МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Кафедра Телекоммуникационные системы

«ДОПУЩЕН К ЗАЩИТЕ»

Зав.кафедрой _____
(ученая степень, звание, Ф.И.О.)

_____ «____» _____ 201___ г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Исследование способов обеспечения безопасной работы в технологии VoIP

Специальность Радиотехника, электроника и телекоммуникации

Выполнил(а) Рахимжанов А.П. (ФИО) Группа АТС-12-5

Научный руководитель к.т.н., ст. преп. Ефремова Ю.И.
(ученая степень, звание, Ф.И.О.)

_____ «____» _____ 201___ г.
(подпись)

Консультанты:

по экономической части:

доцент каф. ЭО и УП Боканова Р.Ш.
(ученая степень, звание, Ф.И.О.)

_____ «02» июня 2016 г.
(подпись)

по безопасности жизнедеятельности:

ст. преподав. Бегимбетова А.С.
(ученая степень, звание, Ф.И.О.)

_____ «26» мая 2016 г.
(подпись)

по применению вычислительной техники:

к.т.н., ст. преп. Ефремова Ю.И.
(ученая степень, звание, Ф.И.О.)

_____ «04» июня 2016 г.
(подпись)

Нормоконтролер: Дашидова Т.Д., ст. пр-ль
(ученая степень, звание, Ф.И.О.)

_____ «7» июня 2016 г.
(подпись)

Рецензент: _____
(ученая степень, звание, Ф.И.О.)

_____ «____» _____ 201___ г.
(подпись)

Алматы 2016 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Факультет Радиотехники и связи

Кафедра Телекоммуникационных систем

Специальность 5В 07 1900 Радиотехника, электроника и телекоммуникации

ЗАДАНИЕ

на выполнение дипломного проекта

Студенту Рахимжанову Аброру Рарпитаевичу
(ФИО)

Тема проекта Исследование способов обеспечения безопасной работы в технологии VoIP

Утверждена приказом по университету №____ от «__» _____ 201__ г.

Срок сдачи законченного проекта «_____» _____ 201__ г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта):

Длительность действия $T_{пр} = 20$ мс. Скорость передачи данных $R_0 = 64$ кбит/с. Кодеки вокодеров в ТФН $f_{кодек} = 10{,}2$ кГц, $f_{кодек} = 12$ кГц, $f_{кодек} = 16{,}2$ кГц. Средняя длительность сеанса связи абонента $t = 100$ с.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта:

1. Анализ подхода к построению сети IP телефонии
2. VoIP - основной инструмент интернет коммуникации.
3. Информационная безопасность
4. Безопасность VoIP-контента
5. Механизмы и стандарты безопасности
6. Стандарт сетевой безопасности
7. Виртуальные локальные сети (VLAN)

Перечень графического материала (с точным указанием обязательных чертежей): 1. Схема подключения к сетям PSTN и Интернет
2. Архитектура сети, базирующейся на протоколе H.323
3. Архитектура сети, базирующейся на протоколе SIP
4. Архитектура сети, базирующейся на протоколе MGCP
5. VLAN и межсетевое экранирование

Основная рекомендуемая литература:

1. Алмто Р. Основы организации сетей Cisco. Том 1. М.: издательский дом „Вильямс", 2002
2. Алмто В. Основы организации сетей Cisco. Том 2. М: издательский дом „Вильямс", 2002
3. Davidson J. Peters J. Voice over IP Fundamentals - Cisco Press, 2000
4. Б.Я. Рябко, А.Н. Фионов. Криптографические методы защиты информации. Учебное пособие - М. Горячая линия - Телеком, 2009

Консультанты по проекту с указание относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
Безопасн. жизн.	Бокальчук А.	01.04 - 30.04.16	
ВКР	Брыкалова А.С.	01.04 - 25.04.16	
Расчетная часть	Воронкова И.И.	04.05 - 3.06.16	
Экономическая	Воронкова И.И.	01.09 - 06.06.16	

График подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки предоставления научному руководителю	Примечание
1. Система обнаружения и предотвращения вторжений	07.02.2016 - 02.03.2016	
2. Качества обслуживания (QoS)	2.04.2016 - 10.01.16	
3. Принцип ранжирования VoIP-рисков		
4. Расчет производительности из-за доступа	4.03.2016 - 15.03.16	
5. Выбор оптимальной структуры узла доступа с узлом агрегации	20.03.16 - 30.03.16	
6. Расчет числа заявок от абонента группы	01.4.2016 - 7.04.2016	
7. Расчет числа пакетов от абонентов каждой группы	1.05.2016 - 1.05.2016	
8. Расчет финансовых результатов реализации проекта	07.04.2016 - 07.04.2016	
9. Расчет абсолютной величины чистого дохода с учетом дисконтирования	20.04.2016 - 10.05.16	
10. Анализ условий труда	2.04.2016 - 7.04.2016	
11. Расчет искусственного освещения	9.04.2016 - 16.04.2016	
12. Расчет системы кондиционирования	17.04.2016 - 25.04.2016	

Дата выдачи задания «___» _____ 201___ г.

Заведующий кафедрой _____ (_____)
(подпись) (Ф.И.О.)

Научный руководитель
Проекта _____ (_____)
(подпись) (Ф.И.О.)

Задание принял к
исполнению студент _____ (Якушенков В. П.)
(подпись) (Ф.И.О.)

Аңдатпа

Бұл дипломдық жобада, VoIP технологиясында қауіпсіздік тәсілдерді зерттеу сұрақтары талқыланған.

IP-телефония желілерін құру нұсқалары,IP-телефониядағы қауіп түрлері, VoIP технологиясындағы қауіпсіздік тәсілдері қарастырылған.

Есеп бөлімінде оптималдық құрылым жүйесіне түсетін салмақты қарастыра отырып, есеп жүргізілген, әр түрлі топтағы абоненттердің пакеттер саны, байланыс жүйесіндегі уақытша көрсеткішті анықтау, кодектер үшін өткізу жолақтары есептелінген.

Бұл жобаның тиімді екенін экономикалық есептер көрсетеді, өміртіршілік қауіпсіздік шаралары жүргізілді.

Аннотация

В данном дипломном проекте рассмотрены вопросы исследования методов безопасности в технологии VoIP.

Были рассмотрены варианты построения сетей IP-телефонии, типы угроз в IP-телефонии, методы безопасности в технологии VoIP .

В расчетной части произведен расчет оптимальной структуры узла доступа с учетом нагрузки, расчет числа пакетов от абонентов различных групп, определение временных параметров сети доступа, расчет полосы пропускания для кодеков.

Экономические расчеты показывают эффективность предложенного варианта проекта, а меры безопасности жизнедеятельности выполняются.

Annotation

In this thesis project the issues of security research techniques in VoIP technology.

Variants of IP-telephony networks were considered, the types of threats to the IP-telephony, security methods in VoIP technology.

In the calculation of the optimal structure of a calculation based on the access point load, the calculation of the number of packets from the subscribers of the various groups, the definition of temporary access network parameters, calculating bandwidth codec’s.

Economic calculations show the effectiveness of the proposed version of the draft, and health and safety measures are met.

Содержание

	Введение	6
1	Анализ подхода к построению сети IP-телефонии	7
1.1	VoIP - основной инструмент интернет коммуникаций	7
1.2	Информационная безопасность	13
2	Безопасность VolP-контента	18
2.1	Механизмы и стандарты безопасности	18
2.2	Общая оценка	22
2.3	Реализация концепции безопасности	26
2.4	Стандарт сетевой безопасности	27
2.5	Виртуальные локальные сети (VLAN)	27
2.6	Шифрование	29
2.7	Аутентификация	29
2.8	Средство межсетевого экранирования	30
2.9	Системы обнаружения и предотвращения вторжения	31
2.10	NAT и STUN	32
2.11	Качество обслуживания (Quality-of-service – QoS)	32
2.12	Удаленное управление	33
2.13	Принципы минимизации VoIP-рисков	33
3	Расчет производительности узла доступа	34
3.1	Выбор оптимальной структуры узла доступа с учетом нагрузки	36
3.2	Расчет числа заявок от абонента группы	38
3.3	Расчет числа пакетов от абонентов каждой группы	39
3.4	Требования к производительности мультисервисного узла доступа	43
3.5	Определение временных параметров сети доступа	45
4	Технико-экономическое обоснование	50
4.1	Резюме	50
4.2	Краткое описание проекта	50
4.3	Финансовый план	51
4.4	Расчет финансовых результатов реализации проекта	55
4.5	Расчет абсолютной величины чистого дохода с учетом дисконтирования	56
4.6	Ожидаемые результаты внедряемого проекта	58
5	Безопасность жизнедеятельности	59
5.1	Анализ условий труда	59
5.2	Расчет естественного освещения	63
5.3	Расчет системы кондиционирования	68
5.4	Выводы по пятой главе	71
	Заключение	72
	Список литературы	73
	Приложение А Технические расчеты	74

Введение

В настоящее время наблюдается бурное развитие сети Интернет, других сетей, основанных на протоколе IP, в том числе сетей IP – телефонии. Глобальная сеть Интернет прочно входит в жизнь людей, предоставляя множество услуг: от новостей и почты до многопользовательских конференций и виртуальных магазинов.

На данном этапе трудно представить успешную работу какой-либо организации, использующей компьютерную технику для ведения своих дел, без локальной сети. Крупные компании создают свои сети, располагающиеся в нескольких зданиях или даже городах.

Сегодня трудно переоценить значение информации и значение обеспечения ее безопасности. Ведь для того, чтобы заполучить важные сведения, взломщику уже нет необходимости физического доступа к ней, как это было раньше. При определенных знаниях, навыках и обладая комплексом современных программно-аппаратных средств, можно осуществить хищение (или копирование) важной информации не выходя из дома.

IP-телефония, будучи результатом слияния технологий обычной телефонии с коммутацией каналов и пакетных IP-сетей, впитала в себя и совокупность их проблем с точки зрения обеспечения безопасности. От обычной телефонии ей, прежде всего, досталась кража сервиса (правда с известными поправками), а от IP-сетей все разнообразие атак компьютерного мира: от DoS-атак на диспетчеры сети IP-телефонии до перехвата информационных пакетов с целью прослушивания или модификации.

Все многообразие угроз сетям IP-телефонии, в конечном счете, можно разделить на две группы: угрозы, возникающие в результате несанкционированного доступа к ресурсам сети и угрозы, связанные с передачей информации непосредственно по каналам. Для решения проблем первой группы необходим, прежде всего, устойчивый к взлому механизм аутентификации, авторизации и учета. Другие проблемы способен в какой-то мере на первый взгляд разрешить верно подобранный алгоритм шифрования или даже некая концепция построения всей сети IP-телефонии, способная в частности реализовать данный алгоритм шифрования.

В работе определяется один из вариантов построения современной безопасной VoIP-сети, приводится анализ типов угроз и конкретные решения как с ними бороться. Как результат, производится выработка рекомендации по обеспечению безопасности в сетях IP-телефонии и дается сценарий безопасного VoIP-соединения.

1 Анализ подхода к построению сети IP-телефонии

1.1 VoIP - основной инструмент интернет коммуникаций

VoIP (Voice over Internet Protocol) или IP-телефония - это технология, которая обеспечивает передачу голоса в сетях с пакетной коммутацией по протоколу IP, частным случаем которых являются сети Интернет, а также другие IP - сети (к примеру, выделенные цифровые каналы). Для взаимосвязи сети Интернет (IP - сети) с телефонной сетью общего пользования PSTN (Public Switched Telephone Network), которая относится к глобальным сетям с коммутацией каналов, применяются специальные аналоговые VoIP-шлюзы. Нужно подметить, что сети Интернет через цифровые шлюзы VoIP связаны с цифровыми телефонными сетями ISDN (Integrated Services Digital Network). Кроме того, интеграция VoIP в сети сотовой связи является практически неминуемым процессом, интеграция даст наиболее низкую по сравнению с традиционной сотовой телефонией стоимость дискусии.

На нынешний день доступ в Интернет возможен непосредственно с мобильных телефонов, которые поддерживают технологии: CSD (Circuit Switched Data или GSM Data), GPRS (General Packet Radio Service), EDGE (Enhanced Data rates for Global Evolution), CDMA (Code Division Multiple Access), EV-DO (Evolution-Data Optimized), которые гарантируют широкий спектр услуг "Мобильный Интернет" и WAP. Необходимо отметить, что в мобильной связи уже внедряются новые технологии беспроводного широкополосного доступа в Интернет на базе технологии связи 4G).

В настоящее время к сетям PSTN и ISDN подключены центры коммутации сотовой связи (сотовые сети разных операторов соединены между собой), что обеспечивает звонки с сотовых телефонов на стационарные телефоны (PSTN или ISDN) и наоборот. Свойственным для сетей 3G мобильной связи является скоростная беспроводная передача данных и мощные магистральные сети пакетной коммутации. В связи с тем, что сети PSTN связаны с сетями Интернет и сетями сотовой связи, может быть обеспечена передача голосовых сигналов между этими сетями.

Голосовой сигнал из канала VoIP может непосредственно поступать на IP-телефон, подключенный к IP-сети или маршрутизироваться на мобильный телефон мобильного оператора, или на аналоговый телефон, подключенный к обычной телефонной сети PSTN, или на цифровой телефонный аппарат, подключенный к цифровой сети с интеграцией услуг ISDN.

Таким образом, IP-телефония обеспечивает передачу голосовых сигналов с компьютера на компьютер, с компьютера на телефон (аналоговый телефон, цифровой телефон, IP-телефон, мобильный телефон) и с телефона на телефон. Звонки исполняются через провайдера услуг VOIP. Качество передачи голоса зависит от VoIP-провайдера и метода подключения к Интернету.

Одно из превосходств IP-телефонии - это экономия финансовых средств на ведение международных и междугородних телефонных переговоров за счет того, что значительную часть расстояния между абонентами голосовой сигнал в цифровом виде (в сжатом состоянии) проходит по сетям пакетной коммутации (по сети Интернет), а не по телефонным сетям с коммутацией каналов. В настоящее время IP-телефония обеспечивает самые дешевые или бесплатные междугородние и международные звонки нужно лишь только оплатить примененный трафик Интернет-провайдеру.

На рисунке 1.1 изображена упрощенная схема сети со шлюзами, установленными в разных городах и подключенных к сетям PSTN и Интернет.

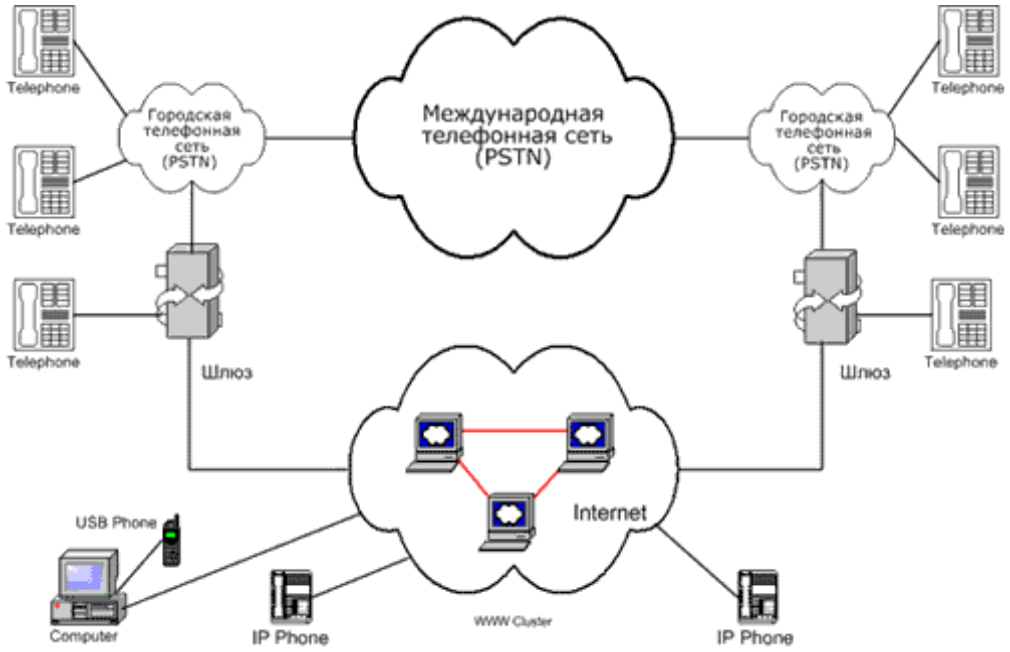

Рисунок 1.1 – Схема подключения к сетям PSTN и Интернет

Как следует из схемы сети абоненты различных городов с обыкновенных телефонов, подключенных к городской сети, имеют все возможности общаться между собой через международную телефонную сеть или сеть Интернет. Однако цена переговоров через Интернет существенно ниже, чем через международную телефонную сеть.

