по уровням управления. Следует выявить, какие показателинеобходимы для принятия управленческих решений, а какие нет. К каждомуисполнителю должна поступать только та информация, которая используется.Методология построения баз данных базируется на теоретических основахих проектирования. Для понимания концепции методологии приведём основные её идеи в виде двух последовательно реализуемых на практике этапов:

1-й этап – обследование всех функциональных подразделений организациис целью:

– понять специфику и структуру её деятельности;

– построить схему информационных потоков;

– проанализировать существующую систему документооборота;

– определить информационные объекты и соответствующий состав реквизитов (параметров, характеристик), описывающих их свойства и назначение.2-й этап – построение концептуальной информационно-логической моделиданных для

обследованной на 1-м этапе сферы деятельности. В этой моделидолжны быть установлены и оптимизированы все связи между объектами и ихреквизитами. Информационно-логическая модель является фундаментом, накотором будет создана база данных.Техническое обеспечение ИС – это комплекс технических средств, обеспечивающих работу ИС, соответствующей документации на эти средства и технологические процессы.

В комплекс технических средств входят:

- устройства сбора, накопления, обработки, передачи и вывода информации;
- устройства передачи данных и линий связи;
- эксплуатационные материалы и др.

Документацией оформляются предварительный выбор технических средств,организация их эксплуатации, технологический процесс обработки данных,технологическое оснащение.

Документацию можно условно разделить на три группы:

– общесистемную, включающую государственные и отраслевые стандартыпо техническому обеспечению;

- специализированную, содержащую комплекс методик по всем этапам разработки технического обеспечения;
- нормативно-справочную, используемую при выполнении расчётов по техническому обеспечению.

Математическое и программное обеспечение – это совокупность математических методов, моделей, алгоритмов и программ для реализации целей и задачИС, а также нормального функционирования комплекса технических средств.

К средствам математического обеспечения относятся:

– средства моделирования процессов;

– типовые задачи;

– методы математического программирования, математической статистики,теории массового обслуживания и др.

К средствам программного обеспечения (ПО) относятся:

Общесистемное ПО – это комплекс программ, ориентированный на пользователей и предназначенный для решения типовых задач обработки информации. Они служат для расширения функциональных возможностей компьютеров, контроля и управления процессом обработки данных.Специальное ПО представляет собой совокупность программ, разработанных при создании конкретной ИС. В его состав входят пакеты прикладных программ, реализующие разработанные модели разной степени адекватности, отражающие функционирование реального объекта.Техническая документация на разработку программных средств должна содержать описание задач, задание на алгоритмизацию, экономико-математическую модель задачи, контрольные примеры.Лингвистическое обеспечение (ЛО) – это совокупность языковых средств,обеспечивающих гибкость представления и обработки информации с помощьюИС. Здесь язык выступает не только как средство коммуникаций между элементами деятельности, находящимися на одном уровне, но и обеспечивающимичеловеко-машинное взаимодействие. Обычно ЛО включает языки запросов иотчётов, реализующие человеко-машинное взаимодействие, а также специальные языки определения и управления данными, обеспечивающие адекватностьвнутреннего представления и согласование внутреннего и внешнего представлений. Очевидно, что именно поэтому ЛО в значительной степени зависит отособенностей предметной области: с одной стороны, от требований к полноте иточности передачи информации (смысла), а с другой – от требований к унифицированности языка и простоте его изучения и использования человеком.Организационное обеспечение – это совокупность методов и средств, регламентирующих взаимодействие работников с техническими средствами и между собой в процессе разработки и эксплуатации ИС.

Организационное обеспечение реализует следующие функции:

– анализ существующей системы управления организацией, где будет использоваться ИС, и выявление задач, подлежащих автоматизации;

– подготовку задач к решению на компьютере, включая техническое задание на проектирование ИС и технико-экономическое обоснование её эффективности;

– разработку управленческих решений по составу и структуре организации,методологии решения задач, направленных на повышение эффективности системы управления. Организационное обеспечение создаётся по результатам предпроектного обследования на 1-м этапе построения БД.

Правовое обеспечение – это совокупность правовых норм, определяющихсоздание, юридический статус и функционирование ИС, регламентирующихпорядок получения, преобразования и использования информации.В состав правового обеспечения входят законы, указы, постановления государственных органов власти, приказы, инструкции и другие нормативные документы министерств, ведомств, организаций, местных органов власти. В правовом обеспечении можно выделить общую часть, регулирующую функционирование любой ИС, и локальную часть, регулирующую функционированиеконкретной системы.Правовое обеспечение этапов разработки ИС включает нормативные акты,связанные с договорными отношениями разработчика и заказчика и правовымрегулированием отклонений от договора.Правовое обеспечение этапов функционирования ИС включает:

- статус ИС;
- права, обязанности и ответственность персонала;
- правовые положения отдельных видов процесса управления;
- порядок создания и использования информации и др.

ГЛАВА II. ИНФОРМАЦИОННО-ЛОГИЧЕСКАЯ МОДЕЛЬ И АРХИТЕКТУРА СИСТЕМ IP ТЕЛЕФОНИИ НА ПРИМЕРЕ БАНКА

2.1.Понятие современной системы IP телефонии

Под IP-телефонией подразумевается голосовая связь, которая осуществляется по сетям передачи данных, в частности по IP-сетям (IP — InternetProtocol). На сегодняшний день IP-телефония все больше вытесняет традиционные телефонные сети за счет легкости развертывания, низкой стоимости звонка, простоты конфигурирования, высокого качества связи и сравнительной безопасности соединения.

При осуществлении звонка голосовой сигнал преобразуется в сжатый пакет данных (подробнее этот процесс будет рассмотрен в главах “Импульсно кодовая модуляция” и “Кодеки”). Далее происходит пересылка данных пакетов поверх сетей с коммутацией пакетов, в частности, IP сетей. При достижении пакетами получателя, они декодируются в оригинальные голосовые сигналы. Эти процессы возможны благодаря большому количеству вспомогательных протоколов, часть из которых будет рассмотрена далее.

В данном контексте, протокол передачи данных — некий язык, позволяющий двум абонентам понять друг друга и обеспечить качественную пересылку данных между двумя пунктами.Отличия от традиционной телефонии следующие. В традиционной телефонии установка соединения происходит при помощи телефонной станции и преследует исключительно цель разговора. Здесь голосовые сигналы передаются по телефонным линиям, через выделенное подключение. В случае же IP-телефонии, сжатые пакеты данных поступают в глобальную или локальную сеть с определенным адресом и передаются на основе данного адреса. При этом используется уже IP-адресация, со всеми присущими ей особенностями (такими как маршрутизация). При этом IP-телефония оказывается более дешевым решением как для оператора, так и для абонента. Происходит это благодаря тому, что:

- Традиционные телефонные сети обладают избыточной производительностью, в то время, как IP-телефония использует технологию сжатия голосовых пакетов и позволяет полностью использовать емкость телефонной линии.
- Как правило, на сегодняшний момент доступ в глобальную сеть есть у всех желающих, что позволяет сократить затраты на подключение или совсем исключить их.
- Звонки в локальной сети могут использовать внутренний сервер и происходить без участия внешней АТС.

Вместе с вышеперечисленным, IP-телефония позволяет улучшить качество связи. Достигается это, опять же, благодаря трем основным факторам:

- Телефонные серверы постоянно совершенствуются и алгоритмы их работы становятся более устойчивыми к задержкам или другим проблемам IP-сетей.
- В частных сетях их владельцы обладают полным контролем над ситуацией и могут изменять такие параметры, как ширина полосы пропускания, количество абонентов на одной линии, и, как следствие, величину задержки.
- Сети с коммутацией пакетов развиваются, и ежегодно вводятся новые протоколы и технологии, позволяющие улучшить качество связи (например, протокол резервирования полосы пропускания RSVP).

Благодаря IP-телефонии очень элегантно решается проблема занятой линии, так как переадресация, либо перевод в режим ожидания могут быть осуществлены несколькими командами в конфигурационном файле на АТС.

В настоящее время существует множество различных программ, позволяющих вести телефонные переговоры через Интернет или локальную сеть. Такая возможность уже никого не удивляет, для этого нужны лишь компьютер, подключенный к сети, соответствующая программа и микрофон с наушниками. Конечно, такое решение явно не подходит для организации

телефонии в серьезной фирме (все же подобные средства носят скорее развлекательный характер), однако идея передачи голоса через сеть передачи данных очень заманчива, особенно если фирма имеет множество офисов в разных городах. И в этом случае рано или поздно возникает вопрос о внедрении IP-телефонии.

IP-телефония, по сути, является способом организации телефонной связи с использованием сети передачи данных для передачи голоса.Преимущества такой организации телефонной связи очевидны, и главное из них — существенное снижение затрат на звонки между офисами, расположенными в разных городах. Кроме этого, данный подход позволяет ввести единый номерной план для всей организации, когда не нужно помнить телефонные коды городов, в которых находятся филиалы компании. Ну и конечно, не стоит забывать о внедрении дополнительных сервисов (рис. 2.1).

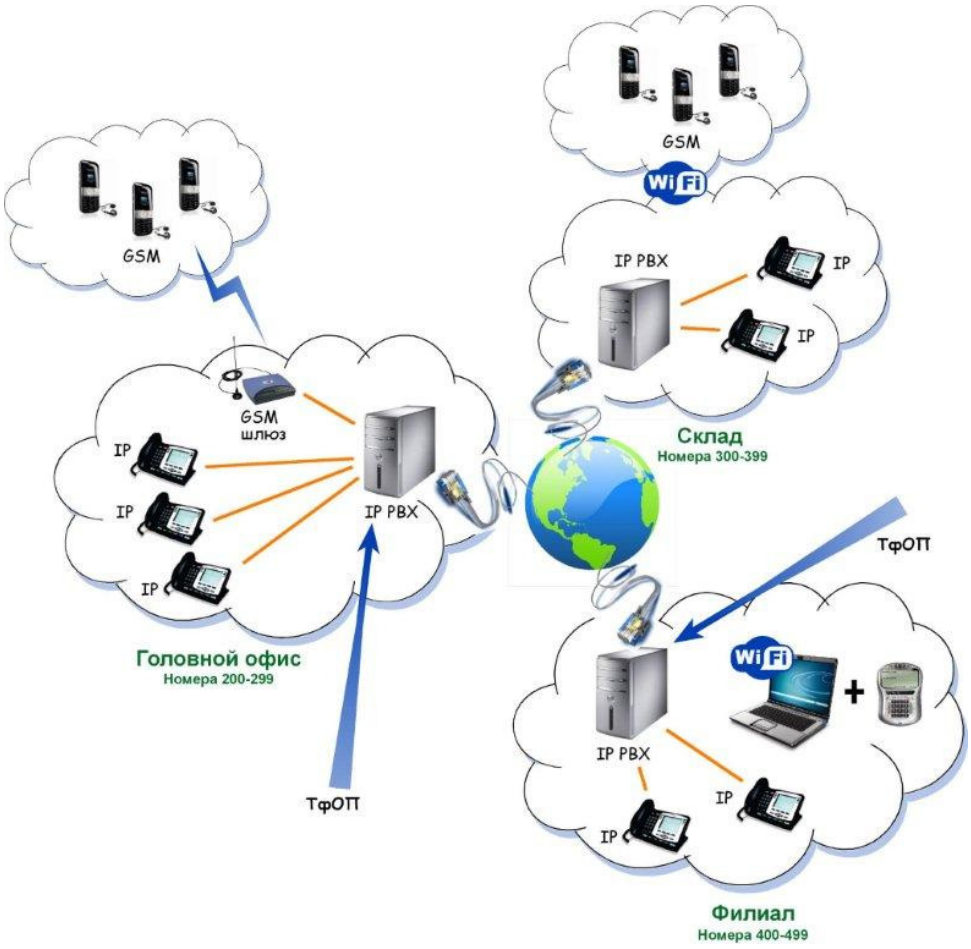

Рис. 2.1. Схема корпоративной IPсети

Корпоративная IP-телефония позволяет объединить уже существующее в организации телефонное оборудование (обычные телефоны, подключенные к УАТС) и специализированные IP-телефоны в одну систему, использующую для передачи голосового трафика сеть передачи данных. Как же организована корпоративная IP-телефония? Как происходит передача голоса, как обеспечивается его быстрое прохождение по сети, как совершается коммутация вызовов? Об этом здесь и пойдет речь. Так как многие фирмы имеют корпоративную сеть передачи данных, построенную с использованием активного сетевого оборудования фирмы CiscoSystems, особое внимание уделено решениям, которые предлагает именно эта компания.

2.2.Использование систем IP телефонии на примере банка. Экономические преимущества корпоративной IP телефонии.

Исследование различных методов и средств представления и управления данными в информационных системах проведем на примере банковской структуры и систем IP телефонии.

На примере представлена сеть банка с основным и резервным ДАТА Центрами, а также с количеством филиалов равным двадцати.

На примере банковской структуры мы можем рассмотреть внедренную систему IP телефонии.

Как указано в графике каждый филиал, а также головные офисы обладают определенным набором IP телефонов. При устойчивых коммуникациях между офисами телефония должна работать стабильно.

Каждый работник оснащается уникальным телефоном и закрепленным за ним уникальным номером телефона. При этом мы получаем следующие возможности:

1. Каждый работник головного офиса и филиалов имеет возможность сделать звонок любому другому сотруднику.

2.Каждый работник головного офиса и филиалов имеет возможность воспользоваться всеми возможностями IP телефонии. К примерупросматривать

и, исходящие и также набранные звонки, иметь доступ к корпоративной директории, пользоваться поиском номеров сотрудников на основе таких факторов как Имя, Фамилия, Должность, Отдел и т.д. Есть возможность запуска любых Java приложений.

3. Контроль доступа осуществляется администраторами, которые могут контролировать “callflow” любого телефона и в любом направлении. К примеру можем закрепить исходящие городские звонки с филиала “А” в филиал “Б”. Можем контролировать возможность исходящих звонков по городу, региону и миру, разрешить или запретить звонки через сеть GSM операторов.

- Кэкономические преимущества корпоративной IP телефонии можно отнести следующие пункты:

-Снижение общей стоимости владения

Уменьшение стоимости наращивания системы и подключения новых площадок.