Кроме того, абоненты разных городов могут вести переговоры, используя компьютер (с микрофоном и наушниками или с USB VoIP телефоном) или IP-телефон, подключенный к сети Интернет. Для работы VoIP потребуется широкополосное подключение к Интернету: по выделенной линии, по локальной сети, по технологии xDSL, с использованием спутникового доступа, мобильного CDMA или любое другое высокоскоростное постоянное подключение.

В настоящее время существуют следующие VoIP-сервисы:

- IP-телефония по карточкам, которые продаются в магазинах для звонков с обычного телефона;
- компьютерная VoIP (IP-телефония), в которой используется специальная программа, работающая на ПК (программный телефон VoIP);
- телефонная VoIP (IP-телефония), в которой обычный телефонный аппарат подключается к специальному адаптеру, имеющему выход в Интернет или в которой IP-телефоны (аппаратные VoIP телефоны) подключаются к Интернет через провайдера.

1.1.1 Варианты построения сетей IP-телефонии

Более известным считается подход, предложенный Международным союзом электросвязи (ITU) в Рекомендации H.323. Сети, построенные на базе протоколов H.323, нацелены на интеграцию с телефонными сетями и имеют все шансы рассматриваться как наложенные на сети передачи данных сети ISDN. В частности, операция установления соединения в таких сетях IP-телефонии основывается на Рекомендации ITU Q.931 и практически идентична данной процедуре в сетях ISDN.

Описанный вариант построения сетей IP-телефонии более идет для операторов телефонной связи, желающих использовать сети с маршрутизацией пакетов IP для предоставления услуг междугородной и международной связи.

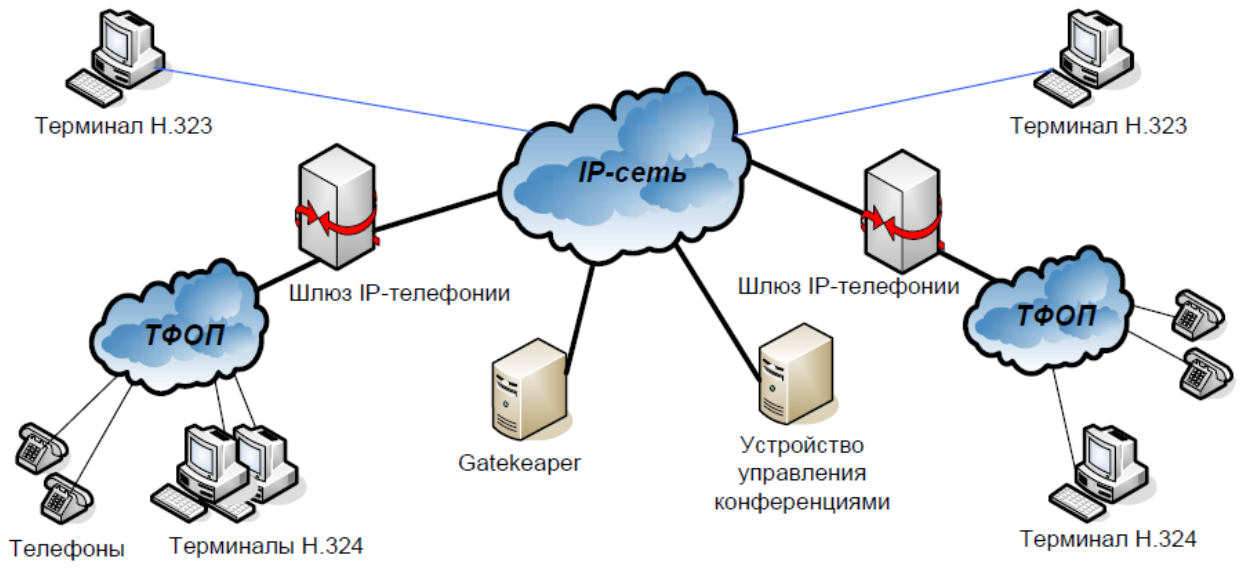

Рисунок 1.2 – Архитектура сети, базирующейся на протоколе H.323

При этом IP-телефония станет для них главной предоставляемой услугой. Протокол RAS, входящий в комплект протоколов H.323, гарантирует операторам связи высочайший степень контроля за использованием сетевых

ресурсов, поддержку аутентификации пользователей и начисление оплаты за предоставленные услуги. Кроме базового вызова в сетях, построенных на базе протоколов H.323, предусмотрено предоставление дополнительных услуг в соответствии с Рекомендациями ITU H.450.x.

Второй подход, соединенный с внедрением протокола SIP(Session Initiation Protocol), нацелен на интеграцию услуги передачи речевого трафика по IP-сетям с остальными услугами Internet. Данный подход, порекомендованный телекоммуникационной стандартизирующей организацией IETF в документе RFC 2543, является гораздо наиболее простым для реализации в сравнении с H.323, но меньше подходит для организации взаимодействия с телефонными сетями.

В основном это связано с тем, что сервер SIP не сохраняет сведений о текущих соединениях (Stateless), то время как узлы ТфОП напротив - сохраняют информацию обо всех установленных соединениях (Statefull). Кроме того, сигнальный протокол SIP, базирующийся на основе протокола HTTP (RFC 2068), плохо согласуется с системами сигнализации, используемыми в ТфОП.

Данный вариант больше подходит для поставщиков услуг Интернет для предоставления еще одной услуги - Интернет-телефонии. При этом данная услуга будет являться всего лишь небольшой частью пакета услуг, и станет предоставляться, например, по фиксированным тарифам, при этом будет использоваться максимально упрощенная схема управления услугами.

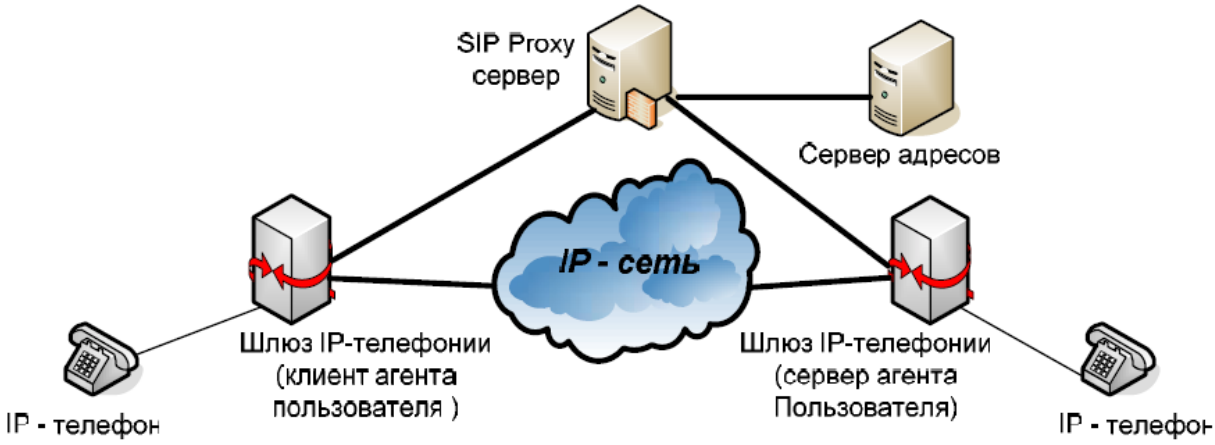

Рисунок 1.3 – Архитектура сети, базирующейся на протоколе SIP

Еще один подход, связанный с декомпозицией шлюзов, подразумевает разбиение шлюзов на главные многофункциональные блоки: шлюз - MG (Media Gateway), устройство управления шлюзом - CA (Call Agent) и сигнальный шлюз - SG (Signalling Gateway), и определение интерфейсов между блоками. Целый интеллект декомпозированного шлюза: обработка

сигнальной информации и логика контроля ресурсов - сосредоточен в устройстве управления. Сами шлюзы лишь выполняют функции преобразования речевой информации, поступающей со стороны ТФОП в вид пригодный для передачи по сетям с маршрутизацией пакетов IP: кодирование и упаковка речевой информации в пакеты RTP/UDP/IP, а также обратное преобразование. Один контроллер шлюзов СА управляет одновременно несколькими шлюзами. Сигнальный шлюз выполняет функции STP, транзитного пункта сигнализации. Такое решение гарантирует высокую степень масштабируемости и простоту эксплуатации сети. Шлюзы не считаются интеллектуальными устройствами, требуют меньше 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) достаточно хорошо подходит для развертывания глобальных сетей IP-телефонии, приходящих на смену традиционным телефонным сетям. Если распределенный шлюз подключается к ТФОП при помощи сигнализации по выделенным сигнальным каналам (ВСК), то сигнальная информация вместе с пользовательской информацией сначала поступает в транспортный шлюз, а затем передается в устройство управления без посредничества шлюза сигнализации. Одно из основных требований, предъявляемых к протоколу MGCP, состоит в том, что устройства, реализующие этот протокол, должны работать в режиме без сохранения информации о последовательности транзакций между устройством управления и транспортным шлюзом, т.е. в устройствах не требуется реализации конечного автомата для описания этой последовательности. Однако не следует распространять подобный подход на последовательность состояний соединений, сведения о которых хранятся в устройстве управления.

Подчеркнем, что протокол MGCP является внутренним протоколом, поддерживающим обмен информацией между многофункциональными блоками распределенного шлюза. Протокол использует принцип master/slave (ведущий/ведомый), причем устройство управления шлюзами является ведущим, а транспортный шлюз – ведомым, выполняющим команды, поступающие от устройства управления.

Подход на базе протокола MGCP обладает очень важным превосходством перед подходом, предложенным ITU в Рекомендации H.323: поддержка управляющим устройством сети - СА сигнализации ОКС7 и других видов сигнализации, а также прозрачная трансляция сигнальной информации по сети IP-телефонии. В H.323 сигнализация ОКС7, как и любая другая сигнализация, конвертируется шлюзом в сигнальные сообщения H.225.0 (Q.931).

Главным недостатком последнего подхода является незаконченность

стандартов. Функциональные составляющие декомпозированных шлюзов, разработанные различными фирмами-производителями телекоммуникационного оборудования, практически не совместимы. Функции управляющего устройства - CA точно не определены. К недостаткам можно также отнести отсутствие стандартизированного протокола взаимодействия между CA. Кроме того, протокол MGCP является протоколом управления шлюзами, но он не предназначен для управления соединениями с участием терминального оборудования пользователей (IP-телефонами). Это означает, что в сети, построенной на базе протокола MGCP, должен присутствовать Привратник или сервер SIP для управления терминальным оборудованием.

Стоит еще подметить, что в существующих приложениях IP-телефонии: таких как предоставление услуг международной и междугородной связи, применять протокол MGCP не целесообразно, в связи с тем, что подавляющее количество систем IP-телефонии сегодня построено на базе протокола H.323. Оператору придется строить отдельную сеть IP-телефонии, построенную на базе протокола MGCP, что связано со значительными капиталовложениями. В то время как, оператор связи, имеющий оборудование стандарта H.323, может подключиться к существующим сетям IP-телефонии.

Стоит также отметить, что в проекте Рекомендации H.323, версии 4 ITU ввел принцип декомпозиции шлюзов, описанный в последнем подходе.

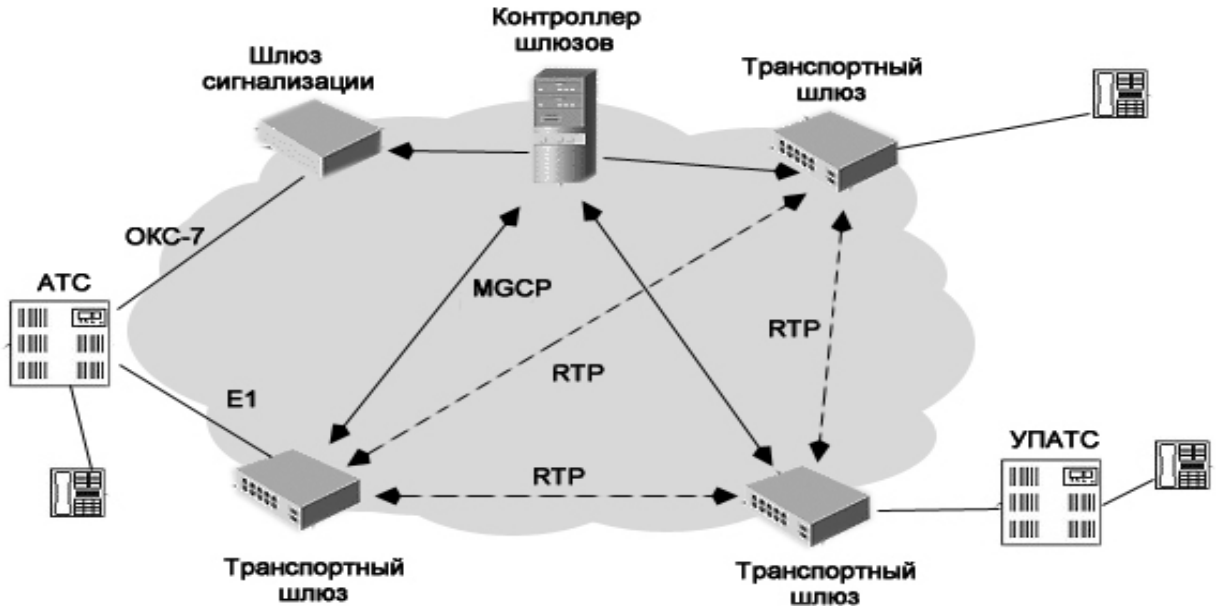

Рисунок 1.4 – Архитектура сети, базирующейся на протоколе MGCP

Управление функциональными блоками декомпозированного шлюза будет осуществляться контроллером шлюза - MGC (Media Gateway

Controller) при поддержки протокола H.248, который пока еще не утвержден ITU, но уже сегодня превосходит протокол MGCP по своим возможностям. Европейский телекоммуникационный институт стандартизации ETSI (рабочая группа TIPHON) также предусмотрел интеграцию принципа декомпозиции шлюза с протоколами H.323.

Также в проекте Рекомендации H.323, версии 4 предусмотрена возможность прозрачной передачи сигнализации ОКС7 и других видов сигнализации по сетям IP-телефонии и обработка всех видов сигнализации Привратником без преобразования в сигнальные сообщения H.225.0.

Выше указанное означает, что Рекомендация H.323 вбирает в себя все самое наилучшее, что предлагается в альтернативных подходах к построению сетей IP-телефонии. Кроме того, поддержка Привратником сигнализации ОКС7 обеспечивает возможность развертывания Интеллектуальных сетей связи (ИС) на базе сетей IP-телефонии.

1.2 Информационная безопасность

1.2.1 Общие положения и определения

Действующим СТ РК 34.007-2002 «Информационная технология. Телекоммуникационные сети. Главные термины и определения » введены последующие ключевые понятия:

– информационная безопасность сети состояние защищенности информационной сферы сети от заданного множества угроз;

– система обеспечения информационной безопасности сети, далее система защиты – совокупность правовых норм, технических мероприятий и механизмов защиты, направленных на противодействие заданному множеству угроз информационной безопасности сети;

– политика информационной безопасности система мероприятий, направленных на обеспечение информационной безопасности.

Не считая того, определим ряд понятий, которые не один раз станем использовать в ходе данной дипломной работы:

– аутентификация процесс проверки какого-либо идентификатора из известного пространства имен. В случае оператора IP-телефонии – проверки номера карты и пин-кода.

– авторизация процесс проверки пользователя на предмет возможности использования какого-либо ресурса.

– аудит процесс учета используемого сервиса.

– хэш-функции – функции, отображающие сообщения каждой длины в значения фиксированной длины, которые часто называют хэш-кодами.

Необходимость познания вероятных угроз, способных привести к необратимым последствиям в функционировании сети в целом, очевидна. Перечень угроз и их классификация, в сочетании с оценкой вероятности реализации конкретной угрозы, служат основой для анализа риска

реализации угроз и формулирования требований к системе защиты. Конечной целью классификации угроз является выбор эффективных средств противодействия при издержках на систему информационной безопасности не превосходящих стоимость потерь, ожидаемых от реализации угроз.

Необходимо оговорить еще один значительный момент, заключающийся во внутреннем противоречии решаемых задач. Он состоит в том, что задачи, которые решает система защиты с точки зрения производителя всегда состоят в противоречии с задачами, которые она должна решать с точки зрения интересов пользователя. Нахождение «золотой середины» для снятия данного противоречия не всегда является рациональным. Достижение необходимого баланса должно осуществляться для каждого частного случая за счет гибкости самой системы защиты. [17].

1.2.2 Типы угроз в сетях IP-телефонии

Не смотря на бесспорные достоинства IP-телефонии нельзя обойти вниманием такую ее проблематичную область как безопасность. IT-специалистам, включая и профессионалов по защите информации, крайне желательно знать вероятные опасности компонентам инфраструктуры IP-телефонии и возможные методы защиты от них, включая и возможности существующих VoIP-стандартов с точки зрения информационной безопасности.

Зачем атакуют сеть IP-телефонии? Это хорошая цель для взломщиков. Некоторые из них могут подшутить над вами, послав вам голосовое сообщение от имени руководства компании. Кто-то может захотеть получить доступ к голосовому почтовому ящику вашего руководства или даже захочет перехватить голосовые данные о финансовых сделках, которыми обмениваются сотрудники финансового департамента или бухгалтерии. Конкуренты могут захотеть подорвать репутацию провайдера IP-телефонии путем выведения из строя шлюзов и диспетчеров, тем самым, нарушая доступность телефонных услуг для абонентов, что, в свою очередь, может также привести к нанесению ущерба бизнесу клиентов. Есть и остальные предпосылки, например, звонки за чужой счет (кража сервиса).

Главная проблема с безопасностью IP-телефонии в том, что она слишком открыта и позволяет злоумышленникам относительно легко совершать атаки на ее компоненты. Несмотря на то, что случаи таких нападений практически неизвестны, они могут быть при желании реализованы, т.к. атаки на обычные IP-сети практически без изменений могут быть направлены и на сети передачи оцифрованного голоса. С другой стороны, похожесть обычных IP-сетей и сетей IP-телефонии подсказывает и пути их защиты, но об этом чуть дальше.

IP-телефония, являясь прямой родственницей обычной телефонии и IP- технологии, вобрала в себя не только их достоинства, но их недостатки. Т.е. атаки, присущие обычной телефонии, также могут быть применены и

для ее IP-составляющей. Перечислим некоторые из них, часть из которых рассмотрим более подробно:

– перехват данных (подслушивание);
– отказ от сервиса (Denial of Service – DoS);
– подмена номера;
– кража сервисов;
– неожидаемые вызовы;
– несанкционированное изменение конфигурации;
– мошенничество со счетом.

1) Перехват данных - самая значительная проблема, как обычной телефонии, так и IP-телефонии. Но в крайнем случае данная угроза гораздо выше, так как злоумышленнику уже не нужно иметь физический доступ к телефонной линии. Обстановку углубляет еще и тот прецедент, что множество протоколов, построенных на базе стека TCP/IP, передают данные в открытом виде. К примеру, это касается HTTP, SMTP, IMAP, FTP, Telnet и, в том числе, протоколы IP- телефонии. Злоумышленник, который сумел перехватить голосовой IP-трафик (а он по умолчанию между шлюзами не шифруется) может без труда восстановить исходные переговоры. Для этого существуют даже автоматизированные средства. Например, утилита vomit (Voice Over Misconfigured Internet Telephones), которая конвертирует данные, приобретенные в результате перехвата трафика с помощью свободно распространяемого анализатора протоколов tcpdump, в обыденный wav-файл, прослушиваемый с помощью любого компьютерного плейера.

Данная утилита позволяет преобразовать голосовые данные, переданные с помощью IP-телефонов Cisco и сжатые с помощью кодека G.711. Мало того, кроме несанкционированного прослушивания злоумышленники могут неоднократно передать перехваченные голосовые сообщения (или их фрагменты) для достижения своих целей.

Однако стоит отметить, что перехват голосовых данных - не такая простая задача, как кажется на первый взгляд. Злоумышленник должен иметь информацию об адресах шлюзов или абонентских пунктов, используемых VoIP-протоколах (например, H.323) и алгоритмах сжатия (например, G.711). В противном случае, злоумышленнику будет трудно настроить ПО для перехвата трафика или объем перехваченных данных и время для их анализа превысит все допустимые пределы.

Перехват данных может быть осуществлен как изнутри корпоративной сети, так и извне. Квалифицированный злоумышленник, имеющий доступ к физической среде передаче данных, может подключить свой IP-телефон к коммутатору и таким образом подслушивать чужие переговоры. Он также может изменить маршруты движения сетевого трафика и стать центральным узлом корпоративной сети через который проходит интересующий его трафик. Причем, если во внутренней сети

вы можете с определенной долей вероятности обнаружить несанкционированно подключенное устройство, перехватывающее голосовые данные, то во внешней сети обнаружить ответвления практически невозможно. Поэтому любой незашифрованный трафик, выходящий за пределы корпоративной сети, должен считаться небезопасным.

2) Отказ в обслуживании

Традиционная телефонная связь всегда гарантирует качество связи даже в случае больших нагрузок, что не является аксиомой для IP-телефонии. Высочайшая перегрузка на сеть, в которой передаются оцифрованные голосовые данные, приводит к существенному искажению и даже пропаданию части голосовых сообщений. Поэтому одна из атак на IP-телефонию может заключаться в посылке на сервер IP-телефонии большого числа "шумовых" пакетов, которые засоряют канал передачи данных, а в случае превышения некоторого порогового значения могут даже вывести из строя часть сети IP-телефонии(т.е. атака “отказ в обслуживании"). Что характерно, для реализации такой атаки нет необходимости "изобретать велосипед" - достаточно использовать широкие известные DoS-атаки Land,Ping of Death, Smurf, UDP Flood и т.д. Одним из решений этой проблемы является резервирование полосы пропускания, которого можно достичь с помощью современных протоколов, например, RSVP. Более подробно способы защиты будут рассмотрены далее. Отказ в обслуживании - серьезная проблема для устройств IP-телефонии. Учитывая, что загруженные сервера могут приносить огромные доходы в час, успешные атаки с организацией отказа в обслуживания приводят к серьезным финансовым потерям.

Одна из атак, которая появилась в конце 1990-х годов, получила название SYN-лавины, так как в ее основе лежало использование пакетов синхронизации, или SYN-пакетов, которые открывают TCP-соединение. Атакующая хост-машина генерирует тысячи отдельных сообщений, каждое из которых пытается начать трехэтапное квитирование по протоколу TCP.

Каждое сообщение содержит другой фиктивный адрес отправителя, так что каждое как бы собирается открыть отдельное соединение. Хост-машина – жертва пытается сгенерировать соответствующий TCP-ответ и посылает его на каждый фиктивный адрес. Она держит эти полуоткрытые соединения, ожидая ответа, который никогда не придет. Одновременно атакующая машина продолжает слать новые и новые фиктивные пакеты, запрашивая все новые и новые соединения. В конечном итоге эти полуоткрытые соединения расходуют все ресурсы хоста по соединениям, и последующие запросы на установление соединений от законных клиентов будут сбрасываться.

Хорошей защитой от подобных атак было улучшение способа обработки набором протоколов полуоткрытых соединений, в частности пересмотр работы в тех ситуациях, когда таких соединений очень много.

Было предложено и реализовано несколько методов, и результаты оказались достаточно успешными. Одна стратегия заключалась в ведении списка полуоткрытых соединений в порядке поступления запросов и отбрасывании более старых при поступлении новых запросов. Хотя при возникновении лавины это могло приводить к отказу в установлении соединения для законных запросов, все же чаще подобный подход позволял устанавливать законные соединения даже во время массового поступления запросов.

3) Подмена номера

Для связи с абонентом в обычной телефонной сети вы должны знать его номер, а в IP-телефонии - роль телефонного номера выполняет IP-адрес. Следовательно, возможна ситуация, когда злоумышленник, используя подмену адреса, сможет выдать себя за нужного вам абонента. Или он может фальсифицировать IP-адрес с целью имитации узла, которому разрешен доступ к приложениям и сервисам, выполняющим аутентификацию запросов на основе проверки адресов. С помощью фальсификации IP-адреса внешний злоумышленник пытается представиться заслуживающим доверия узлом, находящимся внутри или вне сети. Для фальсификации выбирается IP-адрес из диапазона IP-адресов, используемых внутри сети, или же авторизованный внешний IP-адрес, которому вы доверяете, и которому разрешается доступ к определенным ресурсам сети. Фальсификация адреса обычно предполагает манипуляцию данными пакетов TCP/IP, в результате чего нарушитель получает возможность выступать от имени другого узла. Например, злоумышленник может фальсифицировать IP-адрес и представить себя в качестве легального пользователя или даже рабочей станции, чтобы получить привилегии доступа более высокого уровня. При попытке обойти механизм аутентификации, основанный на проверке адресов, он может указать для пакета произвольный адрес источника. Наибольший эффект достигается в случае, когда в качестве адреса источника внешний злоумышленник может указать адрес внутреннего узла, находящимся за маршрутизатором периметра или брандмауэром. Тогда он, используя фальсификацию IP-адреса, может обойти механизмы аутентификации, а при недостаточно квалифицированной их реализации может разрушить и фильтры на фильтрующих маршрутизаторах.

Именно поэтому задачу обеспечения аутентификации не обойдена вниманием во всех существующих VoIP-стандартах и будет рассмотрена в третьей главе. Контрмерой против подобных атак является фильтрация пакетов, приходящих извне, а объявляющих себя пришедшими из самой сети. Соответствующие фильтры устанавливаются в маршрутизаторе периметра, но соответствующие атаки обнаруживаются системой обнаружения вторжений, например, CiscoSecure IDS.

4) Атаки на абонентские пункты

Необходимо понимать, что абонентские пункты, реализованные на

базе персонального компьютера, являются менее защищенными устройствами, чем специальные IP-телефоны. Этот тезис также применим и к любым другим компонентам IP-телефонии, построенным на программной основе. Это связано с тем, что на такие компоненты можно реализовать не только специфичные для IP-телефонии атаки. Сам компьютер и его составляющие (операционная система, прикладные программы, базы данных и т.д.) подвержены различным атакам, которые могут повлиять и на компоненты IP-телефонии. При этом, даже если в самом ПО не найдено уязвимостей (до поры до времени), то используемые им другие программные компоненты третьих фирм (особенно широко известные) могут снизить общую защищенность до нуля. Ведь давно известно общее правило - "защищенность всей системы равна защищенности самого слабого ее звена". Для примера можно привести Cisco CallManager, который использует для своего функционирования Windows 2000 Server, MS Internet Information Server и MS SQL Server, каждый из которых обладает своим набором недостатков с точки зрения обеспечения безопасности.

5) Атаки на узлы сети

Злоумышленники могут атаковать и узлы (Gatekeeper в терминах H.323), которые хранят информацию о разговорах пользователей (имена абонентов, время, продолжительность, причина завершения звонка и т.д.). Это может быть сделано, как с целью получения конфиденциальной информации о самих разговорах, так и с целью модификации и даже удаления указанных данных. В последнем случае биллинговая система (например, у оператора связи) не сможет правильно выставлять счета своим клиентам, что может нарушить функционирование или нанести ущерб всей инфраструктуре IP-телефонии.

2 Безопасность VolP-контента

2.1 Механизмы и стандарты безопасности

2.1.1 SIP-дайджест

Этот алгоритм «дайджест-аутентификации» (*digest authentication, R*FC-2617) в настоящее время наиболее востребован как инструмент защиты, который применяется совместно с SIP. Полученный из развития аналогичного дайджест-алгоритма для HTTP алгоритм SIP-дайджест-аутентификации позволяет производить аутентификацию SIP- абонентов (пользовательских агентов, прокси-серверов или серверов-регистрации). Алгоритм базируется на передаче «общего секрета», который состоит из контрольной суммы поверх nonce (уникальной комбинации для каждой сессии) и параметров (пользовательского имени, пароля, nonce, SIP-метода, Request URI). SIP-дайджест не осуществляет обмен паролями. Общий секрет хэшируется с использованием MD5 или SHA-1 (IETF рекомендовано использование SHA)

2.1.2 SIPS

SIPS (SIP поверх SSL/TLS[1]) защищает такие данные, как SIP URI и IP-адрес, от сниффинга и манипуляции сообщениями. Схема URI немного отличается от обычной SIP URI: sips:this_is_me@sip.com. SIPS шифрует соединение между SIP-абонентом и SIP URI и сетевой точкой (пользовательским агентом, прокси-сервером, DNS-сервером) через SSL/TLS, однако из-за SSL/TLS SIPS передается через TCP вместо UDP. Заданный по умолчанию номер порта для TCP поверх TLS-5061. Пользовательская аутентификация в этом случае проводится с использованием SIP-дайджеста, который хэширует SIP-сообщение (цифровая подпись).

2.1.3 SRTP

Так как RTP- и RTCP-протоколы не предлагают механизмов защиты против сниффинга и манипуляции VoIP-данными, был разработан протокол SRTP *(Secure RealTime Transport Protocol;* RFC-3711), эффективный для использования в приложениях реального времени и являющийся альтернативой базирующимся на IPsec VPN- соединениям. SRTP представляет собой защищенный вариант RTP (как SRTCP для RTCP).

SRTP осуществляет шифрование данных симметрично с AES[2] (Advanced Encryption Standard), тем самым снижая вероятность эффективной реализации таких угроз, как сниффинг, повторы и DoS. При передаче RTP/RTCP-пакеты инкапсулируются в SRTP/SRTCP-пакеты. Алгоритмом SRTP используются следующие механизмы защиты контента:

- шифрование медиапотока (против сниффинга);
- аутентификация отправителя (против спуфинга);
- проверка целостности (против модификаций/манипуляций);
- защита от повторов[3] (против неавторизованного доступа к конечной точке).

SRTP определяет два вида ключей: мастер-ключ (Master Key K_M) и сессионный ключ (Session Key) - (K_E для шифрования и K_A для аутентификации). K_E (минимально –128 бит) и K_A (минимально – 160 бит) получаются из K_M посредством криптографически стойкой псевдослучайной функции (Pseudo-Random Function – PRF).