-Экономия на кабельных системах.

-Сокращение затрат на администрирование.

-Сокращение междугородних расходов.

- Система IP телефонии снабжает нас следующей гибкостью:

-Уменьшение времени добавления пользователей и новых сервисов.

-Повсеместный доступ к сервисам для всех.

- Повышениепроизводительноститруда

-Интегрированные приложения и сервисы для индивидуальных пользователей и рабочих групп.

- К модели систем ip телефонии можно отнести возможности для внедрения дополнительных приложений. К таковымможноотнестиследующие:

-Записьголоса on demand.

-Распознавание голоса – интеграция с телефонной книжкой.

-Информационные сервисы.

-Специфические бизнес приложения.

-Интеграция с телевидением / развлекательными программами.

К экономической выгоде от внедрения систем IP телефонииможно отнести следующие (рис.2.2):

Очевидная экономия:

- Единая сеть (к этому пункту можно отнести: поддержка, кабельные работы, администрирование, перемещения, штат сотрудников)

- Недвижимость (лучшая утилизация места, снижение операционных расходов, гибкость)

- Снижение телефонных расходов (уменьшение пользования городской сети, корпоративный роуминг, удаленная работа, унифицированная система передачи сообщений, аудио-конференции.)

- Небольшой филиал (централизованная обработка звонков, исключение голосовых транков, голос передачи поверх IP, отсутствие отдельной АТС.)

- Отчетности, биллинг, управление расходами (отчетность по телекоммуникациям, по всему предприятию, управление расходами за звонки по предприятию, предсказуемость телефонных счетов)

- Снижение расходов персональных компьютеров (в некоторых случаях IP-телефония может заменить персональный компьютер)

Измеряемое увеличение производительности труда:

- Приложения (конференции, унифицированные сообщения, персональный ассистент, web управление)

- Выгоды, которые трудно подсчитать (удовлетворенность от удобства работы, географическая гибкость, быстрое внедрение приложений, высокая гибкость коммуникаций).

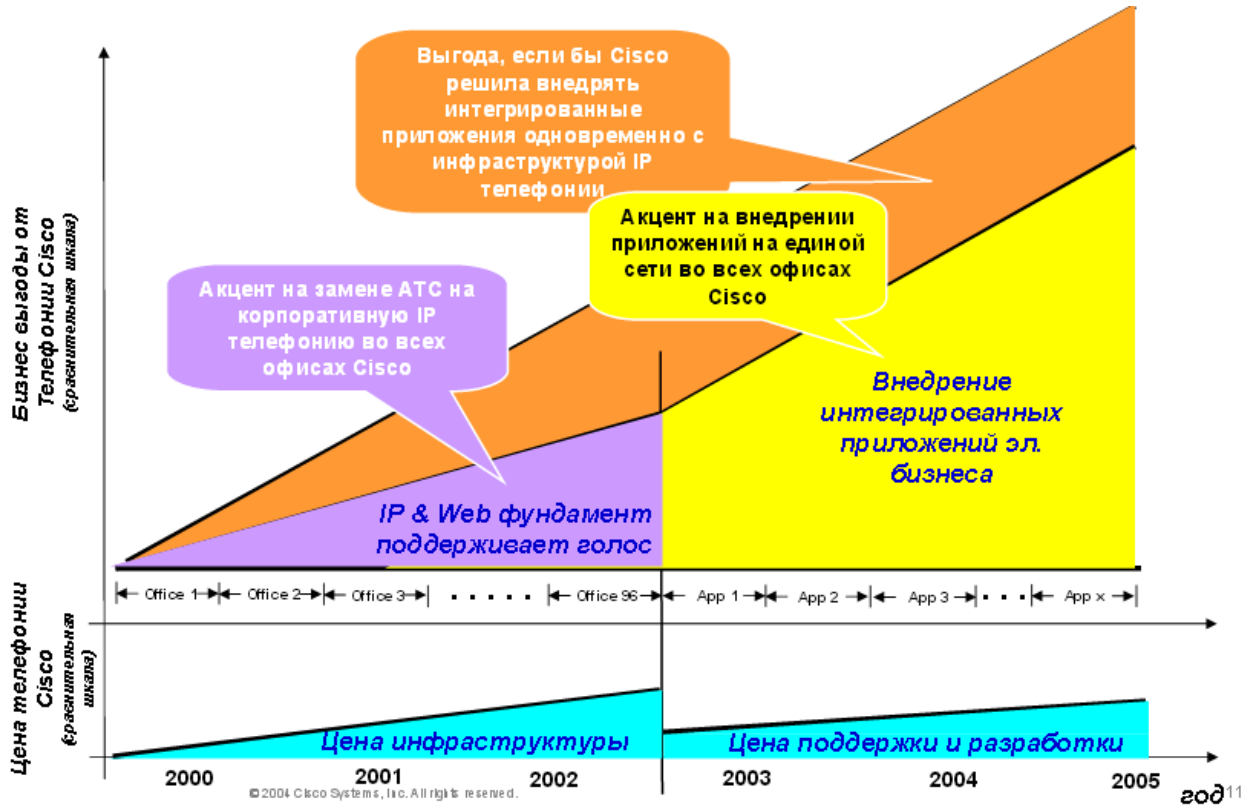

Рис. 2.2. Стратегия Cisco по внедрению IP телефонии

ГЛАВА III. ТЕХНИЧЕСКАЯ ИНФРАСТРУКТУРА IP-ТЕЛЕФОНИИ

3.1. Различные подходы к построению и уровни архитектурыIP-телефонии

Архитектура технологии VoiceoverIP 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.

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.

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 и др. 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.

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.

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 рис. 3.1. представлена архитектура сети на базе рекомендации H.323. Основными устройствами сети являются: терминал (Terminal), шлюз (Gateway), привратник (Gatekeeper) и устройство управления конференциями (MultipointControlUnit- MCU).

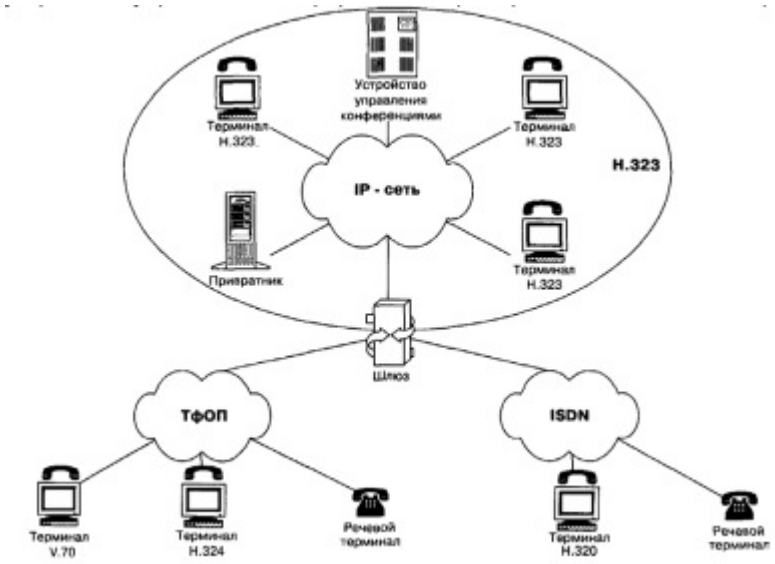

Рис. 3.1. Архитектура сети H.323

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.

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 ITUH.246.

Сеть, построенная в соответствии с рекомендацией H.323, имеет зонную архитектуру (рис. 3.2). 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.

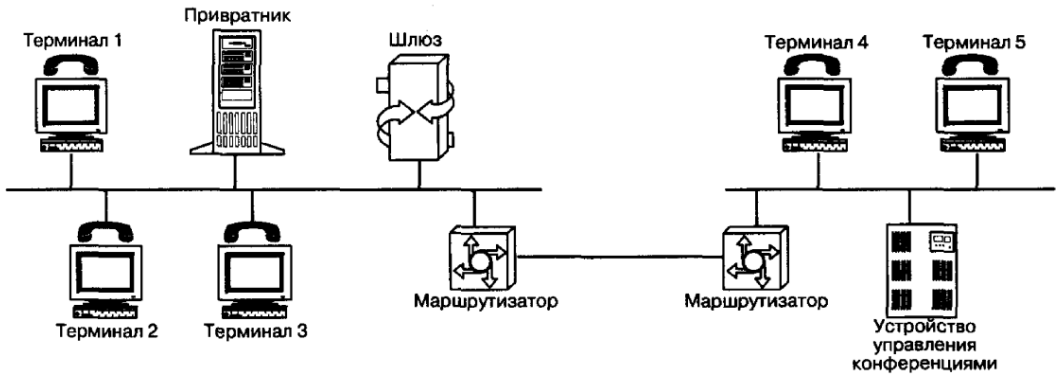

Рис. 3.2. Зона сети H.323

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.

Рекомендация H.323 предусматривает три вида конференции (рис. 3.3): 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.

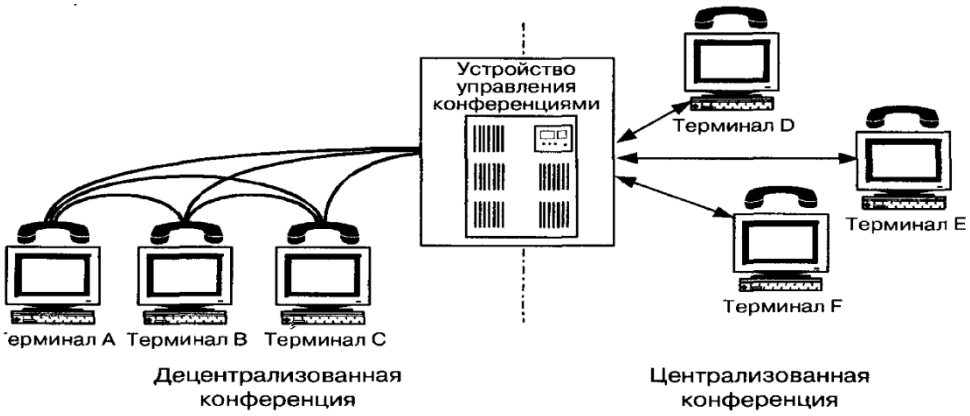

Рис. 3.3. Виды конференции в сетях H.323

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 (IPmulticasting). 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.

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.

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-сервервыполняетследующиеключевыефункции:

– 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.

Сложность протокола H.323 демонстрирует рис.3.4., 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.

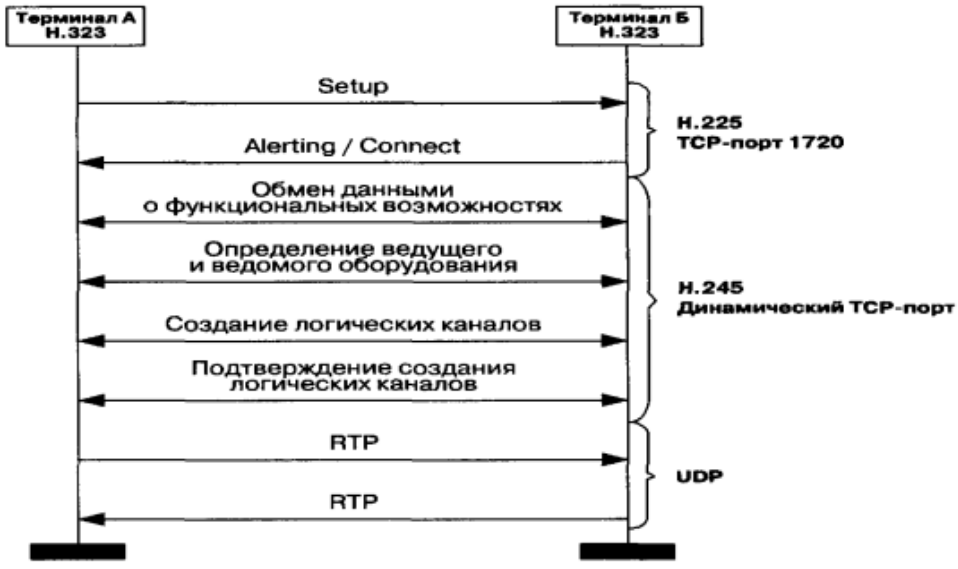

Рис.3.4. Упрощённый сценарий установления соединения в сети H.323

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 ITUH.450.X.

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.

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.

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.

Перейдем непосредственно к архитектуре сетей, базирующихся на протоколе SIP (рис. 3.5.).

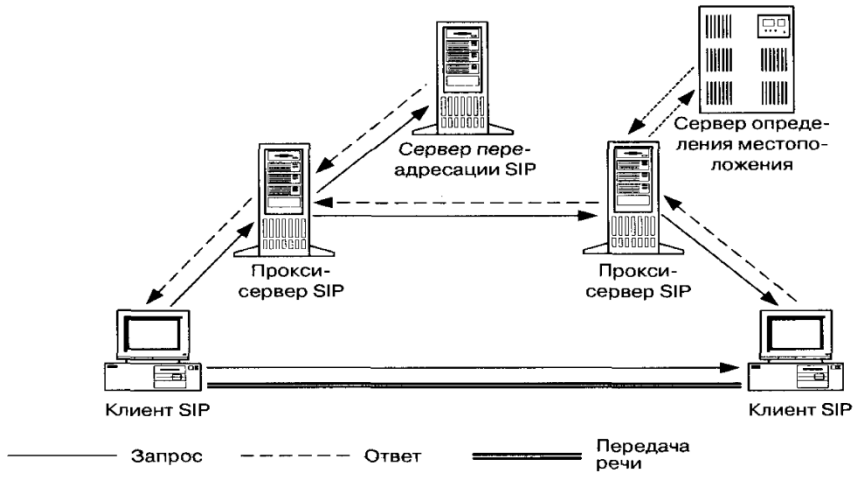

Рис.3.5. Пример сети на базе протокола SIP

Сеть SIP содержит основные элементы трех видов: агенты пользователя, прокси-серверы и серверы переадресации. Агенты пользователя (UserAgent или SIPclient) 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 (рис.3.6.). Ответные сообщения следуют по тому же пути обратно к прокси-серверу, а не к клиенту.