Шифрование применяется к данным RTF-потока, а обмен ключами происходит через сигнальные сообщения, означая тем самым, что требуется использование механизмов безопасной передачи сигнальных сообщений, например SIPS.

В настоящее время не существует какого-то доминирующего метода генерации и распределения маргер-ключей. Наиболее подходящим вариантом является Multimedia Internet Keying (MIKEY; RFC-3830).

MIKEY описывает процедуру управления и обмена ключами (Transport Encryption Key - TEK и Transport Generation Key - TGK) для мультимедийных сессий реального времени, а также процедуру обмена другими параметрами безопасности между абонентами. В общем, MIKEY служит для обмена мастер-ключом (K_M) и параметрами безопасности. Поскольку TEK может быть модифицирован (так называемый рекеинг), K_M также может подвергнуться модификации. В зависимости от используемого основного протокола, то есть SIP/H.323, MIKEY поддерживает соединения «пользователь-пользователь» (peer-to- peer) и «пользователь - много пользователей» (one-to-many). Это означает, что конечный пользователь, использующий SIP, может установить защищенный коммуникационный линк с конечным пользователем, использующим H.323. Кроме того, MIKEY способен поддерживать различные протоколы обмена ключами и параметрами безопасности для нескольких сессий параллельно. То есть RTP- и RTCP- линки, несмотря на использование всеми участниками TEK, могут защищаться одновременно и независимо [1].

2.1.4 S/MIME

S/MIME (Security/Multipurpose Internet Mail Extension; RFC-2311) был разработан для осуществления процедур шифрования и аутентификации тела сообщения (MIME) электронной почты. Однако его реальное использование этим не ограничивается. В IP- коммуникациях MIME может применяться для шифрованной передачи из «конца в конец» (end-to-end) тела сообщений и, тем самым, быть пригодным для SIP. Кроме этого, SDP-параметры, детализирующие данные абонентской информации, могут быть защищены с помощью S/MIME.

В отличие от SIP, где шифрование применяется на базе «точка - точка» (hop-by-hop), не защищая информацию тела сообщения, передаваемого по SIP-сети, S/MIME предлагает шифрование «из конца в конец». Таким образом, информация тела сообщения может быть расшифрована только конечным пользователем посредством ассиметричной криптографии. Обмен публичными ключами в этом случае может быть реализован с помощью SIP или через сертификаты.

2.1.5 H.235

Стандарт H.323 v.4 (ITU-T) в структуре подстандарта H.235 для защищенной реализации H.323 изменен до H.235.9. Сегодня в H.323 v.6 расширены процедуры безопасности. Наиболее значительным из проведенных расширений является поддержка SRTP [7]. К текущим процедурам безопасности можно отнести:

- проведение базовой аутентификации пользователей (с помощью симметричной криптографии);

- аутентификацию посредством сертифицированных публичных ключей;

- метод обмена ключами Diffie-Hell-man (DH) -DH-ключи согласуются с публичными ключами, представляющими симметричные ключи для проведения процедуры аутентификации.

В настоящее время известно об одной уязвимости в H.323, делающей возможным его нецелевое использование посредством ASN.1 parsing в первой фазе обмена данными H.225 (initial call setup). Кроме этого, можно отметить сложность набора протоколов и большое число производителей, реализующих процедуру (ASN.1/PER кодирования/декодирования) [2], что также повышает риск эффективного исполнения потенциальных угроз.

Для получателя существует возможность проверки RTP-пакетов с помощью Media
Anti-Spam на подлинность заявленного отправителя.

2.1.6 ZRTP

ZRTP, разработанный Аилом Циммерманом и представленный ZFone, создан для реализации взаимодействия между конечным SIP-оборудованием различных производителей и проведения процедуры аутентификации между сторонами соединения. ZRTP является расширением RTP и описывает ключевое соглашение/принятие для использования с SIP и SRTP без необходимости применения разделенных секретов или независимой инфраструктуры публичных ключей (Public Key Infrastructure – PKI), используя вместо них для проведения идентификации голосовые аутентификационные дайджесты.

В течение процедуры установления соединения ZRTP осуществляет обмен ключами на основе алгоритма Diffie-Hellman внутри RTF-потока (иными словами, ZRTP-пакеты внедряются в RTF-пакеты). DH-обмен начинается с генерации общего секрета, на основе которого получается мастер-ключ для SRTP-сессии, передаваемый уровню SRTP. Последний из мастер-ключа получает сессионный ключ, осуществляя защиту от атак повтором с помощью аутентификационной числовой последовательности.

AES используется для шифрования полей полезной нагрузки (непосредственных данных) и SRTP-пакетов, включая заголовки, посредством метода аутентификации SHA-1. Протокол опирается на предположение, что запрашиваемое соединение устанавливается с помощью такого механизма обмена сигнальными сообщениями, как SIP. Каждое использование SRTP идентифицируется с помощью уникальных данных (ZRTP Identification Data – ZID) – случайного 96-битового значения, которое создается для инсталляции Zfone. Если предварительно оговорено использование распределенных секретов, работа ZID происходит с учетом этой договоренности.

2.1.7 SPIT filtering

Для противодействия. SPIT-атакам используется SPIT filtering, функционирование которого основывается на использовании механизма создания белых/черных списков. Каждый VoIP-абонент обладает списком желательных/нежелательных абонентов. Использование белого списка является очень эффективной, но непрактичной мерой, так как некоторые абоненты не могут вступить в запрашиваемое соединение не будучи занесенными в белый список. Своеобразным компромиссом между требованиями безопасности и доступности выступает использование так называемых расширенных белых списков, включающих доверенные web-источники.

2.2 Общая оценка

SIP-дайджест обладает некоторыми широко известными уязвимостями, которые легко могут быть использованы злоумышленником. Одной из наиболее потенциально опасных уязвимостей является ограниченная процедура проверки целостности сообщений (заголовок не подвергается этой процедуре) [4]. Злоумышленник способен изменить сообщение или с помощью реализации MitM-сниффинга получить уникальные пользовательские идентификаторы, изменить их и переслать серверу. Кроме того, так как большинство реализаций позволяют использовать уникальные пользовательские идентификаторы в течение некоторого периода времени, злоумышленник может реализовать повторную пересылку, то есть атаку повторением. С учетом этого, злоумышленник в состоянии также осуществить собственную регистрацию в качестве легитимного пользователя. Доступно и перенаправление данных разговора на собственное оконечное устройство. Отметим, что не всеми методами реализации запросов поддерживается алгоритм дайджеста.

Транзакционная модель реализации запросов CANCEL и ACK в SIP обладает слабой аутентификацией. С точки зрения общих задач безопасности это весьма и весьма посредственно. Методы реализации запросов используют режим hop-by-hop и таким образом могут реализовываться на любом из пунктов (серверов) в сигнальной цепочке. Маловероятно, что каждый из задействованных серверов реализует процедуры безопасности, ассоциированные с другими пунктами, что в целом делает проведение аутентификации запросов малореальной. Кроме того, числовые последовательности этих двух запросов должны быть точно такими же, как и для тех запросов, с которыми они ассоциированы (изменение числовой последовательности приводит к потери ассоциативности).

Недостаточность проводимой для CANCEL и ACK аутентификации делает возможным эффективную реализацию угрозы «инъекции».

Злоумышленник может фальсифицировать запросы CANCEL, приводящие к расторжению установленной пользовательской сессии, и злонамеренные АСК-сообщения (уникальные пользовательские данные в АСК-сообщениях идентичны используемым в предыдущем) [7]. В [7] предложен метод противодействия описанным выше возможностям с помощью «связывания» критически значимых полей заголовка, гарантирующего целостность последнего криптографическими методами, не давая злоумышленникам внести в него изменения.

SIP обладает множеством различных механизмов обеспечения безопасности, упомянутых при рассмотрении SIPS. Некоторые из них напрямую интегрированы в SIP-протокол, например http-аутентификация. Эти механизмы имеют альтернативные алгоритмы и параметры. SIPS не обеспечивает реализацию процедур безопасности «из конца в конец», а поддерживает только режим hop-by-hop, что приводит к необходимости проведения пунктами сети аутентификационных процедур друг для друга. RFC-3261 не содержит никаких механизмов достижения этого требования. Кроме того, даже если некоторые механизмы, такие как OPTIONS, были использованы для достижения соглашения об аутентификации, достигнутое соглашение будет уязвимо для атак Bidding-Down. В стандарте RFC-3329 определены три поля заголовка для реализации согласования механизмов безопасности в SIP, между пользовательским агентом SIP и следующим в цепочке SIP-сервером. В целом, существуют пять механизмов безопасности:

- TLS;
- http-дайджест; IPsec с IKE;
- неавтоматический ключевой IPsec без IKE; S/MIME.

В настоящее время в рамках IETF существует два проекта, касающихся процедур обеспечения безопасности на участках«из конца в середину» (end-to-middle), «середина - середина» (middle-to-middle) и «из середины в конец» (middle-to-end): End-to-middle Security in the Session Initiation Protocol (SIP) [10] и A Mechanism to Secure SIP information inserted by Intermediaries [11]. Требования безопасности между двумя подходами несколько отличаются, однако SIP End to Middle Security [10] и SIP Intermediate Security [11] ориентированы на решение одинаковых фундаментальных проблем обеспечения безопасности в SIP [9].

Протокол SRTP реализован по принципу «из конца в конец», то есть его использование не зависит от существующей сетевой инфраструктуры, а, значит, подходит для общественных сетей. Применяемый криптоанализ, в целом, уменьшен за счет повторного использования мастер-и сессионного ключей. Из-за низкого использования ресурсов применение SRTP не оказывает никакого воздействия на качество предоставления VoIP-сервисов.

Механизмы противодействия атакам повторной передачи SRTP

реализует с помощью «списков повторов», которые содержат перечень идентификаторов ранее полученных и подтвержденных (доверенных) пакетов. Это позволяет получателю производить соответствующий сравнительный анализ данных перечня с получаемыми в настоящее время пакетами. Такой механизм требует наличия у IP-телефона соответствующего размера памяти.

Аутентификация и подтверждение целостности получаемых RTP-сообщений реализуется с помощью HMAC-SHA-1 с К_А. Однако из-за недостатков HMAC-SHA-1 экспертами рекомендуется использование SHA-256, несмотря на нестандартизованность такого решения. Рекомендуется также использовать шифрование полезных данных RTP с последующим расчетом цифрового отпечатка (fingerprint) зашифрованных данных.

SRTP поддерживает безопасные RTF-сессии в течение фазы установления соединений, предшествующей обмену SRTP-пакетами. Однако фундаментальные данные (идентификатор вызова, от кого и к кому устанавливается соединение, как оно проходит, с использованием каких кодеков и пр.) передаются в открытом виде, что даетвозможность злоумышленнику эффективно реализовать угрозы типа MitM, спуфинг или фишинг[6]. Таким образом, требуется использовать защитные механизмы (осуществлять кодирование SIP-пакетов) в течение всего времени установления соединения.

SRTP также уязвим для атак Bid-Down (MitM), при которых злоумышленник вынуждает использовать более низкий уровень шифрования (например, AES-128 вместо AES-256) путем удаления информации AES-256 в INVITE-сообщении [3].

При использовании S/MIME возникает одна проблема: в настоящее время нет организации, управляющей распределением сертификатов, то есть не существует глобальной инфраструктуры PKI. Кроме того, установление S/MIME безопасных соединений является продолжительным процессом.

Единственная известная в настоящее время уязвимость протокола H.323 связана с дефектом ASN.1 parsing, имеющим место в первой фазе обмена H.225-данными. H.235 призван изменить эту ситуацию. Можно также отметить сложность набора протоколов и большое число производителей, реализующих процедуру (ASN.I/PER кодирования/декодирования) [2], что повышает риск эффективного исполнения потенциальных угроз.

Несмотря на то что ключевой обмен не защищен против MitM-атак, связь, организованная с помощью ZRTP, является, в целом, безопасной, так как обладает криптографической стойкостью. Однако уязвимости ZRTP вполне могут быть использованы ресурсоемкими злоумышленниками.

IAX, используемый Asterisk-серверами, является основой построения PBX-серверов от Digium. Он используется для реализации VoIP-соединений между Asterisk-серверами и между сервером и клиентами, также

использующими протокол IAX. В настоящее время наиболее широко распространена вторая версия протокола IAX-IAX2.

IAX2 очень рациональный, полный и в то же время простой протокол, являющийся опосредованным к используемым кодекам и числу потоков. Таким образом, он фактически может применяться в качестве транспорта для любого типа данных. IAX2 использует единый UDP-поток данных, обычно инициализируемый на порте 4569 для организации связи между конечными точками, а также передачи сигнальной информации и данных. Голосовой трафик передается внутриполосно, что делает IAX2 более коммуникабельным для межсетевых экранов (МЭ) и отличает от SIP, эксплуатирующего внеполосную передачу RTP-потоков.

Базовая структура IAX разработана для мультиплексирования сигнальной информации и мультимедийных потоков в единый UDP-поток, циркулирующий между двумя компьютерами. Протокол IAX является бинарным, предназначенным для уменьшения объема служебной информации в отношении передаваемого голосового контента. Общая эффективность использования пропускной способности была отодвинута на второй план, выдвигая в качестве приоритетной цели формирования IAX-протокола обеспечение эффективной полосы пропускания для индивидуальных голосовых вызовов. Создание единого UDP-потока и манипуляции с ним являются более простыми задачами для пользователя, расположенного позади МЭ. Кроме этого, IAX2 может использовать механизмы шифрования (AES-128) для защиты голосовых данных и сигнальной информации, тем самым поддерживая возможность реализации безопасных соединений.

Таблица 2.1 - Обзор протоколов безопасности для VoIP

Механизмы безопасности	Конфиденциальность	Целостность	Аутентификация	Контроль доступа	Ответственность	Анонимность
SIP-дайджест	-	-	+	+	+	-
SIPS	+	+	(+)	-	-	-
S/MIME (тело	(+)	(+)	(+)	(+)	(+)	(+)
SRTP	(+)	(+)	(+)	-	-	
H.235	+	+	+	-	-	-
ZRTP	(+)	(+)	(+)	-	-	-
IAX2	+	+	-	-	-	(+)
Skype	(+)	(+)	-	-	-	-

Skype-пользователи, по существу, имеют возможность

осуществлять телефонные вызовы и пользоваться видеосвязью с помощью своего компьютера, программного обеспечения Skype и ресурсов сети Интернет. В основе Skype-соединения лежит инсталлируемое пользователями бесплатное программное обеспечение, при этом установление такого соединения возможно не только со Skype-пользователями, но и с абонентами сетей мобильной и традиционной телефонии. В настоящее время Skype- приложение является бесплатным и может быть загружено с web-сайта компании, однако само программное обеспечение является собственностью разработчика, сохраняющего его закрытым. Главное отличие Skype от других VoIP-приложений заключается в том, что оно использует прямое (peer-to-peer) соединение, в то время как более традиционной является клиент-серверная модель. Директория Skype-пользователей полностью децентрализована и распределена среди сетевых узлов, что означает возможность осуществления легкого масштабирования до очень больших размеров (сегодня насчитывается более 100 миллионов пользователей) без необходимости дополнительных капитальных затрат. Сегодня обсуждение реальной опасности Skype-трафика приобрело значительные масштабы, выходя далеко за пределы непосредственной безопасности Skype, и оказало большое влияние на VoIP- культуру в целом, что в сумме констатировало формирование нескольких ди- зайнерских принципов:

- весь Skype-трафик шифруется по умолчанию, пользователю недоступно отключение опции;
- на основе имеющихся данных предполагается, что Skype использует надежные алгоритмы шифрования;
- пользователи не вовлечены в процесс шифрования и не имеют никакого отношения к открытой ключевой инфраструктуре.

Констатация вышеизложенных принципов оказала большое влияние на существующий рынок, заставив других производителей предлагать сопоставимые, конкурентоспособные продукты.

2.3 Реализация концепции безопасности

В настоящее время VoIP-сети содержат широкий спектр различных компонентов: телефоны, менеджеры вызовов, шлюзы, серверы, маршрутизаторы и т.д. Существующая VoIP-инфраструктура требует воплощения определенных требований безопасности, которые формируются из двух фундаментальных составляющих общих требований безопасности сетей и специфических требований безопасности, актуальных исключительно для VoIP-сетей и сервисов.

В следующих разделах мы коснемся некоторых базовых принципов защиты и сформулируем общие рекомендации по созданию безопасных VoIP-сетей с учетом специфики VoIP-приложений.

2.4 Стандарт сетевой безопасности

Создание защищенной VoIP-сети должно начинаться с использования стандартных механизмов защиты, традиционно используемых для сетей передачи данных. Дополнительные меры безопасности, использование которых применительно к VoIP- сетям является столь же необходимым, обуславливается спецификой самих VoIP-сетей и приложений, для которых характерны специфические и уникальные угрозы безопасности. Необходимым и основным условием создания безопасной VoIP-сети является глубоко продуманное сетевое планирование с учетом требования предоставления услуг с определенным качеством (Quality-of -Service - QoS).

Важно понимать, что восприятие VoIP-сетей и услуг с точки зрения реализации концепции безопасности не должно осуществляться через призму других IP- приложений.

В то время как безопасность сетей передачи данных, прежде всего, сосредоточивается на защите данных сетевого уровня (например, посредством VLAN и МЭ), реализация безопасности ассоциированных с VoIP компонентов требует использования мультиуровневого подхода, включающего идентификацию физических устройств (телефонов, шлюзов и серверов) и сетевых точек доступа вместе с их авторизацией. Необходимо предусмотреть механизмы защиты сессионного и транспортного уровней, так как именно для этих уровней существует вероятность эффективной реализации таких угроз, как DoS и MitM. Наконец, 7-й уровень эталонной модели ISO-OSI - уровень приложений - должен быть защищен от вирусов, SPIT-атак, мошенничеств и других характерных атак.

2.5 Виртуальные локальные сети (VLAN)

В качестве возможного решения проблемы обеспечения информационной безопасности для корпоративных сетей можно рекомендовать развертывание двух независимых VLAN-сетей: одной - для трафика данных, а другой - для голосового трафика. При этом идеально было бы выделить две независимые подсети с различным диапазоном адресов в соответствии с RFC-1918 (Ю.х.х.х, 172.16.X.X и 192.168.X.X). Кроме того, развертывание раздельных DHCP-серверов позволяет легче обнаружить сетевое вторжение и обеспечить защиту с использованием средств межсетевого экранирования.

Логическое разделение гарантирует невозможность одновременной атаки на сеть данных и VoIP-сеть. Одни вирусы не могут быть использованы, злоумышленником для обеих сетевых составляющих. Также описываемая архитектурная модель значительно усложняет злоумышленнику осуществление сниффинга, перехвата или подслушивания трафика.

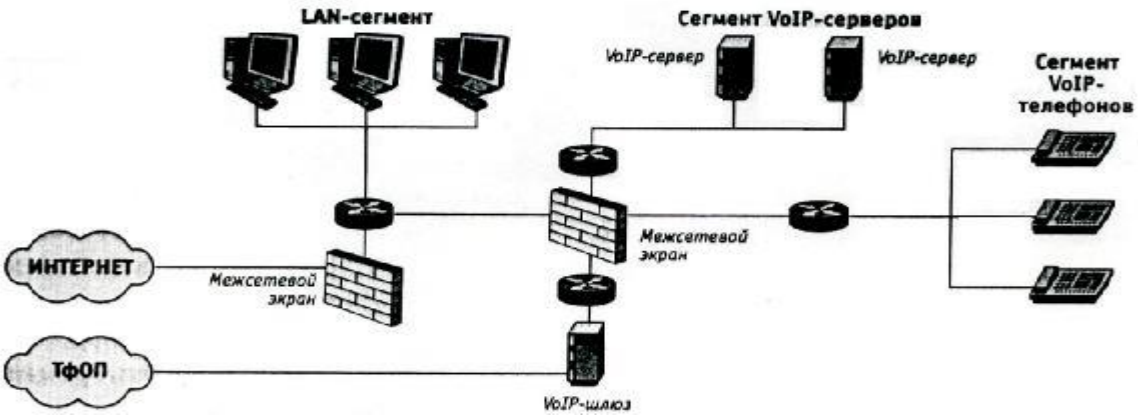

Рисунок 2.1 - VLAN и межсетевое экранирование

Другим преимуществом является возможность введения приоритетных классов для управления качеством обслуживания. В этом случае голосовой трафик может обслуживаться с более высоким приоритетом, чем данные.

В VoIP VLAN используются исключительно телефоны, что дает возможность сетевому администратору отслеживать состояние своей сети и своевременно определять использование доверенных ресурсов в мошеннических целях.

Благодаря разделению и независимой обработке трафика данных и голосового трафика исключается вероятность возникновения коллизий, так как исключено «соревнование» трафика, что, в свою очередь, увеличивает качественные характеристики запрашиваемых сервисов (за счет уменьшений очереди/времени ожидания). Аудиопотоки очень чувствительны к временным характеристикам, так что описанный недорогой подход разделения трафика позволяет существенно улучшить предоставление VoIP-сервисов в существующей сетевой инфраструктуре.

Вместе с тем, несмотря на то что описанная VLAN представляет изящный путь решения проблемы информационной безопасности, полное разделение составляющих сетевого трафика без VLAN-маршрутизации проблематично по ряду причин [12]:

- софтфоны рабочих станций сети данных требуют обеспечения доступа к VoIP-серверам в VoIP-сетях;

- клиентам, совместно использующим общий ресурс, необходимо иметь возможность прямого набора телефонного номера из контакта в приложении (например, Lotus Notes или Outlook);

VoIP-сервер связан с каталогом услуг, таким как LDAP или ADS.

Однако VoIP-инфраструктура некоторых предприятий, использующих большое число различных устройств (VoIP-серверов, VoIP-шлюзов, VoIP-телефонов, софтфонов, СП-систем и др.), связанных друг с другом,

слишком сложна для VLAN. Эти проблемы могут быть решены расположением VoIP-сервера одновременно в сети трафика данных и голоса. Рисунок 2.1 иллюстрирует возможное построение сетевой инфраструктуры с использованием двух МЭ: одного - для сетей передачи данных, а другого - для телефонной сети. Первым обеспечивается передача пакетов из сети Интернет во внутреннюю сеть для сеансов, инициированных пользователем внутренней сети. Второй МЭ управляет трафиком телефонов, VoIP-серверов и VoIP-шлюзов.

2.6 Шифрование

Шифрование используется для обеспечения конфиденциальности и аутентификации в телефонной связи. Реализация безопасных телефонных соединений возможна с использованием SRTP, шифрования RTP-контента и информации сигнализации с TLS. Использование TLS, являющегося альтернативой IPsec, обеспечивает надежную защиту против хакерских атак, в то время как SRTP обеспечивает защиту против подслушивания.

IPsec используется для шифрования сообщений установления соединения и сообщений управления, являясь эффективным средством защиты информации и противодействия подслушиванию. IPsec может использоваться в «туннельном режиме» (tunnelling mode) вместо «транспортного режима» (transport mode), так как туннелирование закрывает IP- адреса источника и получателя, чем обеспечивает защищенное от анализа трафика соединение. Однако использование IPsec предполагает его поддержку на устройствах и менеджерах вызовов[8].

Кроме того, возможно возникновение проблем взаимодействия с некоторыми устройствами управления и мониторинга, не поддерживающими шифрование. Существует и проблема с NAT. IPsec использует порт 500, который обходит мульти- туннели VoIP через NAT.

Большинство пользовательских VoIP-решений, к сожалению, не поддерживает шифрование, что приводит к достаточно простому для злоумышленника прослушиванию VoIP-соединения или даже изменения его содержимого. Существует несколько открытых решений, облегчающих злоумышленнику процедуру сниффинга VoIP-соединений. Некоторые надежды на получение безопасного VoIP-соединения можно связывать с использованием закрытых патентованных кодеков, однако, как показывает практика, закрытость решений еще не гарантирует их надежности. Некоторые производители используют сжатие для повышения уровня защищенности, но важно понимать, что настоящая безопасность связи может быть достигнута только с использованием шифрования и криптографической аутентификации, которые узко доступны на потребительском уровне. [18]

2.7 Аутентификация

В отличие от PSTN-систем, где каждый телефонный аппарат

определяется телефонным номером (ID), соответствующим физическому расположению телефонной линии, к которой аппарат подключен, VoIP-системы назначают телефонам IP-адреса. Так как подобная архитектура предполагает возможность эффективной реализации spoof-атак (при этом злоумышленник присваивает себе чужой ресурс), необходимо принудительное проведение процедуры определения идентичности потенциальных подписчиков при аутентификации в режиме «пользователь - пользователь» (peer-to-peer). Однако такая реализация достаточно сложно применима на практике, так как секретная информация, требующаяся для каждой аутентификации, не может быть легко распределена между пользователями, выдвигая необходимость применения РК1-подхода.

Конфиденциальность связи между VoIP-пользователями - главная задача обеспечения защищенности коммуникаций, так как общедоступные открытые IP-сети являются целью злоумышленников, легко способных реализовать MitM-атаку, чтобы получить доступ к частной информации участников соединения. Поэтому для любого VoIP- соединения требуется проведение соответствующих процедур шифрования и аутентификации.

С тех пор как VoIP-системы, например VoIP-шлюзы или VoIP-серверы, стали составлять основу осуществляемых сотрудниками компании речевых соединений, эффективная в их отношении реализация угроз безопасности ставит под сомнение общую функциональность корпоративной VoIP-сети и ее компонентов, а значит, требует защиты от НСД центральных VoIP-систем. Следовательно, все сетевые пользователи и администраторы должны проходить аутентификацию, проводимую центральной аутентификационной службой, которая связана с системой МЭ, реализующей контроль доступа к сетевым ресурсам.

2.8 Средство межсетевого экранирования

МЭ являются стандартным инструментом защиты сетей передачи данных, проверяя каждый пакет, проходящий из доверенной сети или в нее. Базирующиеся на SIP и H.323 услуги IP-телефонии используют UDP-пакеты и входящие TCP-соединения. Однако в большинстве случаев конфигурации используемых в компаниях МЭ не позволяют протекать VoIP-контенту. Кроме того, из-за динамического распределения портов по запросу МЭ не способны эффективно фильтровать VoIP-трафик. При этом совсем не важно, какой сетевой протокол (SIP или H.323) используется. В обоих случаях требуется реализация stateful-фильтрации[9] протекающего трафика и его ассоциирование с номером порта. Подобный тип МЭ способен запоминать ранее пройденный трафик и анализировать данные прикладного уровня, содержащиеся в пакетах. Более того, подобные экраны способны анализировать адрес отправителя и отвергать пакеты, получаемые от нежелательных источников.

Шлюзы прикладного уровня (Application Level Gateways–ALG[10])

являются альтернативой использованию МЭ. Так как они «понимают» VoIP-протокол, для них возможно осуществление анализа данных прикладного уровня, то есть непосредственно полезной нагрузки, заключенной в анализируемом пакете. ALG обладает программным обеспечением, которое является анализатором для ASN.1- данных (H.323, кодируемый в ASN.l), SIP, MGCP и SDP, осуществляет временную запись состояний сигнальных протоколов и динамически открывает/закрывает порты в соответствии с состоянием сессии.

По сравнению со stateless и stateful межсетевыми экранами ALG предлагает наивысший уровень безопасности, так как открывает UDP-порты только для актуальных соединений, а не предлагает открытие диапазона портов.

Несмотря на существующий на рынке перечень коммерческих предложений по ALG для VoIP-протоколов, большинству существующих сегодня средств межсетевого экранирования недоступна эффективная обработка VoIP-протоколов, таких как SIP. Кроме того, у производителей, использующих протоколы собственной разработки, существует проблема с динамическим открытием диапазона портов и отсутствует поддержка NAT. Пограничный контроллер сессий (Session Border Controllers - SBC) является новым поколением МЭ, призванных решить большинство существующих проблем взаимодействия VoIP-протоколов и средств межсетевого экранирования. SBC контролирует сигнальный и медиатрафик (видео, данные, голосовую информацию).

Адекватные средства межсетевого экранирования должны быть способны контролировать сигнальную информацию, NAT VoIP и управлять медиасессией.

2.9 Системы обнаружения и предотвращения вторжения

Системы обнаружения и предотвращения вторжений (Intrusion Detection Systems и Intrusion Prevention -IDS/IPS) быстро становятся неотъемлемой частью большинства систем безопасности, ориентированных на использование МЭ. Они блокируют злонамеренные пакеты и защищают от вторжения сетевую систему. Однако не достаточно четко и правильно сконфигурированные системы обнаружения и предотвращения вторжений могут существенно понизить качество сетевых сервисов, так как способны ошибочно маркировать нормальные пакеты как злонамеренные и препятствовать их прохождению. Например, обычные UDP-пакеты небольшого размера могут быть восприняты такой системой, как UDP-флудинг при реализации DoS-атаки. Это в состоянии повлечь за собой ретрансляцию, которая станет причиной снижения качества предоставляемых услуг. То есть необходимо использование адаптированных для VoIP пограничных IPS.

2.10 NAT и STUN

NAT – типичная сетевая опция, заключающаяся в переводе частных сетевых адресов в публичные. NAT-маршрутизаторы передают пакеты только тех соединений, которые инициированы из доверенной сети, и отклоняют пакеты, спонтанно поступающие в доверенную сеть из внешней. Поступающие входящие голосовые пакеты UDP переадресовываются на порт получателя, однако ассоциирование с получателем происходит динамически и может быть реализовано различными путями.

Другая проблема связана с интерпретацией исходящих вызовов, поскольку NAT способен осуществлять передачу пакетов третьего уровня, тогда как TCP оперирует с четвертым. NAT изменяет IP-адрес источника (в IP-заголовке) и порт источника (в UDP- или TCP-заголовке).

В то же время информация об IP-адресе и UDP-порте остается неизменной в пределах части передачи сигнальных сообщений, что требует сохранения внутреннего IP-адреса как адреса отправителя в IP-заголовке исходящего пакета. Результат - безответность вызовов ввиду невозможности маршрутизации внутреннего IP-адреса. Публичный (внешний) IP-адрес должен быть передан получателю. Серийное туннелирование (Serial Tunnelling - STUN; RFC 3489) помогает решить эту проблему: конечные точки доступа могут получить публичный IP-адрес и связать NAT со шлюзом. Для этого STUN-клиент (например, VoIP-телефон) посылает на STUN-сервер запрос, в ответ на который ему определяется клиентский мандат (имя пользователя и пароль). Затем клиент посылает второй запрос, указывая данный мандат с целью получения от расположенного перед STUN-сервером NAT-шлюза информации NAT-связи. STUN- сервер извлекает из сообщения IP-адрес источника и IP-порт источника и передает их в ответном сообщении STUN-клиенту. В последствии соответствующие VoIP- приложения меняют публичные IP-адреса на внутренние IP-адреса и вставляют их в заголовок. Дальнейшие запросы позволяют клиенту идентифицировать тип NAT. На сегодняшний день STUN поддерживается многими моделями VoIP-телефонов и провайдерами.