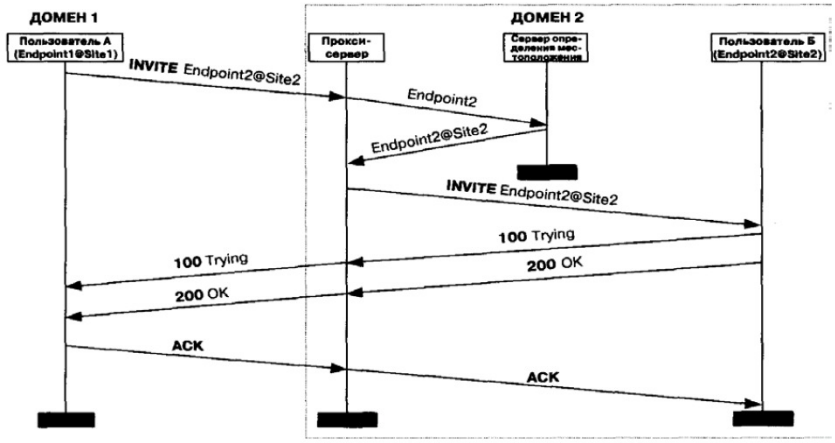

Рис.3.6. Сеть SIP с прокси-сервером

На рисунке 1.9 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.

Сервер переадресации (Redirectserver) определяет текущее местоположение вызываемого абонента и сообщает его вызывающему пользователю (рис.3.7). 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.

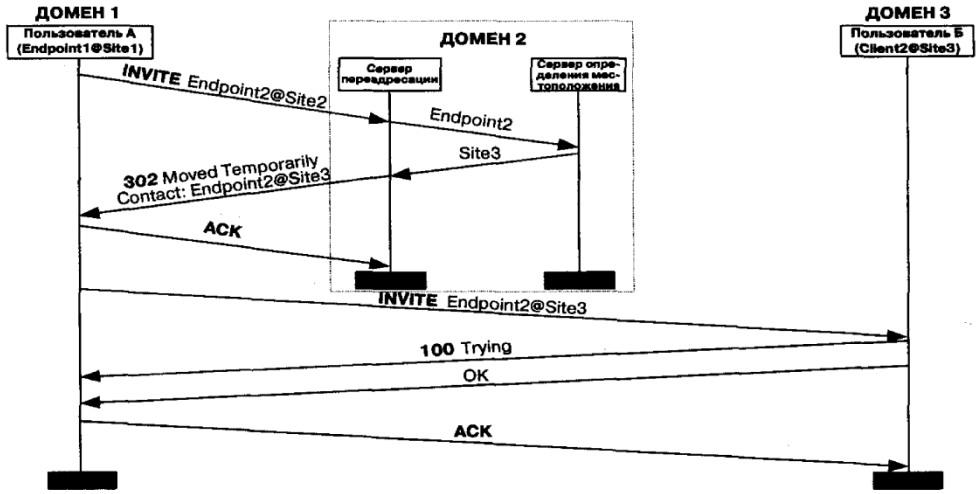

Рис3.7. Сеть SIP с сервером переадресации

Существует также и безсерверный вариант соединения, когда один терминал может передать запрос другому терминалу непосредственно.
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.

АСК - 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.

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 (рис. 3.8):

– 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.

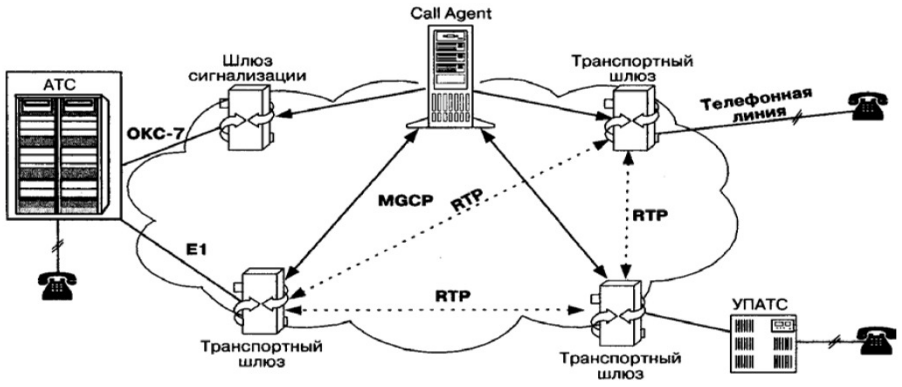

Рис. 3.8. Архитектура сети на базе протокола MGCP

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. 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.

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 (рис. 3.9).

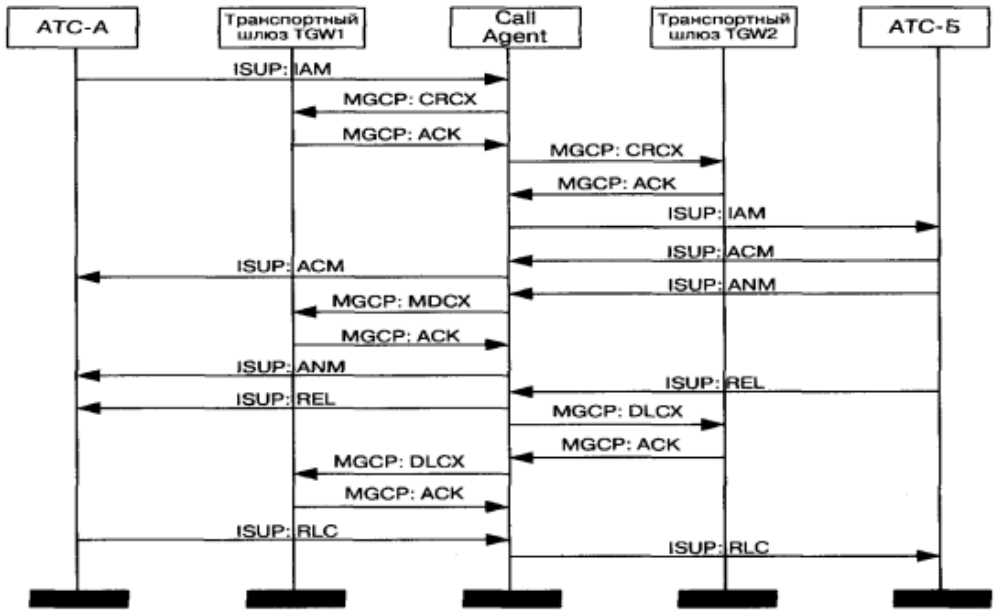

Рис. 3.9.Установление и разрушение соединения с использованием протокола MGCP (пример 1)

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.

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.

Второй пример иллюстрирует взаимодействие протокола MGCP с протоколами ОКС7 и H.323 (рис. 3.10).

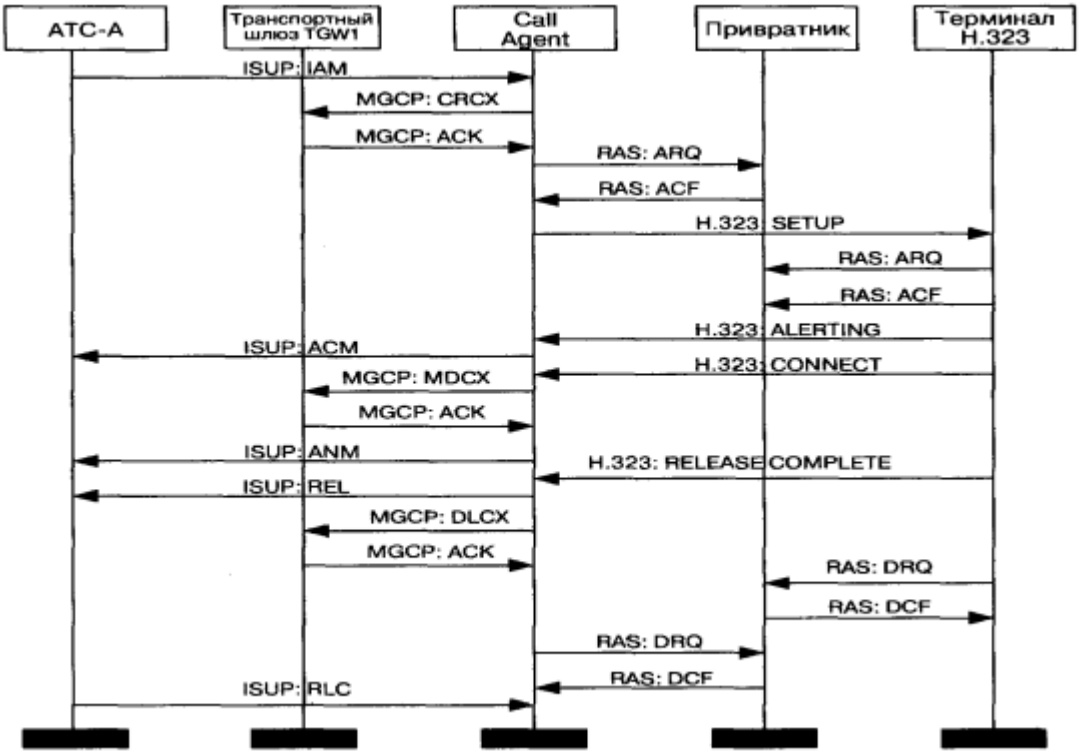

Рис. 3.10. Установление и разрушение соединения с использованиемпротокола MGCP (пример 2)

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 оконечноеоборудование 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.

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.

3.2. Варианты систем IP-телефонии (сценарии)

Существуют три наиболее часто используемых сценария IP-телефонии:

- «компьютер-компьютер»;
- «компьютер-телефон»;
- «телефон-телефон».

Сценарий «компьютер-компьютер» реализуется на базе стандартных компьютеров, оснащенных средствами мультимедиа и подключенных к сети Интернет.

Компоненты модели IP-телефонии по сценарию «компьютер-компьютер» показаны на рисунке 1.14. В этом сценарии аналоговые речевые сигналы от микрофона абонента А преобразуются в цифровую форму с помощью аналого-цифрового преобразователя (АЦП), обычно при 8000 отсчетов/с, 8 битов/отсчет, в итоге - 64 Кбит/с.

Отсчеты речевых данных в цифровой форме затем сжимаются кодирующим устройством для сокращения нужной для их передачи полосы в отношении 4:1, 8:1 или 10:1. Алгоритмы сжатия речи подробно рассматриваются в следующей главе. Выходные данные после сжатия формируются в пакеты, к которым добавляются заголовки протоколов, после чего пакеты передаются через IP-сеть в систему IP-телефонии, обслуживающую абонента Б. Когда пакеты принимаются системой абонента Б, заголовки протокола удаляются, а сжатые речевые данные поступают в устройство, развертывающее их в первоначальную форму, после чего речевые данные снова преобразуются в аналоговую форму с помощью цифро-аналогового преобразователя (ЦАП) и попадают в телефон абонента Б. Для обычного соединения между двумя абонентами системы IP-телефонии на

каждом конце одновременно реализуют как функции передачи, так и функции приема. Под IP-сетью, изображенной на рис. 3.11, подразумевается либо глобальная сеть Интернет, либо корпоративная сеть предприятия Intranet. Описанию протоколов, используемых в IP-сетях, в том числе протоколов передачи речевой информации по IP-сети.

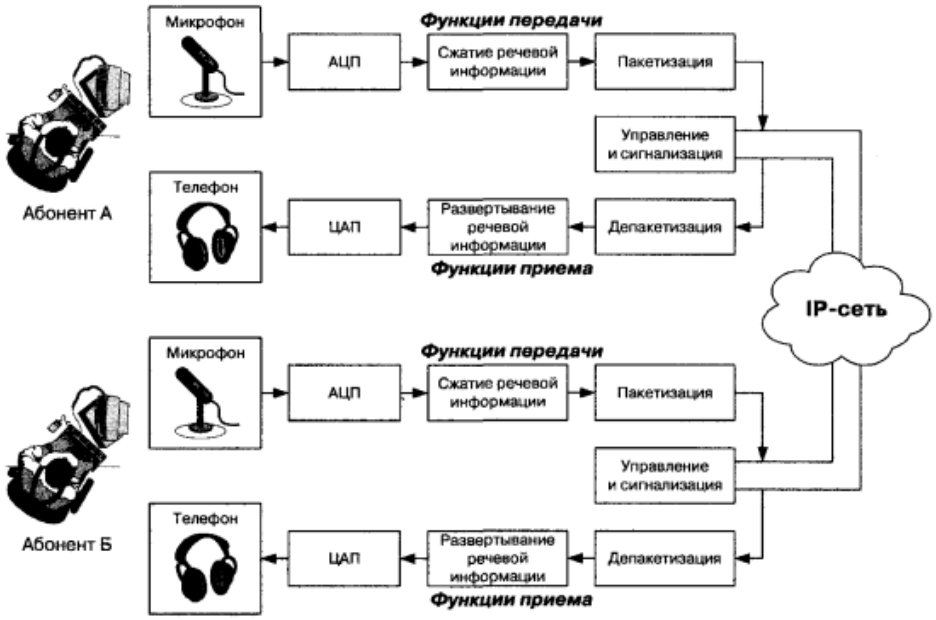

Рис. 3.11. Сценарий IP-телефонии "компьютер-компьютер"

Для поддержки сценария «компьютер - компьютер» поставщику услуг Интернет желательно иметь отдельный сервер (привратник), преобразующий имена пользователей в динамические адреса IP. Сам сценарий ориентирован на пользователя, которому сеть нужна, в основном, для передачи данных, а программное обеспечение IP-телефонии требуется лишь иногда для разговоров с коллегами.

Эффективное использование телефонной связи по сценарию «компьютер-компьютер» обычно связано с повышением продуктивности работы крупных компаний, например, при организации виртуальной презентации в корпоративной сети с возможностью не только видеть документы на Web-сервере, но и обсуждать их содержание с помощью IP-телефона. При этом

между двумя IP-сетями могут использоваться элементы ТфОП, а идентификация вызываемой стороны может осуществляться как на основе E.164, так и на основе IP-адресации. Наиболее распространенным программным обеспечением для этих целей является пакет MicrosoftNetMeeting, доступный для бесплатной загрузки с узла Microsoft.

Рассмотрим представленный на рисунок 1.14 сценарий установления соединения «компьютер-компьютер» более подробно.