Таким образом, по возможности нужно найти компромисс между необходимостью использования NAT или таких механизмов, как STUN или TURN.

2.11 Качество обслуживания (Quality-of-service – QoS)

При построении защищенных VoIP-сетей и систем необходимо учитывать тот факт, что использование таких средств межсетевого экранирования, как stateful или ALG, может увеличить время обработки/ожидания трафика, оказывая сильное влияние на общее качество предоставляемых услуг. Также надо принять во внимание, что другие VoIP-системы, такие как VoIP-телефоны, имеют достаточно низкую

вычислительную мощность, что приводит к трудности эффективной реализации шифрования для повышения общего уровня безопасности. Существует лишь несколько моделей IP- телефонов, предоставляющих возможность реализации AES-шифрования по разумной цене. В этом случае рекомендуется возложить ответственность за шифрование на центральный сетевой пункт – маршрутизатор или шлюз, который шифрует весь трафик от любого хоста или системы, используя, скажем, IPsec-туннелирование.

Необходимо отметить связь между QoS и используемыми протоколами. Например, SIP- протокол кодирует сообщения в ASCII-формате, который в некоторых случаях образует слишком большие объемы данных, не пригодные для использования в сетях с низкой пропускной способностью. Поскольку в общем пакет может превышать MTU- размер при использовании, скажем, беспроводной LAN, не исключены задержки пакетов или их потери. Для решения этой задачи целесообразно применять бинарное кодирование SIP в соответствии с рекомендациями RFC-3485 и RFC-3486.

2.12 Удаленное управление

Для реализации функций удаленного управления и аудита доступа рекомендуется использовать IPsec или Secure Socket Shell (SSH). Другая возможность состоит в использовании HTTPS с TLS. Необходимо избегать возможности получения удаленного управления IP-PBX системами от небезопасных точек. Если предоставление возможности удаленного доступа является необходимостью, целесообразно предусмотреть процедуры шифрования для запрашиваемого доступа.

2.13 Принципы минимизации VoIP-рисков

В настоящее время наиболее актуальными задачами функционирования VoIP-систем представляются обеспечение необходимого качества обслуживания и безопасность. В рамках данной статьи мы проанализировали возможные угрозы безопасности VoIP- систем и VoIP-приложений, а также продемонстрировали некоторые методы и механизмы противодействия таковым.

SIP и RTP имеют приемлемые возможности для реализации шифрования и проведения аутентификации. H.323 также обладает потенциалом для реализации защищенных соединений. Остается вопрос реализации этих возможностей в существующем VoIP- оборудовании. Кроме этого, необходимо напомнить читателю, что работа по улучшению функционирования VoIP-оборудования и приложений постоянно ведется и в ближайшем будущем несомненно можно будет проанализировать новые возможности и механизмы защиты VoIP-контента. Приведенные в таблице 2.2 данные суммируют все сказанное в этой статье и определяют наиболее эффективные принципы минимизации VoIP-рисков.

Таблица 2.2 - Принципы минимизации VoIP-рисков

Потенциальная угроза	Наилучший механизм противодействия
Атака на уровне приложения	ALG, межсетевые экраны, IDS/IPS прикладного уровня
DoS/DDoS	IDS/IPS прикладного уровня Антивирусная система Изменение текущего приложения с помощью патча VLAN Создание домена безопасности с жесткой политикой безопасности
Подслушивание	VPN для изоляции VoIP-трафика Выборочное шифрование
Атаки на протоколы	ALG и IDS/IPS
SPIT	Строгая аутентификация, авторизация и IPsec
SIP-мониторинг, спуфинг	Строгая аутентификация, авторизация и IPsec
Вирусы и черви	Патчи для текущих приложений Антивирусная система IDS/IPS прикладного уровня VLAN Создание домена безопасности с жесткой политикой безопасности

3. Расчет производительности узла доступа

В офисе организовано 40 рабочих мест:

Количество IP телефонов – 10. Количество аналоговых телефонов - 20.

Для подключения 40 рабочих мест потребуется один маршрутизатор Cisco 3845 Series Integrated Services Routers и коммутатор Cisco Systems серии Catalyst 2950.

Включение персональных компьютеров и IP телефонов производится в порты по технологии Fast Ethernet кабелем 5 категории с разъемами RJ-45 на каждом конце.

Для организации IP телефонии используем IP телефон Cisco. Для подключения 20 абонентов аналоговой телефонии используем офисную АТС Panasonic KX-TDA 30.

Таблица 3.1 - Параметры кодеков

Кодек	G.711	G.726	G.729
Скорость передачи, кбит/с	64	32	8
Длительность датаграммы, Мс	20	20	20
Задержка пакетизации, Мс	1	1	25
Полоса пропускания для двунаправленного соединения, кГц	174,4	110,4	62,4
Задержка в джиттер-буфере	2 датаграммы, 40 мс	2 датаграммы, 40 мс	2 датаграммы, 40 мс
Задержка при кодировании, мс	0,75	1	10
Теоретическая максимальная оценка MOS	4,4	4,07	4,07

Таблица 3.2 – Распределение абонентов по службам

Номер узла	Количество FTP, шт.	Количество IP, шт.	Количество IP/АТС, шт.
1	10	10	20

Каждая группа абонентов совершает в среднем f_i вызовов в час средней длительностью t_i минут. Для второй и третьей группы, зададим объём переданных данных в час наибольшей нагрузки, величину обозначим V_i, Мбайт/с. Мультисервисный узел доступа обслуживает N абонентов.

3.1 Выбор оптимальной структуры узла доступа с учетом нагрузки

Расчёт производительности узла доступа необходимо проводить с учётом всех абонентов, пользующихся услугами. Три группы клиентов:

- пользователи телефонии, π_1;
- IP-телефония, π_2;
- передача данных, π_3.

Рассчитаем число пакетов создаваемых пользователями 1 группы (пользующиеся услугой передачи данных), использующие выбранные ранее кодеки. Параметры кодеков представлены в таблице 3.1

Рассчитаем параметры сети для трех кодеков по формуле:

$$n_i = \frac{1}{T_{PDU}} \ , кадров/с. \qquad (3.1)$$

Длительность дейтаграммы T_{PDU} для выбранных кодеков равна 20 мс, согласно рекомендации RFC 1889. Таким образом, в секунду передается:

$$n_i = \frac{1}{20 \cdot 10^3} = 50 \ кадров/с. \qquad (3.2)$$

Размер пакетизированных данных вычисляется по формуле:

$$h_j = V_j \cdot T_{PDU}, \ байт,$$

где V_j – скорость кодирования, байт/с;

h_j – размер пакетизированных данных;

T_{PDU} – длительность одной речевой выборки (длительность пакета).

Рассчитываем v_j – скорость кодирования, байт/с; h_j – размер пакетизированных данных для трех выбранных кодеков.

При использовании кодека скорость кодирования определяется по формуле:

$$V_j = \frac{R_{Gi}}{8} \ , байт/с, \qquad (3.3)$$

где R_{Gi} – скорость передачи данных заданного кодека

Определим скорости кодирования для следующих кодеков:

Для G.711: $$V_1 = \frac{64}{8} = 8 \ кбит/с = 1000 \ байт/с;$$

Для G.726: $V_2 = \frac{32}{8} = 4\ \textit{кбит}/c = 500\ \textit{байт}/c$;

Для G.729: $V_3 = \frac{8}{8} = 1\ \textit{кбит}/c = 125\ \textit{байт}/c$.

По полученным данным построим сравнительную диаграмму:

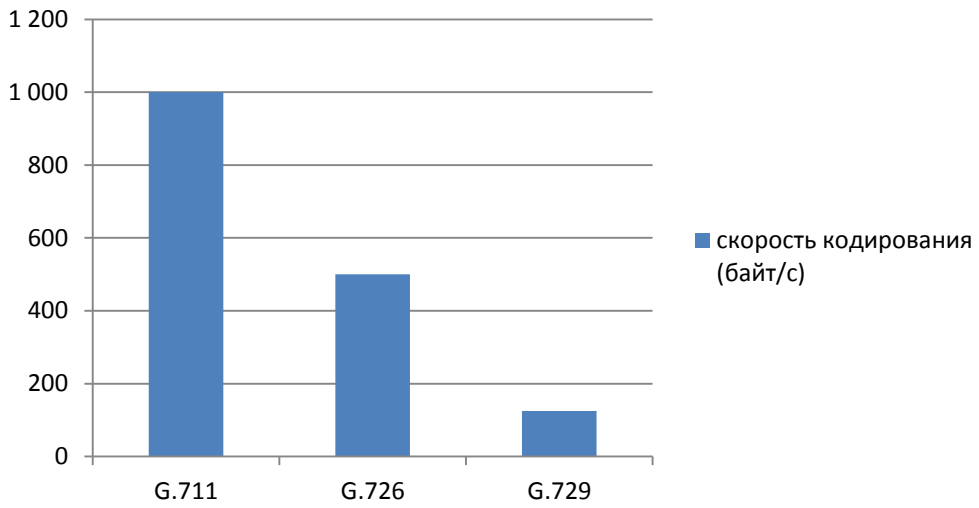

Рисунок 3.1 – Скорость кодирования для трех кодеков

Вычислим размер пакетированных данных для соответствующих кодеков по следующей формуле (3.2):

Для G.711: $h_1 = v_1 \cdot T_{PDU} = 1000 \cdot 20 \cdot 10^{-3} = 20$ *байт,*

Для G.726: $h_2 = v_2 \cdot T_{PDU} = 500 \cdot 20 \cdot 10^{-3} = 10$ *байт,*

Для G.729: $h_3 = v_3 \cdot T_{PDU} = 125 \cdot 20 \cdot 10^{-3} = 2{,}5$ *байт.*

Расчеты выполнены на программе Mathcad, приложение А, рисунок А.1

Таблица 3.3 – Длины заголовков пакетов

Пакет	Длина заголовка байт (бит)
Ethernet	26(208)
IP	20(160)
TCP	24(192)
UDP	8(64)
RTP	16(128)

Суммарный размер пакета рассчитывается по формуле:

$$h_{\Sigma G} = h_j + IP + UDP + RTP \text{ байт}, \quad (3.4)$$

Суммарный размер пакета для кодека G.711

$$h_{\Sigma G1} = h_1 + IP + UDP + RTP = 20 + 20 + 8 + 16 = 64 \text{ байт},$$

Суммарный размер пакета для кодека G.726

$$h_{\Sigma G2} = h_2 + IP + UDP + RTP = 10 + 20 + 8 + 16 = 54 \text{ байт},$$

Суммарный размер пакета для кодека G.729

$$h_{\Sigma G3} = h_3 + IP + UDP + RTP = 2{,}5 + 20 + 8 + 16 = 46{,}5 \text{ байт}.$$

3.2 Расчет числа заявок от абонента группы

Примем следующие обозначения:
s - номер службы;
$y_{аб}$ - число заявок, поступающих от абонента службы s;
$f_{чнн}$ - число вызовов в ЧНН.
Параметр $y_{аб}$ рассчитывается по формуле:

$$y_{аб} = \frac{f_{ЧНН}^{S}}{3600}, \ \frac{1}{c} \quad (3.5)$$

Для различных служб параметр $f_{ЧНН}^{S}$ принимает следующие значения:

$f_{ЧНН}^{FTP} = 10{,}8 \frac{1}{c}$ для передачи файлов;

$f_{ЧНН}^{IP} = 162 \ \frac{1}{c}$ для IP-телефонии;

$f_{ЧНН}^{IP/ATC} = 162 \ \frac{1}{c}$ для телефонии.

Рассчитаем число заявок, поступающих от абонента каждой службы, по формуле (3.5):

$$y_{аб_1}^{FTP} = \frac{f_{ЧНН}^{FTP}}{3600} = \frac{10,8}{3600} = 0,003, \frac{1}{c};$$

$$y_{аб_1}^{IP} = \frac{f_{ЧНН}^{IP}}{3600} = \frac{162}{3600} = 0,045, \frac{1}{c};$$

$$y_{аб_1}^{IP/ATC} = \frac{f_{ЧНН}^{IP/ATC}}{3600} = \frac{162}{3600} = 0,045, \frac{1}{c}.$$

Расчеты выполнены на программе MathCad, приложение А, рисунок А.2

3.3 Расчет числа пакетов от абонентов каждой группы

Рассчитаем число пакетов, генерируемых группой абонентов услуги аналоговой телефонии IP/АТС.

Для этого необходимо учесть их долю в общей структуре пользователей, количество вызовов в час наибольшей нагрузки, среднюю длительность разговора.

Средняя длительность сеанса связи абонента t равна 100 с для телефонии, IP-телефонии и 1 с для передачи файлов

Число пакетов, генерируемых группой абонентов, рассчитывается по формуле:

$$N_{1j} = n_{1j} \cdot t_1 \cdot \pi_1 \cdot N \cdot f_{ЧНН}^{IP/ATC}, пакетов. \quad (3.6)$$

где N_{1j} – число пакетов, генерируемое первой группой пользователей в час наибольшей нагрузки;

n_{1j} – число пакетов, генерируемых в секунду одним абонентом;

t_1 – средняя длительность сеанса связи абонента в секундах для первой группы;

$f_{ЧНН}^{IP/ATC}$ – число вызовов в час наибольшей нагрузки для первой группы абонентов;

π_1 – доля абонентов группы IP/АТС от общего числа.

N – общее число пользователей.

Тогда, по формуле (3.6):

$$N_{1j} = 50 \cdot 100 \cdot 0,5 \cdot 40 \cdot 162 = 16,2\ 10^6\ пакетов.$$

Рассчитаем число пакетов, генерируемых группой абонентов услуги IP-телефонии

Рассуждения, приведённые для абонентов аналоговой телефонии, в полной мере можно применить и группе абонентов IP-телефонии для расчёта числа пакетов, возникающих в результате пользования голосовыми сервисами:

$$N_{2j} = n_{1j} \cdot t_2 \cdot \pi_2 \cdot N \cdot f_{ЧНН}^{IP}, пакетов. \quad (3.7)$$

где N_{2j} – число пакетов, генерируемое второй группой пользователей в час наибольшей нагрузки при использовании IP-телефонии;

n_{1j} – число пакетов, генерируемых в секунду одним абонентом;

t_2 – средняя длительность сеанса связи абонента в секундах для второй группы абонентов;

$f_{ЧНН}^{IP}$ – число вызовов в час наибольшей нагрузки для второй группы абонентов;

π_2 – доля абонентов второй группы от общего числа абонентов;

N – общее число пользователей.

Тогда число пакетов генерируемой второй группой по формуле (3.7) будет равно:

$$N_{2j} = 50 \cdot 100 \cdot 162 \cdot 0{,}25 \cdot 40 = 8{,}1\ 10^6\ пакетов.$$

Для расчёта числа пакетов, генерируемых группой пользователей IP-телефонии при использовании сервисов передачи данных, необходимо задаться размером пакетов. При построении сети, как правило, на одном или нескольких участках сети на уровне звена данных используется та или иная разновидность технологии Ethernet, поэтому использовать пакеты, превышающие максимальную длину поля данных Ethernet, не имеет смысла. Очень длинный пакет рано или поздно будет фрагментирован, что приведёт, во-первых, к излишней нагрузке на коммутаторы, и, во-вторых, к возможным перезапросам в случае потерь.

Кроме того, использование пакетов большого размера затрудняет обеспечение качества обслуживания и на магистральной сети, и в сети доступа. Более того, как правило, корпоративные пользователи устанавливают на границе своей сети «firewall», который, иногда, ограничивает максимальный размер кадра. При передаче данных вместо протоколов RTP и UDP используется TCP, вносящий точно такую же избыточность (20 байт).