Для проведения телефонных разговоров друг с другом абоненты А и Б должны иметь доступ к Интернет или к другой сети с протоколом IP. Предположим, что такаяIP-сеть существует, и оба абонента подключены к ней. Рассмотрим возможный алгоритм организации связи между этими абонентами.

1) Абонент А запускает свое приложение IP-телефонии, поддерживающее протокол H.323;

2) Абонент Б уже заранее запустил свое приложение IP-телефонии, поддерживающее протокол H.323;

3) Абонент А знает доменное имя абонента В элемент системы имен доменов - DomainNameSystem (DNS), вводит это имя в раздел «кому позвонить» в своем приложении IP-телефонии и нажимает кнопку Return;

4) Приложение IP-телефонии обращается к DNS-серверу (который в данном примере реализован непосредственно в персональном компьютере абонента А для того, чтобы преобразовать доменное имя абонента Б в IP-адрес;

5) Сервер DNS возвращает IP-адрес абонента Б;

6) Приложение IP-телефонии абонента А получает IP-адрес абонента Б и отправляет ему сигнальное сообщение H.225 Setup;

7) При получении сообщения H.225 Setup приложение абонента Б сигнализирует ему о входящем вызове;

8) Абонент Б принимает вызов и приложение IP-телефонии отправляет ответное сообщение H.225 Connect;

9) Приложение IP-телефонии у абонента А начинает взаимодействие с приложением у абонента Б в соответствии с рекомендацией H.245;

10) После окончания взаимодействия по протоколу H.245 и открытия логических каналов абоненты А и Б могут разговаривать друг с другом через IP-сеть.

Несмотря на нарочитую простоту изложения, рассмотренный пример довольно сложен, что обусловлено сложностью технологии IP-телефонии. В этом примере не показаны все шаги и опущены весьма существенные детали, которые необходимы поставщику услуг для развертывания сети IP-телефонии.

Сам характер сценария «компьютер-компьютер» на рис.3.11. обуславливает сосредоточение всех необходимых функций IP-телефонии в персональном компьютере или другом аналогичном устройстве конечного пользователя. При описании других сценариев в этой главе вместо громоздкого изображения компонентов оконечного устройства будет приводится только упрощенное изображение терминала IP-телефонии. Таким аналогом рисунка 3.11 является упрощенное представление того же сценария на рис.3.12.

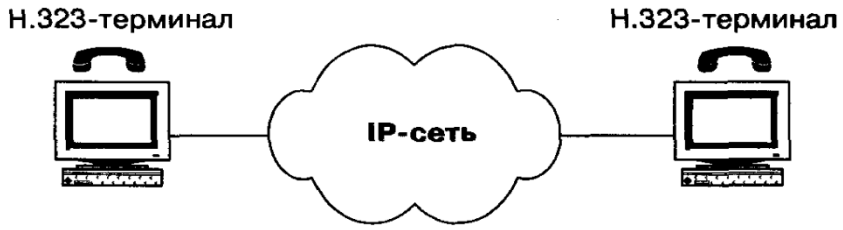

Рис.3.12. Упрощенный сценарий IP-телефонии "компьютер-компьютер"

Замена изображений имеет и более глубокий смысл. Название сценария «компьютер - компьютер» отнюдь не означает, что в распоряжении пользователя обязательно должен быть стандартный PC с микрофоном и колонками, как это представлено на рисунке 1.14.

Главным требованием для такой схемы является то, что оба пользователя должны иметь подключенные к сети персональные компьютеры. И эти PC должны быть всегда включены, подсоединены к сети и иметь в запущенном виде программное обеспечение IP-телефонии для приема входящих вызовов. При всем этом должна быть полная совместимость между программно-

аппаратными средствами IP-телефонии, полученными от разных поставщиков, т.е. пользователи, желающие разговаривать друг с другом, должны иметь идентичное программное обеспечение, например, реализующее протокол H.323.

Принимая во внимание эти обстоятельства, под названием «компьютер» во всех сценариях мы будем понимать терминал пользователя, включенный в IP-сеть, а под названием «телефон» - терминал пользователя, включенный в сеть коммутации каналов любого типа: ТфОП, ISDN или GSM.

Соединение пользователей IP-сетей через транзитную СКК Следующий сценарий - «телефон-компьютер» - находит применение в разного рода справочно-информационных службах Интернет, в службах сбыта товаров или в службах технической поддержки. Пользователь, подключившийся к серверуWWW какой-либо компании, имеет возможность обратиться к оператору справочной службы. Этот сценарий в ближайшие несколько лет будет, по всей вероятности, более активно востребован деловым сектором

Компании будут использовать данную технологию для наращивания своих WeЬ - страниц (и своего присутствия во всемирной паутине). Пользователи компьютеров смогут просматривать в «реальном времени» каталоги, почти мгновенно заказывать товары и получать множество других услуг. Это вполне соответствует стилю жизни современных потребителей, связанному с потребностью в дополнительных удобствах и экономии времени. Уже сегодня осознаются все выгоды и удобства централизованного приобретения предметов широкого потребления (например, компакт-дисков, книг, программного обеспечения и т. д.) и уже привычно совершаются операции электронной коммерции. Чащевсегорассматриваютсядвемодификацииэтогосценария IP-телефонии:

– от компьютера (пользователя IP-сети) к телефону (абоненту ТфОП), в частности, в связи с предоставлением пользователям IP-сетей доступа к телефонным услугам, в том числе, к справочно- информационным услугам и к услугам Интеллектуальной сети;

– от абонента ТфОП к пользователю IP-сети с идентификацией вызываемой стороны на основе нумерации по E.164 или IP- адресации.

В первой из упомянутых модификаций сценария «компьютер - телефон» соединение устанавливается между пользователем IP-сети и пользователем сети коммутации каналов (рис.3.13). Предполагается, что установление соединения инициирует пользователь IP-сети.

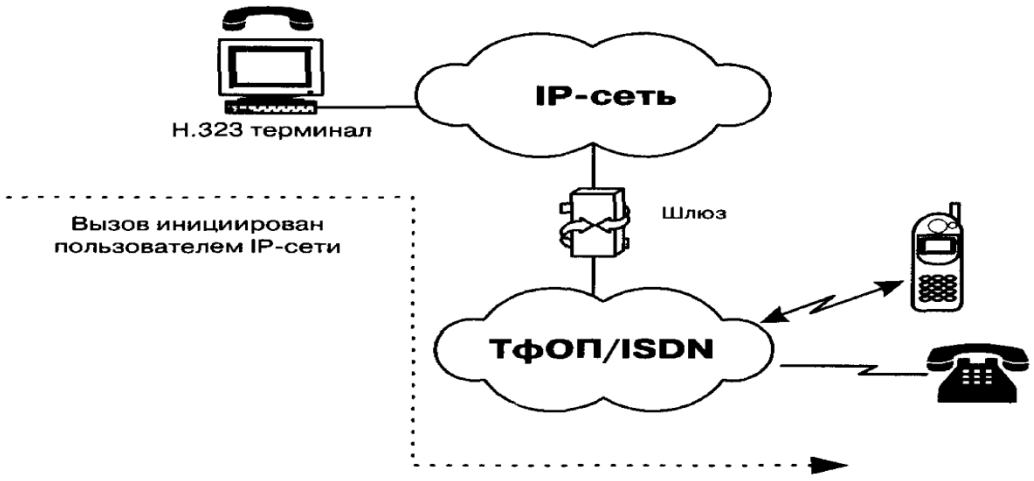

Рис. 3.13. Вызов абонента ТфОП пользователем IP-сети по сценарию "компьютер - телефон"

Шлюз (GW) для взаимодействия сетей ТфОП и IP может быть реализован в отдельном устройстве или интегрирован в существующее оборудование ТфОП или IP-сети. Показанная на рисунке сеть СКК может быть корпоративной сетью или сетью общего пользования.

В соответствии со второй модификацией сценария «компьютер - телефон» соединение устанавливается между пользователем IP-сети и абонентом ТфОП, но инициирует его создание абонент ТфОП (рисунок 1.17).

На рис.3.14. представлена упрощенная архитектура системы IP-телефонии по сценарию «телефон-компьютер». При попытке вызвать справочно-информационную службу, используя услуги пакетной телефонии и обычный телефон, на начальной фазе абонент А вызывает близлежащий шлюз IP-телефонии. От шлюза к абоненту А поступает запрос ввести номер, к

которому должен быть направлен вызов (например, номер службы), и личный идентификационный номер (PIN) для аутентификации и последующего начисления платы, если это служба, вызов которой оплачивается вызывающим абонентом.

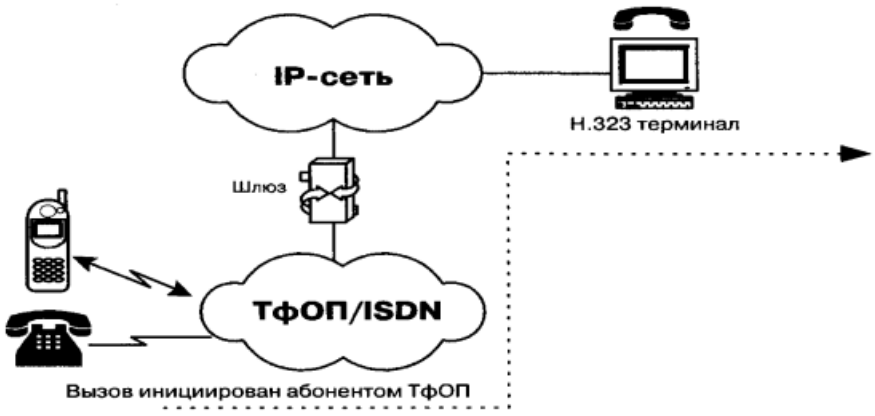

Рис. 3.14. Пользователя IP-сети вызывает абонент ТФОП по сценарию "компьютер - телефон"

Основываясь на вызываемом номере, шлюз определяет наиболее доступный путь к данной службе. Кроме того, шлюз активизирует свои функции кодирования и пакетизации речи, устанавливает контакт со службой, ведет мониторинг процесса обслуживания вызова и принимает информацию о состояниях этого процесса (например, занятость, посылка вызова, разъединение и т.п.) от исходящей стороны через протокол управления и сигнализации. Разъединение с любой стороны передается противоположной стороне по протоколу сигнализации и вызывает завершение установленных соединений и освобождение ресурсов шлюза для обслуживания следующего вызова.

Для организации соединений от службы к абонентам (рисунок 1.17) используется аналогичная процедура. Популярными программными продуктами для этого варианта сценария IP-телефонии «компьютер-телефон» являются IDTNet2Phone и DotDialer, организующие вызовы к обычным абонентским телефонным аппаратам в любой точке мира.

Эффективность объединения услуг передачи речи и данных является основным стимулом использования IP-телефонии по сценариям «компьютер-

компьютер» и «компьютер-телефон», не нанося при этом никакого ущерба интересам операторов традиционных телефонных сетей.

Сценарий «телефон-телефон» в значительной степени отличается от остальных сценариев IP-телефонии своей социальной значимостью, поскольку целью его применения является предоставление обычным абонентам ТфОП альтернативной возможности междугородной и международной телефонной связи. В этом режиме современная технология IP-телефонии предоставляет виртуальную телефонную линию через IP-доступ. Как правило, обслуживание вызовов по такому сценарию IP-телефонии выглядит следующим образом. Поставщик услуг IP-телефонии подключает свой шлюз к коммутационному узлу или станции ТфОП, а по сети Интернет или по выделенному каналу соединяется с аналогичным шлюзом, находящимся в другом городе или другой стране.

Типичная услуга IP-телефонии по сценарию «телефон-телефон» использует стандартный телефон в качестве интерфейса пользователя, а вместо междугородного компонента ТфОП использует либо частную IP-сеть/Intranet, либо сеть Интернет.

Благодаря маршрутизации телефонного трафика по IP-сети стало возможным обходить сети общего пользования и, соответственно, не платить за междугородную/международную связь операторам этих сетей.Следует отметить, что сама идея использовать альтернативные транспортные механизмы для обхода сети ТфОП не является новой.

Достаточно вспомнить статистические мультиплексоры, передачу речи по сети FrameRelay или оборудование передачи речи по сети ATM. Как показано на рис. 3.15., поставщики услуг IP-телефонии предоставляют услуги «телефон-телефон» путём установки шлюзов IP-телефонии на входе и выходе IP-сетей. Абоненты подключаются к шлюзу поставщика через ТфОП, набирая специальный номер доступа.

Абонент получает доступ к шлюзу, используя персональный идентификационный номер (PIN) или услугу идентификации номера

вызывающего абонента (CallingLineIdentification). После этого шлюз просит ввести телефонный номер вызываемого абонента, анализирует этот номер и определяет, какой шлюз имеет лучший доступ к нужному телефону. Как только между входным и выходным шлюзами устанавливается контакт, дальнейшее установление соединения к вызываемому абоненту выполняется выходным шлюзом через его местную телефонную сеть.

Полная стоимость такой связи будет складываться для пользователя из расценок ТфОП на связь с входным шлюзом, расценок Интернет-провайдера на транспортировку и расценок удалённой ТфОП на связь выходного шлюза с вызванным абонентом.

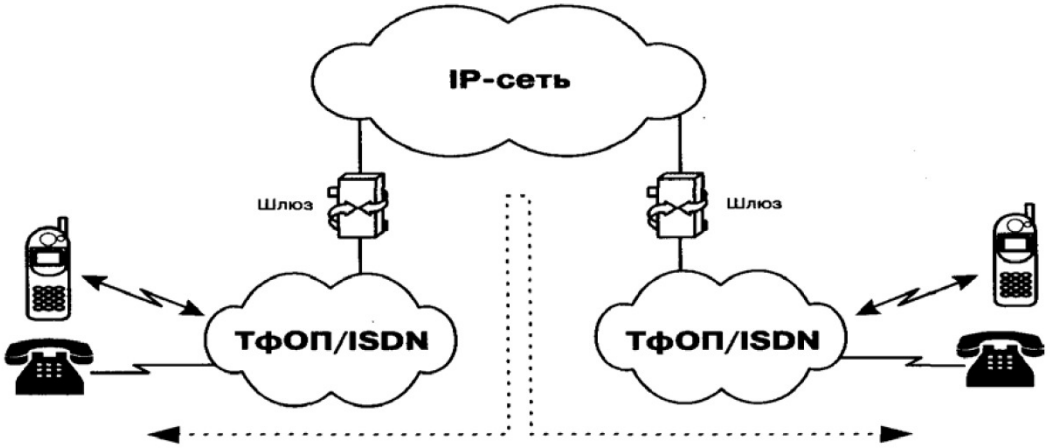

Рис.3.15. Соединение абонентов ТфОП через транзитнуюIP-сеть по сценарию "телефон-телефон"

Одним из алгоритмов организации связи по сценарию «телефон-телефон» является выпуск поставщиком услуги своих телефонных карт. Имея такую карту, пользователь, желающий позвонить в другой город, набирает номер данного поставщика услуги, затем в режиме донабора вводит свой идентификационный номер и PIN-код, указанный на карте. После процедуры аутентификации он набирает телефонный номер адресата.

Возможны и другие алгоритмы реализации этого сценария: вместо телефонной карты может использоваться информация об альтернативном счете. Счет для оплаты может быть выслан абоненту и после разговора, аналогично тому, как это делается при междугородном соединении в ТфОП.

3.3. Типы угроз, методы и внедрение безопасности в системы 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.

– 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. Методышифровкиданныхснижаютвероятностьэтойугрозы.

– 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.

– 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.

Число фишинг рассылок и фишерских сайтов в мире с мая 2008 по май 2009 года

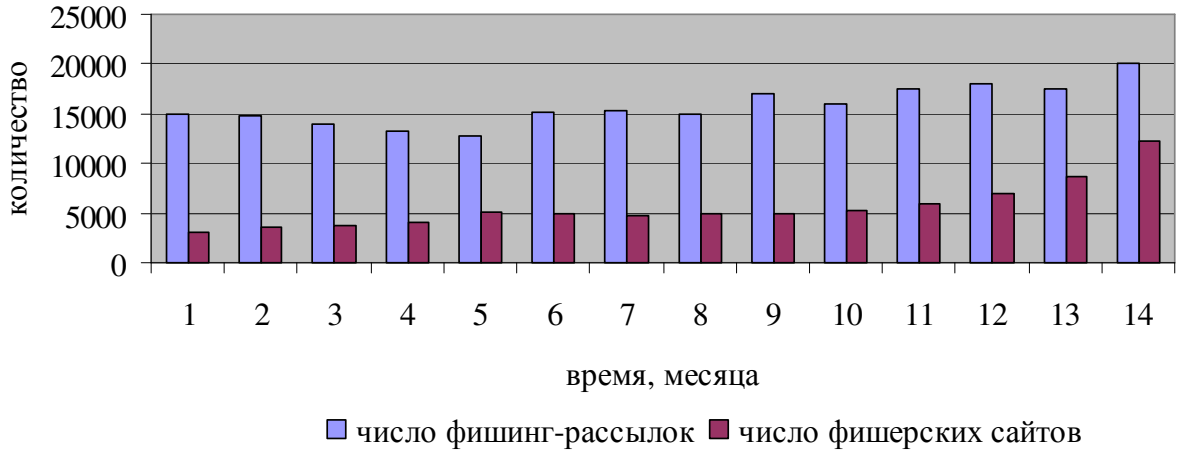

Рис. 3.17.

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.

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 криптографические ключи. Причем чем больше битов в таком ключе, тем менее он уязвим.

В системах обеспечения безопасности используются три основных криптографических метода:

- симметричноешифрование;
- асимметричноешифрование;
- односторонниехэш-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.

В настоящее время широко используются алгоритмы секретных ключей типа DataEncryptionStandard (DES), 3DES (или «тройнойDES») 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:

– обеспечениеконфиденциальностиданных;

– аутентификацияотправителя;

– 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.

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.

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

Обычныехэш-функциивключают:

- алгоритм Message Digest 4 (MD4);
- алгоритм Message Digest 5 (MD5);
- алгоритмбезопасногохэша (Secure Hash Algorithm — 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.

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:

- номерверсии;
- серийныйномерсертификата;
- эмитентинформациюбалгоритме;
- эмитентсертификата;
- даты начала и окончания действия сертификата;
- информация об алгоритме общего ключа субъекта сертификата;
- подписьэмитирующейорганизации.

На практике часто используют совместно шифрование и цифровые сертификаты. Например, маршрутизатор и межсетевой экран имеют по одной паре общих/частных ключей (Рис 3.18). 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.

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

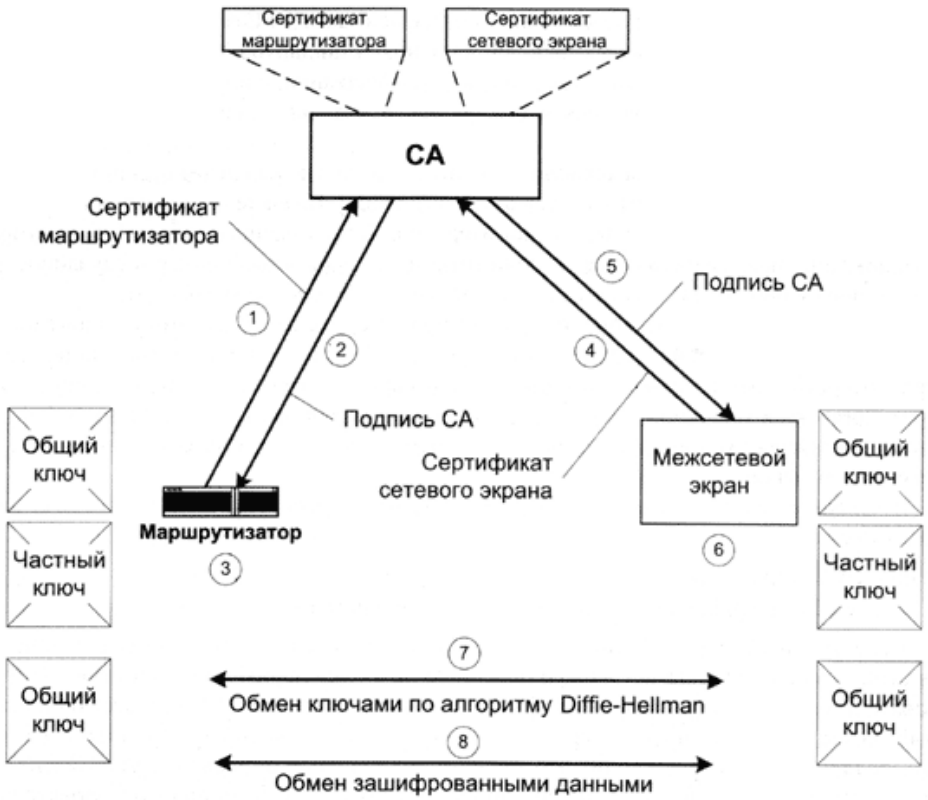

Рис. 3.18. Безопасная связь с использованием шифрования

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 СА запрос на получение общего ключа маршрутизатора.

СА отправляет ему сертификат маршрутизатора, зашифрованный частным ключом СА.

Межсетевой экран расшифровывает сертификат общим ключом СА 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 следующим образом (рис. 3.19).

Рис. 3.19. Общий вид криптографической системы

Для использования такой системы для определенного сообщения Mi выбирается некоторый ключ Ki из множества возможных ключей K. После чего при помощи ключа Ki формируется криптограмма Ei. Эта криптограмма, полученная при помощи преобразования TKi, по каналу передачи передается в точку приема. На приемном конце с помощью отображения TK–i1, обратного выбранному, из криптограммы Ei восстанавливается исходное сообщение Mi.

Если противник перехватит криптограмму, то он не сможет ее расшифровать, если не знает ключа Ki. Поэтому, чем больше мощность

множества K, тем меньше вероятность того, что криптограмма будет расшифрована. Эта вероятность называется апостериорной вероятностью. Вычисление апостериорных вероятностей – есть общая задача дешифрования.

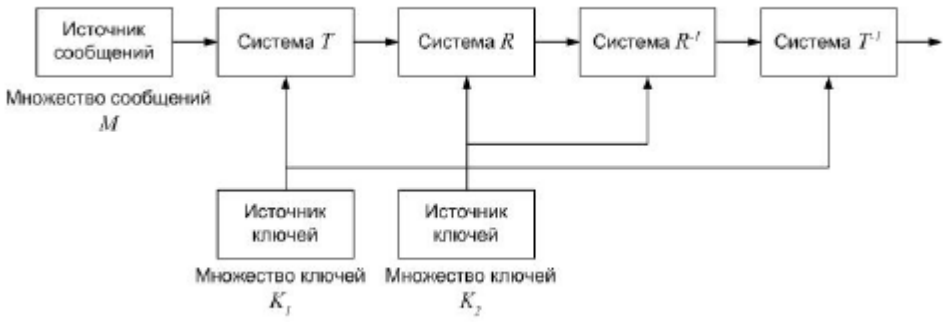

Рис 3.20. Произведение двух секретных систем

Образование произведения двух секретных систем (Рис 3.20) осуществляется следующим образом: S = RT, причемRS = SR, а RS ≠ RS.

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

Ключ системы S состоит как из ключа системы T, так и из ключа системы R.

Рис. 3.21. Классификация современных криптосистем

По характеру использования ключа все криптосистемы можно разделить на симметричные (одноключевые с секретным ключом) и асимметричные (несимметричные, с открытым ключом). В первом случае как для шифрования, так и для дешифрования применяется один и тот же ключ. Он является секретным и передается отправителем получателю по каналу связи, исключающем перехват. В асимметричных системах для шифрования и дешифрования используются разные ключи, связанные между собой некоторой математической зависимостью. Причем зависимость является такой, что из одного ключа вычислить другой ключ очень трудно за приемлемый промежуток времени.

Функции шифрования и дешифрования в зависимости от алгоритма могут быть одинаковыми или, что чаще всего, разными, причем процесс дешифрования является инверсией процесса шифрования.

Все многообразие симметричных криптографических систем (рисунок 2.5) основывается на следующих базовых классах:

– Блочные шифры. Представляют собой семейство обратимых преобразований блоков (частей фиксированной длины) исходного текста. Фактически блочный шифр – это система подстановки блоков. После разбиения текста на блоки каждый блок шифруется отдельно независимо от его положения и входной последовательности.

Одним из наиболее распространенных способов задания блочных шифров является использование так называемых сетей Фейстела. Сеть Фейстела представляет собой общий метод преобразования произвольной функции в перестановку на множестве блоков.

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

– Шифры замены (подстановки). Шифры замены (подстановки) – это наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному

правилу. Подстановки различают моноалфавитные и многоалфавитные. В первом случае каждый символ исходного текста преобразуется в символ шифрованного текста по одному и тому же закону. При многоалфавитной одстановке закон меняется от символа к символу. К этому классу относится так называемая система с одноразовым ключом.

– Шифры перестановки. Перестановки – метод криптографического преобразования, заключающийся в перестановке местами символов исходного текста по некоторому правилу. Шифры перестановки в настоящее время не используются в чистом виде, так как их криптостойкостьнедостаточна.

– Гаммирование. Гаммирование – представляет собой преобразование, при котором символы исходного текста складываются по модулю, равному мощности алфавита, с символами псевдослучайной последовательности, вырабатываемой по некоторому правилу. В принципе, гаммирование нельзя выделить в отдельный класс криптопреобразований, так как эта псевдослучайная последовательность может вырабатываться, например, при помощи блочного шифра.

– Потоковые шифры. Потоковые шифры представляют собой разновидность гаммирования и преобразуют открытый текст в шифрованный последовательно, по одному биту.Генератор ключевой последовательности, иногда называемый генератором бегущего ключа, выдает последовательность бит k1,k2,...,ki ,.... Эта ключевая последовательность складывается по модулю 2 с последовательностью бит исходного текста p1, p2,..., pi ,... для получения шифрованного текста ci = pi*ki . На приемной стороне текст складывается по модулю 2 с идентичной ключевой последовательностью для получения исходного текста. Такое преобразование называется гаммированием с помощью операции XOR. Однако при потоковом шифровании для повышения криптостойкости генератор ключевой последовательности «завязывается» на текущее состояние кодируемого символа. То есть значения, выдаваемые

генератором, зависят не только от ключа, но и от номера шифруемого бита и входной последовательности.

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.

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.

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.

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. 3.21.

Рис 3.21. Передача данных в открытом канале данных

Рис. 3.22. 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 рис 3.23.

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.

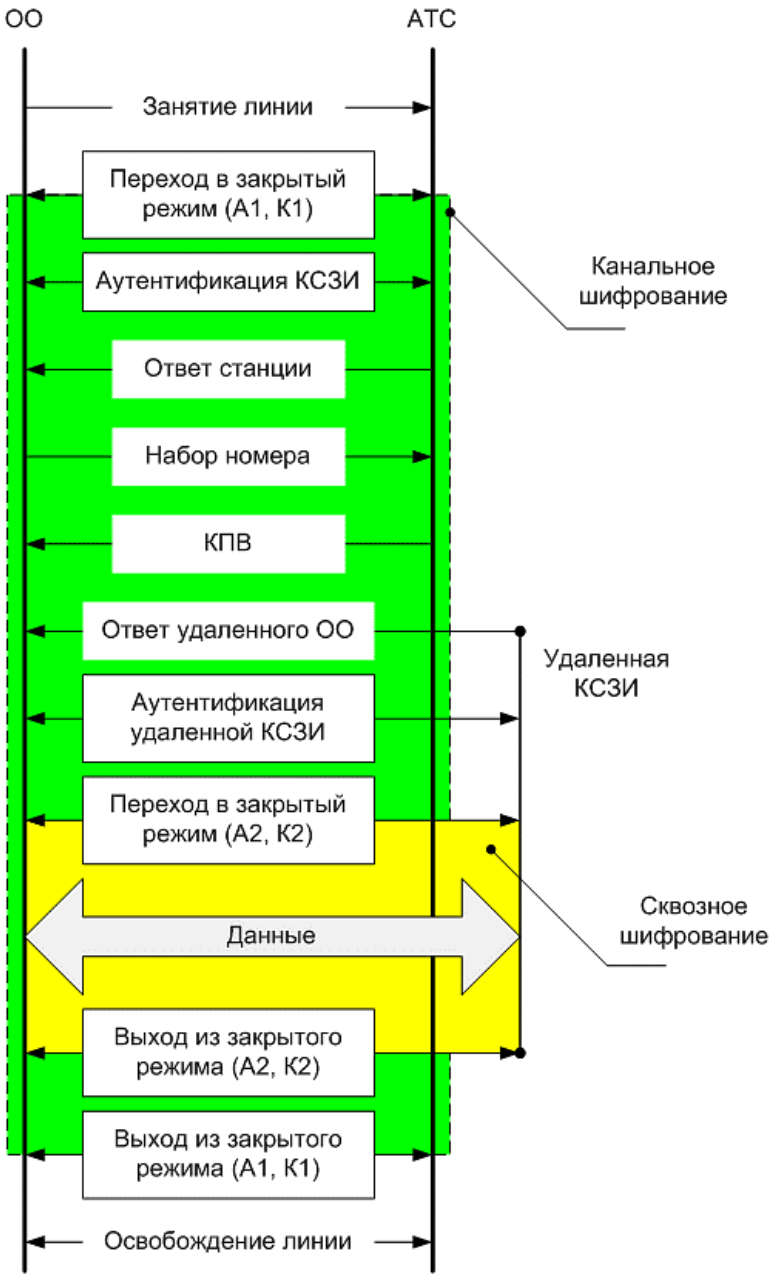

Рис. 3.23. Передача данных в закрытом канале данных

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.