Для расчёта числа пакетов в час наибольшей нагрузки необходимо задаться объёмом переданных данных. Допустим, что абоненты

IP-телефонии относятся к интернет-сёрферам. Средний объём данных, переданных за час при таком способе подключения, составляет :

$$V_2 \approx V_2(Мбайт) \cdot \frac{1024 \cdot 1024}{8}. \qquad (3.8)$$

Число пакетов, переданных в ЧНН, будет рассчитываться по формуле:

$$N_{2_\partial j} = \pi_2 \cdot N \cdot \frac{V_{2j}}{h_{2j}}, пакетов. \qquad (3.9)$$

где $N_{2_\partial j}$ – количество пакетов, генерируемых в час наибольшей нагрузки абонентами второй группы при использовании сервисов IP-телефонии;

π_2 – доля пользователей группы 2 в общей структуре абонентов;

h_{2j} – размер поля данных пакета;

N – общее число пользователей.

Тогда:

Для G.711: $N_{2_\partial j} = 0{,}25 \cdot 40 \cdot \frac{1310720}{20} = 6{,}554 \cdot 10^5$ *пакетов*;

Для G.726: $N_{2_\partial j} = 0{,}25 \cdot 40 \cdot \frac{1310720}{10} = 13{,}11 \cdot 10^5$ *пакетов*;

Для G.729: $N_{2_\partial j} = 0{,}25 \cdot 40 \cdot \frac{1310720}{2{,}5} = 52{,}43 \cdot 10^5$ *пакетов*.

Суммарное число пакетов, генерируемых второй группой пользователей в сеть в час наибольшей нагрузке рассчитаем по формуле:

$$N_{2_j} = N_{2_j} + N_{2_\partial j}, пакетов. \qquad (3.10)$$

Тогда:

Для G.711: $N_{21} = 8{,}1 \cdot 10^6 + 0{,}6554 \cdot 10^6 = 8{,}755 \cdot 10^6$ *пакетов;*

Для G.726: $N_{22} = 8{,}1 \cdot 10^6 + 1{,}311 \cdot 10^6 = 9{,}41 \cdot 10^6$ *пакетов;*

Для G.729: $N_{23} = 8{,}1 \cdot 10^6 + 5{,}243 \cdot 10^6 = 13{,}34 \cdot 10^6$ *пакетов.*

Все рассуждения, проведённые относительно первых двух групп, остаются в силе и для третьей группы, пользующимися услугами передачи данных, а именно:

$$N_{3_TJ} = n_{1j} \cdot t_3 \cdot \pi_3 \cdot N \cdot f_{ЧНН}^{FTP}, пакетов. \quad (3.11)$$

где N_{3_mj} – число пакетов, генерируемое третьей группой пользователей в час наибольшей нагрузки при использовании голосовых сервисов;

n_{1j} – число пакетов, генерируемых в секунду одним абонентом;

t_3 – средняя длительность разговора в секундах;

$f_{ЧНН}^{FTP}$ – число вызовов в час наибольшей нагрузки;

π_3 – доля пользователей группы 3 в общей структуре абонентов;

N – общее число пользователей.

Тогда по формуле (3.11):

$$N_{3_TJ} = 50 \cdot 1 \cdot 0{,}25 \cdot 40 \cdot 10{,}8 = 5{,}4 \cdot 10^3 \ пакетов.$$

Расчеты выполнены на программе MatchCad, приложение А, рисунок А.3

Будем предполагать, что абоненты третьей группы относятся к «активным» пользователям интернета. Объём переданных и принятых данных данных при таком использовании интернета составляет V_3=8,5197·10^6 байт. Число пакетов, переданных в ЧНН рассчитаем по формуле:

$$N_{3_\partial j} = \pi_3 \cdot N \cdot \frac{V_{3j}}{h_j}, пакетов. \quad (3.12)$$

Тогда:

Для G.711: $N_{3_\partial 1} = 0{,}25 \cdot 40 \cdot \frac{8{,}5197 \cdot 10^6}{20} = 4{,}26 \cdot 10^6 \ пакетов$;

Для G.726: $N_{3_\partial 2} = 0{,}25 \cdot 40 \cdot \frac{8{,}5197 \cdot 10^6}{10} = 8{,}52 \cdot 10^6 \ пакетов$;

Для G.729: $N_{3_\partial 3} = 0{,}25 \cdot 40 \cdot \frac{8{,}5197 \cdot 10^6}{2{,}5} = 34{,}08 \cdot 10^6 \ пакетов$.

Суммарное число пакетов, генерируемых третьей группой пользователей в сеть в час наибольшей нагрузке, будет равно

$$N_{31} = N_{3j_T} + N_{3j_\partial}, \ пакетов. \quad (3.13)$$

Тогда:

Для G.711: $N_{31} = 5{,}4 \cdot 10^3 + 4{,}26 \cdot 10^6 = 4{,}265 \cdot 10^6$ *пакетов*;

Для G.726: $N_{32} = 5{,}4 \cdot 10^3 + 8{,}52 \cdot 10^6 = 8{,}525 \cdot 10^6$ *пакетов*;

Для G.729: $N_{33} = 5{,}4 \cdot 10^3 + 34{,}08 \cdot 10^6 = 34{,}085 \cdot 10^6$ *пакетов*.

Расчеты выполнены на программе MathCad, приложение А, рисунок А.3

3.4 Требования к производительности мультисервисного узла доступа

Мультисервисный узел доступа должен обслуживать трафик от всех трёх групп пользователей. Кроме того, именно узел доступа должен обеспечить поддержку качества обслуживания путем приоритезации трафика, которая должна осуществляться независимо от используемой технологии транспортной сети доступа.

Суммарное число пакетов, которое должен обработать мультисервисный узел доступа, будет равно:

$$N_{j\sum j} = N_{1j} + N_{2j} + N_{3j}, \ \textit{пакетов}. \tag{3.14}$$

Следовательно, по формуле (3.14):

Для G.711: $N_{\sum 1} = 16{,}2 \cdot 10^6 + 8{,}755 \cdot 10^6 + 4{,}265 \cdot 10^6 = 29{,}22 \cdot 10^6$ *пакетов*;

Для G.726: $N_{\sum 2} = 16{,}2 \cdot 10^6 + 9{,}41 \cdot 10^6 + 8{,}525 \cdot 10^6 = 34{,}14 \cdot 10^6$ *пакетов*;

Для G.729: $N_{\sum 3} = 16{,}2 \cdot 10^6 + 13{,}34 \cdot 10^6 + 34{,}085 \cdot 10^6 = 63{,}63 \cdot 10^6$ *пакетов*.

Расчеты выполнены на программе MathCad, приложение А, рисунок А.4

Среднее число пакетов в секунду рассчитывается для трех выбранных кодеков равно:

$$N_{\sum_секj} = \frac{N_{\sum j}}{3600}, \ \textit{пакетов}. \tag{3.15}$$

Тогда:

Для G.711: $N_{\sum_сек1} = \dfrac{29{,}22 \cdot 10^6}{3600} = 8{,}117 \cdot 10^3$, *пакетов/с*;

Для G.726: $N_{\sum_сек2} = \dfrac{34{,}14 \cdot 10^6}{3600} = 9{,}482 \cdot 10^3$, *пакетов/с*;

Для G.729: $N_{\sum_сек3} = \dfrac{63{,}63 \cdot 10^6}{3600} = 17{,}67 \cdot 10^3$, *пакетов/с*.

Расчеты выполнены на программе MathCad, приложение А, рисунок А.4

Данные показатели позволяют оценить требования к производительности маршрутизатора, агрегирующего трафик мультисервисной сети доступа, который рассчитывается по формуле:

$$N_{i_j}\% = \frac{N_{i_j} \cdot 100}{N_{j\sum j}}, \ \% \qquad (3.16)$$

$$N_{\sum 1} = 29{,}22 \cdot 10^6 \, пакетов;$$

$$N_{\sum 2} = 34{,}14 \cdot 10^6 \, пакетов;$$

$$N_{\sum 3} = 63{,}63 \cdot 10^6 \, пакетов.$$

Тогда:

$$N_{11}\% = \frac{16{,}2 \cdot 10^6 \cdot 100}{29{,}22 \cdot 10^6} = 55{,}44 \ \%$$

$$N_{21}\% = \frac{8{,}755 \cdot 10^6 \cdot 100}{29{,}22 \cdot 10^6} = 29{,}963 \ \%$$

$$N_{31}\% = \frac{4{,}265 \cdot 10^6 \cdot 100}{29{,}22 \cdot 10^6} = 14{,}597 \ \%$$

$$N_{12}\% = \frac{16{,}2 \cdot 10^6 \cdot 100}{34{,}14 \cdot 10^6} = 47{,}457 \ \%$$

$$N_{22}\% = \frac{9{,}41 \cdot 10^6 \cdot 100}{34{,}14 \cdot 10^6} = 27{,}568 \ \%$$

$$N_{32}\% = \frac{8{,}525 \cdot 10^6 \cdot 100}{34{,}14 \cdot 10^6} = 24{,}974\%$$

$$N_{13}\% = \frac{16{,}2 \cdot 10^6 \cdot 100}{63{,}63 \cdot 10^6} = 25{,}461 \ \%$$

$$N_{23}\% = \frac{13{,}34 \cdot 10^6 \cdot 100}{63{,}63 \cdot 10^6} = 20{,}97 \ \%$$

$$N_{33}\% = \frac{34{,}085 \cdot 10^6 \cdot 100}{63{,}63 \cdot 10^6} = 53{,}569 \ \%$$

Расчеты выполнены на программе MathCad, приложение А, рисунок А.5

Таблица 3.4 - Количество передаваемых пакетов в секунду для трех групп пользователей

Группа Абонентов	Количество передаваемых пакетов в сек		
	G.711	G.726	G.729
Пользователи телефонии (π_1),%	55,44	47,457	25,461
IP-телефония (π_2),%	29,963	27,568	20,97
Передача данных (π_3),%	14,597	24,974	53,569

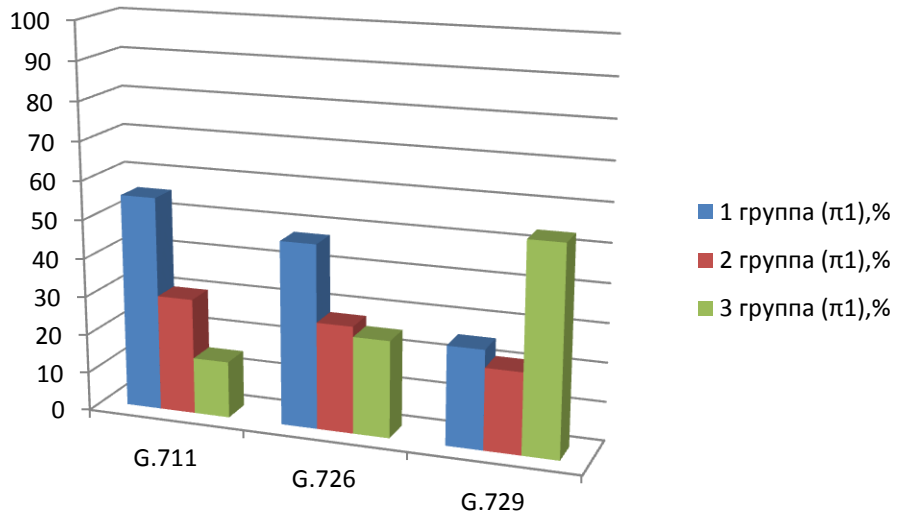

Рисунок 3.2 – Доля передаваемых пакетов тремя группами

Вывод о загрузке системы пользователями трех групп.
Проанализировав все вышеизложенные расчеты, можно сделать вывод о целесообразности использования в IP-телефонии кодека G.711.

3.5 Определение временных параметров сети доступа

Требования к полосе пропускания определяются гарантиями качества обслуживания, предоставляемыми оператором пользователю. Параметры QoS описаны в рекомендации ITU Y.1541. В частности, задержка распространения из конца в конец при передачи речи не должна превышать 100 мс, а вероятность превышения задержки порога в 50 мс не должна превосходить 0,001, т.е.

$$\bar{t}_p \le 100, мс$$

$$\{t_p > 50\ мс\} \le 0{,}001$$

Задержка из конца в конец складывается из следующих составляющих:

$$t_p = t_{пакет} + t_{ад} + t_{core} + t_{буф}, мс \tag{3.17}$$

где t_p – время передачи пакета из конца в конец;
$t_{пакет}$ – время пакетизации (зависит от типа трафика и кодека);
$t_{ад}$ – время задержки при транспортировке в сети доступа;
t_{core} – время задержки при распространении в транзитной сети;
$t_{буф}$ – время задержки в приёмном буфере.

Применение низкоскоростных кодеков «съедает» основную часть бюджета задержки. Задержка в приёмном буфере также велика, поэтому на сеть доступа и транспортная сеть должны обеспечивать минимальную задержку.

Допустим, что задержка сети доступа не должна превышать 5 мс. Время обработки заголовка IP-пакета близко к постоянному. Распределение интервалов между поступлениями пакетов соответствует экспоненциальному закону. Поэтому для описания процесса, происходящего на агрегирующем маршрутизаторе, можно воспользоваться моделью M/G/1.

Для данной модели известна формула, определяющая среднее время вызова в системе (формула Полячека – Хинчина)

$$\bar{t}_{адj} = \frac{\tau_j (1 + C_b^2)}{2(1 - \lambda_j \tau_j)},\ c \tag{3.18}$$

где τ_j – средняя длительность обслуживания одного пакета;
C_b^2 – квадрат коэффициента вариации, $C_b^2 \approx 0{,}2$;
λ_j – параметр потока, из первой задачи $N_{\Sigma_секj}$;
$\bar{t}_{адj}$ – среднее время задержки пакета в сети доступа, $\bar{t}$ = 0,005 с.

Ненулевой коэффициент вариации учитывает возможные отклонения при использовании в заголовках IP полей ToS. Кроме того, время обработки IP-пакета в значительной мере зависит от используемых на маршрутизаторе правил обработки. Из формулы (3.17) следует зависимость максимальной величины для средней длительности обслуживания одного пакета от среднего времени задержки в сети доступа.

$$\tau_j = \frac{1}{\lambda_j + \frac{1+C_b^2}{2\bar{t}_{\text{ад}\,j}}}, \ c \qquad (3.19)$$

Для G.711: $\tau_1 = \frac{1}{\lambda_1 + \frac{1+C_b^2}{2\bar{t}_{\text{ад}\,j}}} = \frac{1}{8{,}117 \cdot 10^3 + \frac{1+0.2}{2 \cdot 0.005}} = 1.214 \cdot 10^{-4}, c$

Для G.726: $\tau_2 = \frac{1}{\lambda_2 + \frac{1+C_b^2}{2\bar{t}_{\text{ад}\,j}}} = \frac{1}{9{,}482 \cdot 10^3 + \frac{1+0.2}{2 \cdot 0.005}} = 1.041 \cdot 10^{-4}, c$

Для G.729: $\tau_3 = \frac{1}{\lambda_3 + \frac{1+C_b^2}{2\bar{t}_{\text{ад}\,j}}} = \frac{1}{17{,}67 \cdot 10^3 + \frac{1+0.2}{2 \cdot 0.005}} = 5.62 \cdot 10^{-5}, c$

Интенсивность обслуживания связана со средним временем задержки пакета в сети доступа обратно пропорционально:

$$\beta_j = \frac{1}{\tau_j}, \ \frac{1}{c} \qquad (3.20)$$

Для G.711: $\beta_1 = \frac{1}{\tau_1} = \frac{1}{1.214 \cdot 10^{-4}} = 8.237 \cdot 10^3$

Для G.726: $\beta_2 = \frac{1}{\tau_2} = \frac{1}{1.041 \cdot 10^{-4}} = 9.602 \cdot 10^3$

Для G.729: $\beta_3 = \frac{1}{\tau_3} = \frac{1}{5.62 \cdot 10^{-5}} = 17.79 \cdot 10^3$

Расчеты выполнены на программе MathCad, приложение А, рисунок А.6

Рассчитали по формулам 3.19 и 3.20 среднее время задержки в сети доступа и интенсивность обслуживания при норме задержки $\bar{t}_{\text{ад}}$ = 5 мс для трех типов кодеков.