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.

Технологии аутентификации:

Под аутентификацией понимается определение пользователя или конечного устройства (клиента, сервера, коммутатора, маршрутизатора, межсетевого экрана и т.д.) и его местоположения в сети с последующей авторизацией пользователей и конечных устройств. Наиболее простым способом аутентификации является использование паролей, но для поддержания высокого уровня безопасности пароли приходится часто менять. Методы использования одноразовых паролей применяются по-прежнему широко. Среди них можно отметить методы аутентификации по протоколу S/Key или при помощи специальных аппаратных средств (tokenpasswordauthentication). Механизм аутентификации по протоколу Point-to-PointProtocol (PPP) часто применяется в среде модемного доступа и включает использование протоколов PasswordAuthenticationProtocol (PAP), ChallengeHandshakeProtocol (CHAP) и ExtensibleAuthenticationProtocol (EAP). Разработка протокола EAP все еще продолжается, но уже сейчас он дает возможность более гибкого

использования существующих и только появляющихся технологий аутентификации в каналах PPP. TACACS+ и RemoteAccessDial-InUserService (RADIUS) — это протоколы, которые поддерживают масштабируемые решения в области аутентификации. Протокол Kerberos (Цербер) используется в ограниченных областях для поддержки единой точки входа в сеть.

Система одноразовых паролей S/Key, определенная в RFC 1760, представляет собой систему генерирования одноразовых паролей на основе стандартов MD4 и MD5. Она предназначена для борьбы «повторными атаками», когда хакер подслушивает канал, выделяет из трафика идентификатор пользователя и его пароль и в дальнейшем использует их для несанкционированного доступа.

Система S/Key основана на технологии клиент-сервер, где клиентом обычно является персональный компьютер, а сервером — сервер аутентификации. Вначале и клиента, и сервер нужно настроить на единую парольную фразу и счет итерации. Клиент начинает обмен S/Key, отправляя серверу пакет инициализации, а сервер в ответ отправляет порядковый номер и случайное число, так называемое «зерно» (seed). После этого клиент генерирует одноразовый пароль.

После создания одноразового пароля его нужно проверить. Для этого клиент передает одноразовый пароль на сервер, где он и проверяется. Для проверки аутентификации система однократно пропускает полученный одноразовый пароль через защищенную хэш-функцию. Если результат этой операции совпадает с предыдущим паролем, хранящимся в файле, результат аутентификации считается положительным, а новый пароль сохраняется для дальнейшего использования.

Аутентификация с помощью аппаратных средств работает по одной из двух альтернативных схем:

- посхемезапрос-ответ;
- по схеме аутентификации с синхронизацией по времени.

В схеме запрос-ответ пользователь подключается к серверу аутентификации, который, в свою очередь, предлагает ввести персональный идентификационный номер (PIN) или пользовательский идентификатор (userID). Пользователь передает PIN или userID на сервер, который затем делает «запрос» (передает случайное число, которое появляется на экране пользователя). Пользователь вводит это число в специальное аппаратное устройство, похожее на кредитную карточку, где число запроса шифруется с помощью пользовательского шифровального ключа. Результат шифрования отображается на экране. Пользователь отправляет этот результат на сервер аутентификации. В то время как пользователь подсчитывает этот результат, сервер аутентификации рассчитывает этот же результат самостоятельно, используя для этого базу данных, где хранятся все пользовательские ключи. Получив ответ от пользователя, сервер сравнивает его с результатом собственных вычислений. Если оба результата совпадают, пользователь получает доступ к сети. Если результаты оказываются разными, доступ к сети не предоставляется.

При использовании схемы с синхронизацией по времени на аппаратном устройстве пользователя и на сервере работает секретный алгоритм, который через определенные синхронизированные промежутки времени генерирует идентичные пароли и заменяет старые пароли на новые. Пользователь подключается к серверу аутентификации, который запрашивает у пользователя код доступа. После этого пользователь вводит свой PIN в аппаратное карточное устройство, и в результате на экран выводится некоторая величина, которая представляет собой одноразовый пароль. Этот пароль и отправляется на сервер. Сервер сравнивает его с паролем, который был вычислен на самом сервере. Если пароли совпадают, пользователь получает доступ к сети.

3. Обеспечение безопасности с точки зрения проверки прав доступа к ресурсам (AAA):

Сеть IP-телефонии любого провайдера, как правило, имеет несколько точек доступа к услуге; при такой схеме организации реализовывать процесс

аутентификации пользователей для каждой точки доступа в отдельности (на месте) не целесообразно. Гораздо разумнее централизовать процесс аутентификации, используя для этого отдельный сервер и общую базу данных, к которым будут обращаться серверы доступа (такое решение получило название непрямой аутентификации). Объясняется это главным образом с точки зрения проблем администрирования, возникающих в случае организации аутентификации на месте.

3.1 Непрямая аутентификация

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.

Решения на основе непрямой аутентификации позволяют справляться с проблемой масштабируемости на вычислительных центрах, у которых одна группа пользователей, но несколько точек обслуживания. Даже на той площадке, где всего два сервера, будет затруднительно поддерживать совместимость двух отдельных баз данных аутентификации. Если другие проектные шаблоны предусматривают объединение механизмов аутентификации и управления доступом, то шаблон непрямой аутентификации перемещает механизм аутентификации из точки обслуживания в отдельный аутентификационный сервер. Все другие компоненты сети предоставляют услуги или управляют доступом к ресурсам, но не принимают решений об аутентификации. Вместо этого они аутентифицируют пользователей непрямым способом, связываясь с аутентификационным сервером всякий раз, когда кто-то пытается зарегистрироваться в системе.

С точки зрения обеспечения безопасности соединения как в сетях IP-телефонии в частности, так и в IP-сетях вообще, проблему можно условно разделить на две составляющих.

Первое – это проблема обеспечения правомерного и безопасного доступа к сетевым ресурсам и услугам, а второе – это обеспечение безопасности информации уже непосредственно в каналах. Именно первой

части проблемы обеспечения безопасности в сетях IP-телефонии и посвящена эта дипломная работа.

Совершенно очевидно, что основная роль при решении подобных задач будет принадлежать процессу аутентификации пользователей. В силу структуры мультисервисной сети, на базе которой предоставляются услуги IP-телефонии нас будет интересовать непрямая аутентификация, ее протоколы, а также слабые и сильные места.

Многие широко известные сегодня системы обеспечивают непрямую аутентификацию с помощью специально разработанных протоколов.

Открытым стандартом для реализации непрямой аутентификации является протокол RADIUS. В общем случае протокол непрямой аутентификации начинает свою работу, когда кто-нибудь пытается зарегистрироваться в точке обслуживания с удаленного места, которым может быть, например, рабочая станция. Когда точка обслуживания принимает запрос на регистрацию, она пересылает имя пользователя и пароль аутентификационному серверу. Часто для пересылки данных таких сообщений используется внутренний протокол типа RADIUS или протокол, разработанный изготовителем. Если сервер подтверждает аутентификацию, то он посылает в точку обслуживания подтверждение, сформатированное в соответствии с этим внутренним протоколом. Получив его, точка обслуживания принимает к исполнению попытку пользователя зарегистрироваться. Если сервер посылает отказ, то точка обслуживания отвергает запрос. Поскольку аутентификационные запросы перенаправляются аутентификационному серверу, имеется риск, что взломщик будет подделывать сообщение «Доступ разрешен», чтобы обмануть точку доступа; поэтому для аутентификации двусторонних сообщений между точкой обслуживания и аутентификационным сервером должно использоваться шифрование.

Некоторые системы, использующие непрямую аутентификацию, могут иметь высокий уровень устойчивости к отказам, поддерживая функцию перенаправления. Если какой-либо из серверов теряет работоспособность (в

том числе и при DOS-атаке), то запросы на аутентификацию могут перенаправляться на альтернативный сервер, содержащий копию всей аутентификационной базы данных. Это позволяет провайдеру IP-телефонии реплицировать свои службы на несколько хост-машин и реализовать аутентификацию на нескольких аутентификационных серверах, исключаятем самым появление точки критического отказа.

3.2 Технологии AAA на основе протокола TACACS+

3.2.1 Протокол TACACS+

TACACS+ – это простой протокол управления доступом, основанный на стандартах UDP и разработанных компанией Bolt, BeranekandNewman, Inc. (BBN). TACACS+ представляет собой приложение сервера защиты, позволяющее на основе соответствующего протокола реализовать централизованное управление доступом пользователей к услугам. Информация о сервисах TACACS+ и пользователях хранится в базе данных, обычно размещенной на компьютере под управлением UNIX или WindowsNT. TACACS+ позволяет с помощью одного сервера управления приложениями реализовать независимую поддержку сервисов AAA.

Протокол TACACS+ работает по технологии клиент-сервер.

Фундаментальным структурным компонентом протокола TACACS является разделение аутентификации, авторизации и учета. Это позволяет обмениваться идентификационными сообщениями любой длины и содержания, и, следовательно, использовать для клиентов TACACS+ любой идентификационный механизм, в том числе PPPPAP, PPPCHAP, аппаратные карты и т.д.

Свойства протокола TACACS+

TACACS+ поддерживает следующие возможности сервера защиты:

- Пакеты TCP для надежной передачи данных. Использование TCP в качестве протокола связи для соединений TACACS+ между сервером доступа и сервером защиты. Для TACACS+ резервируется TCP-порт 49.

- Архитектура AAA. Каждый сервис предоставляется отдельно и имеет собственную базу данных, но, тем не менее, они работают вместе, как один сервер защиты.

- Канальное шифрование. Часть TCP-пакета, содержащая данные протокола TACACS+, шифруется с целью защиты трафика между сервером доступа и сервером защиты.

- Каждый пакет TACACS+ имеет 12-байтовый заголовок, пересылаемый в виде открытого текста, и тело переменной длины, содержащее параметры TACACS+. Тело пакета шифруется с помощью алгоритма, использующего псевдослучайный заполнитель, получаемый посредством MD5. Пакеты TACACS+ передаются по сети и хранятся сервером TACACS+ в шифрованном виде. Когда это необходимо, пакет дешифруется сервером доступа и приложением TACACS+ путем обращения алгоритма шифрования.

- Аутентификация PAP и CHAP. Обеспечивает полный контроль аутентификации с помощью средств вызова/ответа PAP и CHAP, а также посредством использования диалоговых окон ввода пароля доступа и поддержки сообщений интерактивной процедуры начала сеанса.

- Защита локальных и глобальных сетей. Поддержка средств AAA удаленного и локального сетевого доступа для серверов доступа, маршрутизаторов и другого сетевого оборудования, поддерживающего TACACS+. Дает возможность осуществлять централизованное управление сетевым оборудованием.

- Функция обратного вызова. Данная функция возвращает телефонные вызовы, заставляя сервер доступа звонить соответствующему пользователю, что может дать дополнительные гарантии защиты.

- Индивидуальные списки доступа пользователей. База данных TACACS+ может дать указание серверу сетевого доступа контролировать доступ данного пользователя к сетевым службам и ресурсам в течении фазы авторизации на основе списка доступа.

Процессы AAA в протоколе TACACS+:

Аутентификация не является обязательной. Она рассматривается как опция, которая конфигурируется на месте. В некоторых местах она вообще не требуется, в других местах она может применяться лишь для ограниченного набора услуг.

Заголовок пакета TACACS+ содержит поле типа, являющееся признаком того, что пакет представляет собой часть процесса AAA. Аутентификация TACACS+ различает три типа пакетов: START (начало),CONTINUE (продолжение) и REPLY (ответ).

В запросе на авторизацию можно указать, что аутентификация пользователя не проведена (личность 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 или 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.

В процессе авторизации TACACS+ используется два типа пакетов: REQUEST (запрос) и RESPONSE (ответ). Данный процесс авторизации пользователя контролируется посредством обмена парами «атрибут/значение» между сервером защиты TACACS+ и сервером доступа.

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 использованных услуг (например, для выставления счетов). 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» говорят о том, что услуга только что окончилась. Записи «обновление» (update) являются промежуточными и указывают на то, что услуга все еще предоставляется. Учетные записи TACACS+ содержат всю информацию, которая используется в ходе авторизации, а также другие данные: время начала и окончания (если это необходимо) и данные об использовании ресурсов. Транзакции между клиентом TACACS+ и сервером TACACS+ идентифицируются с помощью общего «секрета», который никогда не передается по каналам связи. Обычно этот «секрет» вручную устанавливается на сервере и на клиенте. TACACS+ можно настроить на шифрование всего трафика, который передается между клиентом и демоном сервера TACACS+.

В процессе аудита TACACS+ использует два типа пакетов – REQUEST (запрос) и RESPONSE (ответ). Данный процесс во многом подобен процессу авторизации. В процессе аудита создаются записи с информацией об активности пользователя в отношении заданных сервисов. Записи, регистрирующие выполненные сетевым оборудованием действия, могут сохраняться в некотором стандартном формате, на сервере защиты с целью дальнейшего анализа.

В рамках TACACS+ аудит AAA не является средством надежной защиты и обычно используется только для учета или управления. Однако с помощью аудита AAA можно контролировать действия пользователя, чтобы, например, вовремя заметить его необычное поведение при работе с сетевым оборудованием.

3.3 Технологии AAA на базе протокола RADIUS

3.3.1 Протокол RADIUS

Протокол RADIUS был разработан компанией LivingstonEnterprises, Inc. (теперь находящейся в составе LucentTechnologies) в качестве протокола аутентификации серверного доступа и учета. В настоящее время протокол RADIUS описывается в документе RFC 2865, а аудит RADIUS – в RFC 2866.

RADIUS (RemoteAccessDial-InUserService – сервис идентификации удаленных абонентов) представляет собой распределенный протокол, используемый в рамках технологии клиент/сервер и обеспечивающий защиту сети от несанкционированного доступа. Так например компания Cisco поддерживает RADIUS как одну из составляющих системы защиты AAA.

Рассматриваемый протокол скорее объединяет аутентификацию и авторизацию, чем трактует их отдельно, как это делается в отношении аудита.

Протокол RADIUS может использоваться с другими протоколами защиты AAA, например с TACACS+, Kerberos и локальными базами данных защиты. Протокол RADIUS реализован во многих сетевых средах, требующих высокого уровня защиты при условии поддержки сетевого доступа для удаленных пользователей. Он представляет собой полностью открытый протокол, поставляемый в формате исходного текста, который можно изменить для того, чтобы он мог работать с любой доступной в настоящий момент системой защиты. Широкую популярность RADIUS обеспечивает возможность добавлять новые пары «атрибут/значение» в дополнение к тем, которые описаны в документе RFC 2865. Протокол RADIUS имеет атрибут поставщика , позволяющий поставщику осуществлять поддержку своих собственных расширенных наборов атрибутов, включающих нестандартные атрибуты. Вследствие использования пар «атрибут/значение» конкретных поставщиков могут возникать трудности при интеграции серверных продуктов защиты RADIUS в другие системы защиты. Серверы защиты RADIUS и соответствующие клиенты должны игнорировать нестандартные пары «атрибут/значение», созданные конкретными поставщиками.

Связь между NAS и сервером RADIUS основана на протоколе UDP. В целом считается, что протокол RADIUS не имеет отношения к подключению. Все вопросы, связанные с доступностью сервера, повторной передачей данных и отключениями по истечении времени ожидания, контролируются устройствами, работающими под управлением протокола RADIUS, но не

самим протоколом передачи. Протокол RADIUS основан на технологии клиент-сервер. Клиентом RADIUS обычно является NAS, а сервером RADIUS считается «демон», работающий на машине UNIX или NT. Клиент передает пользовательскую информацию на определенные серверы RADIUS, а затем действует в соответствии с полученными от сервера инструкциями. Серверы RADIUS принимают запросы пользователей на подключение, проводят идентификацию пользователей, а затем отправляют всю конфигурационную информацию, которая необходима клиенту для обслуживания пользователя.

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

3.3.2 Свойства и возможности протокола RADIUS

RADIUS поддерживает следующие возможности сервера защиты:

- Пакеты UDP. Для связи RADIUS между сервером доступа и сервером защиты используется протокол UDP и UDP-порт 1812, официально назначенный для этого. Некоторые реализации RADIUS используют UDP-порт 1645. Использование UDP упрощает реализацию клиента и сервера RADIUS.
- Объединение аутентификации и авторизации и выделение аудита. Сервер RADIUS получает запросы пользователя, выполняет аутентификацию и обеспечивает клиенту информацию о конфигурации. Аудит выполняется сервером аудита RADIUS.
- Шифрование паролей пользователей. Пароли, содержащиеся в пакетах RADIUS (а это только пользовательские пароли), шифруются посредством хэшированияMD5.
- Аутентификация PAP и CHAP. Обеспечивает управление аутентификацией с помощью средств вызова/ответа PAP и CHAP, а также посредством диалога начала сеанса и ввода пароля наподобие входа в систему UNIX.
- Защита глобальной сети. Обеспечивает поддержку средств AAA удаленного доступа для серверов доступа многих поставщиков, поддерживающих клиентов RADIUS. Дает возможность централизовать управление удаленным доступом.

- Поддержка ряда протоколов, обеспечивающих терминальный доступ к серверу защиты RADIUS.

- Функция обратного вызова. Данная функция возвращает телефонные вызовы, заставляя сервер доступа звонить соответствующему пользователю, что может дать дополнительные гарантии защиты пользователям, использующим доступ по телефонным линиям.

- Расширяемость. Все транзакции предполагают использование пар «атрибут/значение» переменной длины. Новые атрибуты могут быть добавлены в существующие реализации протокола.

- Гарантированная сетевая защита. Аутентификация транзакций между клиентом и сервером защиты RADIUS предполагает использование общего секретного значения.

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). Как показано на рис. 3.25, при попытке подключиться к серверу сетевого доступа, имеющему конфигурацию клиента RADIUS, выполняются следующие шаги:

– Пользователь инициализирует запрос аутентификации PPP к серверу сетевого доступа.

– У пользователя запрашивается имя пользователя и пароль

– Сервер сетевого доступа посылает серверу защиты RADIUS пакет Access-Request, содержащий имя пользователя, шифрованный пароль и другие атрибуты.

Рис. 3.25. Процесс аутентификации и авторизации RADIUS

– Сервер защиты RADIUS идентифицирует клиента-инициатора, выполняет аутентификацию пользователя, проверяет параметры авторизации пользователя и возвращает один из следующих ответов:

Access-Accept – пользователь аутентифицирован.

Access-Reject – пользователь не аутентифицирован, и сервер сетевого доступа либо предлагает ввести имя пользователя и пароль снова, либо запрещает доступ.

Access-Challenge – вызов является дополнительной возможностью сервера защиты RADIUS.

– Сервер сетевого доступа обращается к параметрам аутентификации, разрешающим использование конкретных служб.

– Ответ Access-Accept или Access-Reject связывается с дополнительными данными (парами «атрибут/значение»), используемыми для сеансов EXEC и авторизации. Процесс аутентификации RADIUS должен быть завершен до начала процесса авторизации.

– Сервер защиты RADIUS может периодически посылать пакеты Access-Challenge серверу сетевого доступа, чтобы потребовать повторного введения имени пользователя и пароля пользователем, информировать о состоянии сервера сетевого доступа или выполнить какие-то другие

действия, предусмотренные разработчиками сервера RADIUS. Клиент RADIUS неможетпосылатьпакеты Access-Challenge.

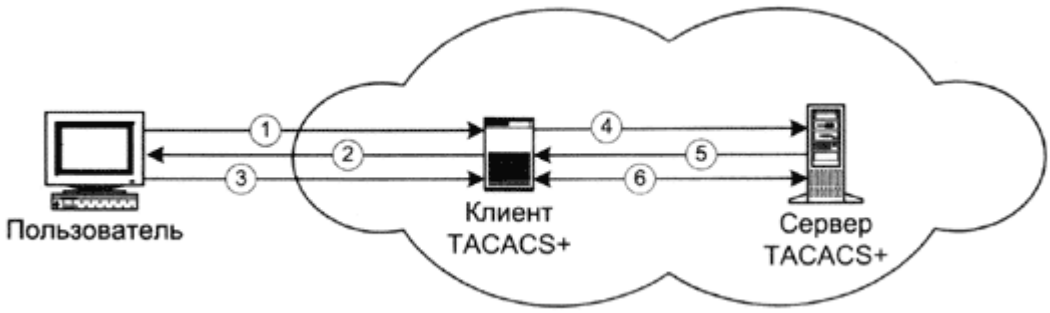

Рис. 3.26. Взаимодействие между пользователем и системой TACACS+

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.

3.3.4 Процесс аудита на базе протокола RADIUS

Протокол RADIUS был усовершенствован с тем, чтобы обеспечить доставку информации аудита от клиента RADIUS серверу аудита RADIUS через UDP-порт 1813. Клиент RADIUS отвечает за отправку информации аудита пользователя соответствующему серверу аудита RADIUS, для чего

используется пакет типа Accounting-Request (аудит-запрос) с соответствующим набором пар «атрибут/значение». Сервер аудита RADIUS должен принять запрос аудита и вернуть ответ, подтверждающий успешное получение запроса. Дляэтогоиспользуетсяпакеттипа Accounting-Response (аудит-ответ).

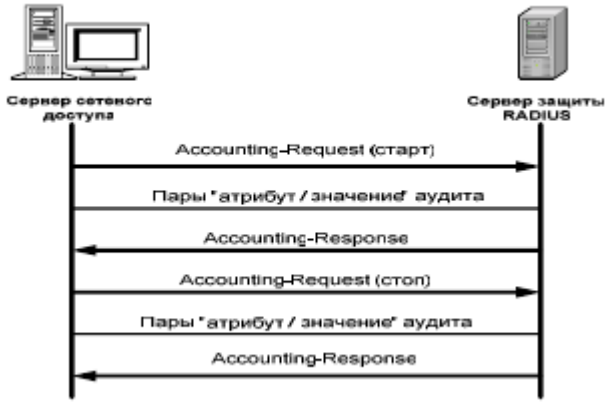

Рисунок 3.26. Процесс аудита RADIUS

Как видно из рис. 3.25, при попытке подключиться к серверу сетевого доступа, имеющему конфигурацию клиента RADIUS, выполняются следующие шаги:

1) После исходной аутентификации сервер сетевого доступа посылает серверу защиты RADIUS старт-пакет Accounting-Request.

2) Сервер защиты RADIUS подтверждает получение старт-пакета, возвращая пакет Accounting-Response.

3) По окончании использования сервиса сервер сетевого доступа посылает стоп-пакетAccounting-Request; в этом пакете указывается тип предоставленного сервиса и дополнительные статистические данные.

4) Сервер защиты RADIUS подтверждает получение стоп-пакета, возвращая пакет Accounting-Response.

Сравнение возможностей протоколов TACACS и RADIUS:

Хотя TACACS и RADIUS очень похожи по своим функциональным возможностям, они имеют несколько важных отличий, указанных в таблице 3.1.

Таблица 3.1 – Сравнение протоколов TACACS+ и RADIUS

Функциональныевозможности	TACACS+	RADIUS
Поддержка AAA	Разделениетрехсервисов AAA	Аутентификация и авторизация объединяются, а аудит отделяется
Транспортныйпротокол	TCP	UDP
Обмен сообщениями между клиентом и сервером защиты	двунаправленный	однонаправленный
Поддержка протоколов удаленного и межсетевого доступа	Полнаяподдержка	Отсутствуетподдержка NetBEUI
Целостностьданных	Шифруетсявесьпакет TACACS	Шифруютсятолькопаролипользователей
Возможностьперенаправлениязапроса	нет	есть

Помимо этого TACACS+ поддерживает двунаправленный поток вызовов/ответов между серверами сетевого доступа подобно тому, как это сделано в CHAP. RADIUSподдерживает однонаправленный вызов/ответ от сервера защиты RADIUS к клиенту RADIUS.

Целостность данных. TACACS+ предполагает шифрование содержимого пакетов. RADIUS предусматривает шифрование только атрибутов пароля в пакете Access-Request. Это означает лучшую защищенность TACACS+.

Кроме того, сравнивая TACACS+ и RADIUS, можно отметить следующие:

– Возможности настройки. Гибкость протокола TACACS+ обеспечивает возможность настройки множества параметров в соответствии с требованиями отдельных пользователей. Из-за недостаточной гибкости RADIUS многие возможности, доступные в рамках TACACS+, при использовании RADIUS недоступны (например, каталоги сообщений). Однако, RADIUS поддерживаетвозможностьизмененияналоровпар «атрибут/значение».

– Процесс авторизации. При использовании TACACS+ сервер принимает или отвергает запрос аутентификации на основании данных пользовательского профиля. Клиенту (NAS) содержимое пользовательского профиля остается неизвестным. В системе RADIUS все посылаемые с ответом атрибуты пользовательского профиля передаются серверу сетевого доступа. Сервер принимает или отвергает запрос аутентификации на основании полученных им значений атрибутов.

По большому счету протокол RADIUS не поддерживает авторизацию. То есть RADIUS есть смысл использовать только там, где заранее известно какой сервис предоставляет конкретный RADIUS-клиент. У TACACS+ заложена поддержка авторизации. Но следует отметить, что количество авторизуемых сервисов довольно ограничено в текущей. То есть для доступа к какому-либо сервису RADIUS обрабатывает один запрос (аутентификацию - запрос, ответ), а TACACS+ - два (аутентификацию и авторизацию), но при этом при использовании TACACS+ есть возможность получить доступ к другому сервису.

– Аудит. Аудит TACACS+ предполагает использование ограниченного числа информационных полей. Аудит RADIUS может предоставить больше информации, чем можно получить из записей аудита TACACS, что является главным преимуществом в сравнении с TACACS+.

– Возможность перенаправления запроса. В TACACS+ такая возможность просто отсутствует. RADIUS-протокол же имеет такую возможность. Это очень существенное достоинство этого протокола, в случае если есть представительства оператора IP-телефонии в других регионах. В этом случае клиент, находясь в другом регионе, набирает код доступа (номер и пин-код). Далееместный RADIUS-серверперенаправляетзапрос в соответствующийрегион.

Происходит аутентификация, и ответ отправляется назад. Таким образом, RADIUS позволяет проектировать гибкую распределенную RADIUS схему. Следовательно, RADIUS-клиент на любой запрос должен дожидаться ответа от сервера в течение некоторого времени (timeout'a) и в случае отсутствии оного перепослать пакет еще раз. TACACS+ клиент тоже должен дожидаться всегда ответа от сервера, но в отличии от RADIUS-клиента, в случае отсутствия ответа, пакет еще раз не посылается. Гарантия доставки обеспечивается тем, что для обработки какого-либо запроса TACACS+ сервер и клиент должны установить TCP-соединение (даже если весь процесс будет состоять из посылки и приема 2-ух небольших пакетов), а с точки зрения времени это довольно длительный процесс (по этой причине TACACS+ по определению относительно медленен). На основании этого, можно сказать, что RADIUS будет более эффективен в сетях, где процент потерянных пакетов менее 5-10 %; в других сетях лучше использовать TACACS+. Именно по этой причине в сетях IP-телефонии, где необходимо быстродействие применяется, как правило, протокол RADIUS.

Технические несоответствия с теоретическими характеристиками протоколов TACACS и RADIUS

Различий между протоколами RADIUS и TACACS+ достаточно много, но выполняемые ими функции, по сути, одинаковы. Протокол RADIUS, являющийся стандартом, использует на транспортном уровне протокол UDP. Протокол же TACACS+, являясь частной разработкой, применяет на транспортном уровне протокол TCP. Протокол RADIUS хорошо работает

только в IP-средах, тогда как протокол TACACS+ полезен в многопротокольных средах. В настоящее время протоколом RADIUS поддерживается больше количество атрибутов, и он позволяет передавать клиенту и серверу больше информации, чем протокол TACACS+. Наконец, RADIUS шифрует только пароль, пересылаемый между клиентом и сервером, тогда как TACACS+ шифрует всю пересылаемую информацию.

Если сеть в значительной степени гетерогенна, то лучше всего выбрать протокол RADIUS, так как его поддерживают многие поставщики. Если сеть использует главным образом устройства компании Cisco, то, скорее всего, правильным решением будет применение протокола TACACS+.

Часто возникает задача проверить пользователя до предоставления ему доступа к определенным ресурсам. Такая проверка называется «перехватывающая аутентификация» (cut-throughproxy).

Этот сервис использует инфраструктуру AAA (Authentication, Authorization, Accounting).

TACACS+ – протокол, работающий по TCP/49. Имеет отдельные запросы на аутентификацию, авторизацию и учет. За счет отдельного запроса на авторизацию позволяет учитывать и проверять все вводимые команды. Не расширяемые параметры, слабый «учет». Как правило, используется для административного доступа.

RADIUS – стандартный протокол. Работает по UDP/1645,1646 или UDP/1812,1813. Один новый, другой старый стандарт. Первый порт используется для аутентификационного запроса и ответа, в котором заодно передаются авторизационные атрибуты пользователя, если есть. Второй – для учета (как правило, при помощи RADIUS учитывают переданные пакеты, считают трафик и некоторые системные параметры)

Таким образом, с аутентификацией все просто: если более ничего не указывать, то пользователю, а вернее, ip-адресу его компьютера, будет можно все.

Гораздо более интересный момент – авторизация, то есть ограничение прав пользователя.

По протоколу TACACS можно ограничивать доступ к определенным ресурсам (сетям и протоколам), однако формат такого ограничения весьма странный: на сервере описываются все такие протоколы и сети, и обращение с ASA на сервер идёт всякий раз, когда появляется ранее не изученный пакетик.

Для этого надо отдельно писать команду для авторизации. Можно использовать тот же список доступа, который был использован для аутентификации, а можно написать новый.

Проще использовать протокол RADIUS, у которого предусмотрена возможность в атрибутах пользователя передавать строки списка доступа, который применяется непосредственно к пользователю. Никаких дополнительных команд писать не надо. Правда, такая возможность есть у ciscoACS (AccessControlServer). Доподлинно я не знаю, есть ли бесплатные и свободные реализации сервера RADIUS, умеющие также передавать строчки.

Понятно, что учет нельзя делать на сервер LOCAL (локально), а также на сервер LDAP. На TACACS передается не так много атрибутов, как хотелось бы, а вот RADIUS подходит лучше всего. Причем использовать можно любой. В частности я, когда настраиваю аутентификацию и авторизацию через LDAP для учета использую IAS (это как раз и есть RADIUS, встроенные в сервер Windows). Отчеты, правда, с него снимать не так удобно, как с ACS или других, более приспособленных решений.

Внешняя аутентификация. В данном случае циска не знает пользователей в логин всегда сверяется с внешним сервером по протоколу TACACS или RADIUS (более распространено). Минусы очевидны: есть необходимость в дополнительной организации и поддержке RADIUS-сервера, а при его недоступности доступ в сеть будет запрещён. Однако при масштабировании системы, добавлении новых серверов доступа или резервных серверов RADIUS

ВЫВОДЫ И ПРЕДЛОЖЕНИЯ

По моему мнения в настоящее время в системе ip-телефонии имеются определенные уязвимости, что несет за собой плохое качество связи при передаче логоса. Например:

Плохой Интернет. Возможно, это самая главная проблема, которая делает Интернет-звонки ненадежными и неудовлетворительными. Интернет всегда влияет на связь, поэтому не рассчитывайте на хорошее качество, если он у вас медленный или ненадежный.

Интернет-провайдеры не заботятся о голосовом трафике на их сетях, их настройки рассчитаны на простое просматривание веб-страниц. Потоковое видео и аудио требует быстрого отклика и больших доступных ресурсов, что будет стоить провайдерам намного дороже, и часто такой трафик для них убыточен.

Оборудование. Может это удивительно, но оборудование тоже может отрицательно влиять на качество IP-телефонии. Некоторые модели слишком медленные, чтобы без проблем передавать трафик в реальном времени вместе с обычным для веб-серфинга. В некоторых случаях такие модели могут вызывать зависание, что выражается в задержках и потерях IP-пакетов. Это очень разочаровывает, так как роутер – это последнее средство, которое может обычно попасть под подозрение, к тому же оборудования в процессе ip-телефонии имеют довольно высокую финансовую стоимость.

ЛИТЕРАТУРА

1.Балдин К.В. Информационные системы в экономике. Издательско-торговая корпорация «Дашков и Ко»

2. Издательство: Макс Пресс. Интернет-телефония: протокол SIP и его применения

3. Гвоздева Т.В., Баллад Б.А. Проектирование информационных систем.

4. Голицына О.Л., Попов И.И. Информационные системы

5. Синченков Ю.Б. Моделирование бизнес-процессов с AllFusion PM. Издательство Диалог-МИФИ

6. Шон Харрис «CISSP All-In-One Exam Guide» 5-е издание.

7. Шуремов Е.Л., Чистов Д. В., Лямова Г. В. Информационные системы управления предприятиями

8. Издательство: Вильямс. Основы организации сетей Cisco. Том 1.

9. Cisco Systems. Руководство по сдачи экзамена CCNA: Voice

10. Cisco Systems. Руководство по сдачи экзамена CCNP: Voice

11. Веб-страница: *www.ru.wikipedia.org*

12. Веб-страница: *www.cisco.com*

XÜLASƏ

Təqdim edilmiş dissertasiya materialların xülasəsində İP-telefoniya mövzusunda seçilmiş məsələlərə baxılmışdır.Dissertasiyada İP-telefoniyanın texniki realizasiyasının şərtləri, elmi və texniki problemlər, onların əmələ gəlmə səbəbləri və mümkun olan həlli yolları, həmcinin İP-telefoniyanın kiçik və orta biznesdə tətbiqinin iqtisadi səmərəliliyinin effektivliyi göstərilmişdir. İP-telefoniya siqnalların rəqəmsal emalının metodlarını və vasitələrin inteqrasiyasında telefon rabitəsinin xüsusi sahəsini, danışıq texnologiyalarını, yüksək texnologiyaların əsasında hesablama vəsaitlərin idarə edilməsini təsvir edir. İqtisadı nöqtəyi nəzərdən bu çox əlverişli sistem olaraq onun tətbiqi şirkətlərin işçilərinin danışıq kommunikasıyalarını asanlaşdırır və bu da öz növbəsində biznesə maliyyə qazancı gətirir.Bu sahə daimi olaraq qəzet və jurnallarda dərc edilmiş məqalələrdə göstərilən kimi nəik ki böyük kommersiya maraqları, həmcinin maraqlı elmi tətqiqatların və mühəndisi işləmələrin sahəsidir.

SUMMARY

In conclusion, materials presented in the dissertation show a great topic of IP telephony. There are technical realization of IP telephony, scientific and technical issues, ways to get around it, as well as, economic benefits of having IP telephony, using this system in small and middle sizes businesses. IP telephony offers special field of communications, which integrates methods of digital data handling, speech technologies, managing of computational resources based on high technologies. From the economical point of view integrating this kind of system is beneficial in a means of business and financials, because it could make communications between colleagues much easier. It is a field of many commercial interests, which we can see from articles in magazines and newspapers, at the same time there are scientific researches, engineering development, beneficial and perspective field for students and young engineers.

Р Е Ф Е Р А Т

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В БИЗНЕСЕ

Информацию на сегодняшний день рассматривают как один из основных ресурсов развития общества, а информационные системы и технологии как средство повышения производительности и эффективности работы людей.

Наиболее широко информационные системы и технологии применяются в производственной, управленческой и финансовой деятельности, хотя наблюдаются подвижки в сознании людей, занятых и в других сферах. Это определило угол зрения, под которым будут рассмотрены основные области их применения. Главное внимание следует уделять рассмотрению информационных систем и технологий с позиций использования их возможностей для повышения эффективности труда работников информационной сферы производства и поддержки принятия решений.

В современных условиях быстрое наращивание объемов бизнеса компании за счет расширения филиальной сети, слияний и поглощений приводит к тому, что телекоммуникационная инфраструктура предприятий в конечном итоге образует множество разнородных АТС и телефонных систем. Это делает актуальной необходимость перехода к более современным системам.

Внедрение IP-телефонии в компаниях, как неотъемлемой части унифицированных коммуникаций, повышает эффективность ведения бизнеса и позволяет осуществлять многие операции, которые невозможно применять в традиционной телефонии.

Цель диссертации-выявление основной идеи, связанной с использованием информационных систем и информационных технологий, на примере IP телефонии, а также ее применение в бизнесе.

В первой главе рассмотрены информационные системы, в том числе осуществление поиска, обработки и хранения информации, которая

накапливается в течение большого периода времени, хранение данных разной структуры, анализ и прогнозирование потоков информации, исследование способов представления и хранения информации, а также построение процедур и технических средств для их реализации.

Важное внимание уделяется структуре информационной системы. Структуру информационных систем составляют совокупность отдельных её частей, называемых подсистемами.

Рассмотрены также классификационные признаки систем. Согласно общепринятой классификации информационные системы подразделяются на:

- по масштабам применения – настольные и офисные;
- попризнакуструктурированностизадач;
- пофункциональномупризнаку;
- пооперативностиобработкиданных;
- постепениавтоматизации;
- по характеру использования вычислительных ресурсов;
- поконцепциипостроения.

Во второй главе рассматриваются понятия системы IP телефонии, а также процессы происходящие в ней. Под IP-телефонией подразумевается голосовая связь, которая осуществляется по сетям передачи данных, в частности по IP-сетям (IP-InternetProtocol). На сегодняшний день IP-телефония все больше вытесняет традиционные телефонные сети за счет легкости развертывания, низкой стоимости звонка, простоты конфигурирования, высокого качества связи и сравнительной безопасности соединения.

IP-телефония, по сути, является способом организации телефонной связи с использованием сети передачи данных для передачи голоса. Преимущества такой организации телефонной связи очевидны, и главное из них-существенное снижение затрат на звонки между офисами, расположенными в разных городах. Кроме этого, данный подход позволяет ввести единый номерной план для всей

организации, когда нет необходимости запоминать телефонные коды городов, в которых расположены филиалы компании.

Отмечая экономическую выгоду от внедрения систем IP телефонии, можно остановиться на примере банковской структуры. Каждый работник банка оснащается телефоном и закрепленным за ним уникальным номером. Приэтомможнополучитьследующиевозможности:

- каждый работник головного офиса и филиалов имеет возможность позвонить любому другому сотруднику;
- каждый работник головного офиса и филиалов имеет возможность воспользоваться всеми услугами IP телефонии. К примеру, просматривать исходящие и набранные звонки, иметь доступ к корпоративной директории, пользоваться поиском номеров сотрудников на основе таких факторов как имя, фамилия, должность, отдел и т.д. Есть возможность запуска любых Java приложений.
- контроль доступа осуществляется администраторами, которые могут контролировать “callflow” любого телефона и в любом направлении. К примеру, можно закрепить исходящие городские звонки с филиала “А” в филиал “Б”. Можно контролировать возможность исходящих звонков по городу, региону и миру, разрешить или запретить звонки через сеть GSM операторов.

Система IP телефонии снабжает нас гибкостью, повышает производительность труда, также имеет множество других экономических преимуществ.

В третьей главе рассматривается техническая сторона внедрения системы телефонии, варианты и сценарии систем, а также типы угроз и методы безопасности.

Подробно описываются возможности и архитектура протоколов телефонии, таких как: H.323, SIP, MGCP. Также отмечены сценарии подключения систем телефонии, среди которых можно отметить следующие:

- «компьютер-компьютер»;

- «компьютер-телефон»;
- «телефон-телефон».

Отдельное внимание уделяется типам угроз и внедрению безопасности.

Конфиденциальность и безопасность являются обязательными требованиями для любой телефонной сети. В настоящее время удалось обеспечить определенный, хотя и далекий от совершенства уровень безопасности в традиционных сетях. В диссертации также рассматриваются методы криптографической защиты информации, методы шифрования, аутентификации, использования метода секретных ключей, защита от прослушивания, проверка прав и доступ к ресурсам и т.д.

В заключении, представленный в диссертации, материал, затрагивает избранные вопросы огромной темы - IP-телефонии. В диссертации показана условия технической реализации IP-телефонии, научные и технические проблемы, причины их появления и возможные пути решения, также экономические выгоды от внедрения IP-телефонии, использование данной системы в среднем и малом бизнесе. IP-телефония представляет собой специальную область телефонной связи, интегрирующая методы и средства цифровой обработки сигналов, речевых технологий, управления вычислительными ресурсами на базе высоких технологий. С экономической точки зрения это очень выгодная система, внедрение которой может упростить речевые коммуникации работников компании, что несет за собой финансовую выгоду для бизнеса. Эта область не только крупных коммерческих интересов, о чем постоянно публикуются статьи в газетах и журналах, но и увлекательных научных исследований и инженерных разработок, благодатная и благодарная нива для студенчества и молодых инженеров.