Время τ_j должно выбираться как минимальное из двух возможных значений. Первое значение – величина, полученная из последней формулы. Второе значение – та величина, которая определяется из условия ограничения загрузки системы – ρ. Обычно эта величина не должна превышать 0,5.

При среднем значении задержки в сети доступа 5 мс коэффициент использования высчитывается по формуле:

$$\rho_j = \lambda_j \cdot \tau_j (0.005) \qquad (3.21)$$

Тогда:

$$\text{Для G.711: } \rho_1 = \lambda_1 \cdot \tau_1 = 8.117 \cdot 10^3 \cdot 1.214 \cdot 10^{-4} \approx 0.985$$

$$\text{Для G.726: } \rho_2 = \lambda_2 \cdot \tau_2 = 9.482 \cdot 10^3 \cdot 1.041 \cdot 10^{-4} \approx 0.988$$

$$\text{Для G.729: } \rho_3 = \lambda_3 \cdot \tau_3 = 17.79 \cdot 10^3 \cdot 5.62 \cdot 10^{-5} \approx 0{,}993$$

Рассчитаем коэффициент использования для случаев с различными кодеками.

При таком высоком использовании малейшие флуктуации параметров могут привести к нестабильной работе системы.

Определим параметры системы при её использовании на 50%.

Средняя длительность обслуживания будет равна

$$\tau_j = \frac{\rho_j}{\lambda_j} \tag{3.22}$$

$$\text{Для G.711: } \tau_1 = \frac{\rho_1}{\lambda_1} = \frac{0{,}5}{8{,}117 \cdot 10^3} = 6{,}16 \cdot 10^{-5}$$

$$\text{Для G.726: } \tau_2 = \frac{\rho_2}{\lambda_2} = \frac{0{,}5}{9{,}482 \cdot 10^3} = 5.273 \cdot 10^{-5}$$

$$\text{Для G.729: } \tau_3 = \frac{\rho_3}{\lambda_3} = \frac{0{,}5}{17{,}67 \cdot 10^3} = 2.829 \cdot 10^{-5}$$

Определим интенсивность обслуживания при этом

$$\beta_j = \frac{1}{\tau_j} \tag{3.23}$$

$$\text{Для G.711: } \beta_1 = \frac{1}{\tau_1} = \frac{1}{6{,}16 \cdot 10^{-5}} = 1{,}623 \cdot 10^4$$

$$\text{Для G.726: } \beta_2 = \frac{1}{\tau_2} = \frac{1}{5{,}273 \cdot 10^{-5}} = 1.896 \cdot 10^4$$

$$\text{Для G.729: } \beta_3 = \frac{1}{\tau_3} = \frac{1}{2{,}829 \cdot 10^{-5}} = 3{,}535 \cdot 10^4$$

Расчеты выполнены на программе MathCad, приложение А, рисунок А.7

Задержка в сети доступа рассчитывается по формуле:

$$\bar{t}_{ад\,j} = \frac{\tau_j(1+C_b^2)}{2(1-\lambda_j\tau_j)}, c \qquad (3.24)$$

$$\text{Для G.711:}\ \bar{t}_{ад1} = \frac{6{,}16\cdot 10^{-5}(1+0{,}2)}{2(1-8{,}117\cdot 10^{3}\cdot 6{,}16\cdot 10^{-5})} = 7{,}392\cdot 10^{-5}\ c$$

$$\text{Для G.711:}\ \bar{t}_{ад2} = \frac{5.273\cdot 10^{-5}(1+0{,}2)}{2(1-9.482\cdot 10^{3}\cdot 5.273\cdot 10^{-5})} = 6{,}328\cdot 10^{-5}\ c$$

$$\text{Для G.711:}\ \bar{t}_{ад3} = \frac{2.829\cdot 10^{-5}(1+0{,}2)}{2(1-17.67\cdot 10^{3}\cdot 2.829\cdot 10^{-5})} = 3{,}395\cdot 10^{-5}\ \textit{секунд}$$

При известном среднем размере пакета h_j,определим требуемую полосу пропускания по формуле:

$$\varphi_j = \beta_j \cdot h_j\ ,\textit{бит/с} \qquad (3.25)$$

$$\text{Для G.711:}\ \varphi_1 = \beta_1\cdot h_1 = 1{,}623\cdot 10^{4}\cdot 20 = 3{,}247\cdot 10^{5}\ \textit{бит}/c$$

$$\text{Для G.726:}\ \varphi_2 = \beta_2\cdot h_2 = 1.896\cdot 10^{4}\cdot 10 = 1{,}896\cdot 10^{5}\ \textit{бит}/c$$

$$\text{Для G.729:}\ \varphi_3 = \beta_3\cdot h_3 = 3.535\cdot 10^{4}\cdot 2.5 = 8{,}837\cdot 10^{4}\ \textit{бит}/c$$

Расчеты выполнены на программе MathCad, приложение А, рисунок А.7

Построим диаграмму, для анализа результатов

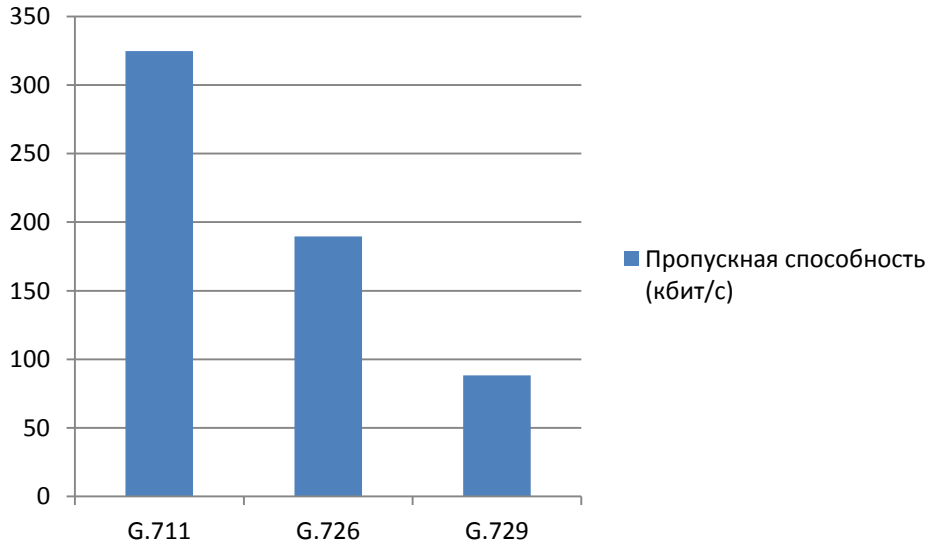

Рисунок 3.3 – Требуемая полоса пропускания

Из графика видно, что для передачи одной и той же информации, то есть одного объема при использовании IP-телефонии, необходима различная

полоса пропускания. В нашем случае при использовании кодека G.726 с длиной пакета 10 бит и G711A с длиной пакета 20 бит необходима большая полоса пропускания, чем при использовании кодека G729A с длиной пакета 2,5 бит.

4 Технико-экономическое обоснование

4.1 Резюме

В компании «ТОО CONNECTION NETWORK SYSTEMS» существует IP сеть. Она построена с использованием маршрутизатора Cisco 3845 Series Integrated Services Routers и коммутаторов Cisco Systems серии Catalyst 2950. Внедрение данного оборудования дает возможность организовать сеть передачи голоса и факсимильных данных по IP протоколу.

1) Цель проекта:

- снижение расходов на междугородние, международные направления;

- модернизация телефонной сети компании.

2) Задачи проекта:

- приобретение оборудования;

- провести установку и монтаж оборудования;

- настройка программного обеспечения.

4.2 Краткое описание проекта

В связи с повышением абонентской платы за использование телефонной сети, IP телефония становится более актуальным и выгодным вариантом передачи голоса и факсимильных данных.

Обычные телефонные звонки настоятельно просят разветвленной сети связи телефонных станций, связанных закрепленными телефонными линиями, подвода волоконно-оптических кабелей и спутников связи. Высокие затраты телефонных компаний приводят для нас к дорогим междугородным разговорам. Выделенное подключение телефонной станции также имеет много избыточной производительности или времени простоя в течение речевого сеанса.

Интернет-телефония частично базируется на существующей сети закрепленных телефонных линий. Однако главное, она использует самую современную технологию сжатия наших голосовых сигналов, и полностью использует емкость телефонных линий. Поэтому пакеты данных от разных запросов, и даже различные их типы, могут перемещаться по одной и той же линии в одно и тоже время.

Уменьшение расходов, связанных с перемещением сотрудников. Пользователи могут перемещаться с одного места на другое в пределах компании; для того чтобы начать работу на новом месте, им нужно просто зарегистрироваться в системе, используя IP-телефон Cisco. Далее данному телефонному аппарату присваиваются настройки пользователя и его телефонный номер.

4.3 Финансовый план

4.3.1 Расчет капитальных вложений. Капитальные вложения рассчитываются по формуле:

$$K_{\sum ВЛ} = K_0 + K_м + K_{тр} + K_{проект}, \quad (4.1)$$

где K_0 – капитальные вложения на приобретение оборудования;

$К_м$ - капитальные вложения на монтажные работы (5-8% от стоимости оборудования);

$K_{тр}$ - капитальные вложения на транспортные расходы (5-10% от стоимости оборудования);

$K_{проект}$ - капитальные вложения на проектирование (1-2% от стоимости оборудования).

Определяется величина затрат.

Для этой цели составляются сметы на приобретение оборудования.

Таблица 4.1 - Сводная таблица цен необходимого оборудования для данного проекта [http://ciscoshop.kz]

Наименование	Цена (тенге)
ПО Cisco CallManager лицензия на 16 телефонов	36 000
Модуль Cisco Systems VWIC-2MFT-E1	116 800
IP телефоны 14 шт	140 600
Программное обеспечение	42 000
Итого	335 400

Процесс внедрения состоит из последующих шагов:

1. Установка программного обеспечения Cisco CallManager на маршртизатор Cisco 3845;

2. Настройка данной программы для обеспечения маршрутизации голосовой информации между номерами абонентов.

Так как основа (IP сеть) для IP телефонии существует и хорошо организована, это позволит снизить затраты на приобретение дорогостоящего оборудования и привлечения специалистов для настройки оборудования.

Таким образом, реализация данного проекта позволит значительно уменьшить затраты рабочего времени на организационные вопросы а, следовательно, повысить производительность труда и экономическую эффективность проводимых работ. Для обслуживания 14 телефонов и маршрутизатора достаточно одного инженера.

Таблица 4.2 - Основные показатели сравнительного анализа вариантов [http://telecom.kz/services/phone/view/rates-phone]

Показатели	Варианты	
	Базовый	Проектируемый
Расходы на междугородные переговоры, тенге	335 500	52 000

Капитальные вложения на монтажные работы:

$$К_м = 0,05 \cdot К_о \quad (4.2)$$

$$К_м = 0,05 \cdot К_о = 0,05 \cdot 335\ 400 = 16\ 770 \text{ тенге}$$

Транспортные расходы составляют 5 % от стоимости оборудования. Исходя из этого, получим:

$$К_{тр} = 0,05 \cdot К \quad (4.3)$$

$$К_{тр} = 0,05 \cdot 335\ 400 = 16\ 770 \text{ тенге}$$

Капитальные вложения на проектирование рассчитываются по формуле:

$$К_{проект} = 0,02 \cdot К_о \quad (4.4)$$

$$К_{проект} = 0{,}02 \cdot 335\ 400 = 6\ 708 \text{ тенге.}$$

Тогда сумма капитальных вложений составит

$$К_{\sum ВЛ} = 335\ 400 + 16\ 770 + 16\ 770 + 6\ 708 = 375\ 648 \text{ тенге.}$$

4.3.2 Расчет годовых эксплуатационных расходов

$$\sum Э = ФОТ + О_c + М + Сэл + А + Н \qquad (4.5)$$

где ФОТ – фонд оплаты (основная и дополнительная заработная плата);

$О_с$ – социальный налог (11% от ФОТ); $С_{эл}$

М – материальные затраты и запасные части (расходы на запасные части и текущий ремонт составляют 0,5% от капитальных вложений);

$С_{эл}$ – электроэнергия для производственных нужд;

А – амортизационные отчисления;

Н – накладные расходы (косвенные расходы, сюда можно отнести все неучтенные расходы – управленческие, хозяйственные, затраты на обучение кадров, транспортные расходы). Обычно это 75% от себестоимости.

Аппаратура передачи сигналов IP-телефонии рассчитана на 100% рабочий цикл и получает питание от электросети общего пользования. Поэтому для обслуживания объекта достаточно 1 инженера.

Таблица 4 .3 – Обслуживающий персонал [http://mojazarplata.kz/]

Должность	Оклад, тенге	Количество	Сумма, тенге
Инженер	120 000	1 ставки	120 000

Фонд оплаты труда (ФОТ) складывается из основной и дополнительной заработной платы и рассчитывается по формуле:

$$ФОТ = ЗП_{осн} + ЗП_{доп} \qquad (4.6)$$

Расчет основной заработной платы произведем следующим образом:

$$ЗП_{осн} = ЗП\ мес \cdot 12 \qquad (4.7)$$

Произведем расчет ЗП до внедрения нового оборудования и после внедрения:

$$ЗП_{осн} = 120\ 000 \cdot 12 = 1\ 440\ 000 \text{ тенге}$$

Расчет дополнительной заработной платы будем производить по формуле:

$$ЗП_{доп} = 0{,}3 \cdot ЗП_{осн} \quad (4.8)$$

$$ЗП_{доп} = 0.3 * 1\ 440\ 000 = 432\ 000 \text{ тенге}$$

Таким образом, фонд оплаты труда будет равен:
ФОТ = 1 440 000 + 432 000= 1 872 000 тенге

Социальный налог составляет 11 процентов фонда оплаты труда, за вычетом отчислений в пенсионный фонд (ПФ), в размере 10% от ФОТ и рассчитывается по формуле:

$$О_с = 0{,}11 \cdot (ФОТ - ФОТ \cdot 0{,}1)$$

$$О_с = 0{,}11 \cdot (1\ 872\ 000 - 1\ 872\ 000 \cdot 0{,}1) = 185\ 328 \text{ тенге.}$$

Материальные затраты и запасные части (расходы на запасные части и текущий ремонт составляют 0,5% от капитальных вложений) и рассчитываются по следующей формуле

$$М = К \cdot 0{,}005 \quad (4.10)$$

$$М = 375\ 648 \cdot 0{,}005 = 1\ 878{,}16 \text{ тенге}$$

Затраты на электроэнергию рассчитаем по формуле:

$$С_{эл} = W \cdot T \cdot S \quad (4.11)$$

где *W* – потребляемая мощность, W=0,3 кВт;
T – количество часов работы, T=8 760 ч/год;
S – стоимость киловатт-часа электроэнергии, S=16,02 тг/кВт-час.
[http://www.esalmaty.kz/index.php/ru/rates-and-services/tariff-plans]

$$С_{эл} = 0,3 \cdot 8\,760 \cdot 16,02 = 42\,100,56 \text{ тенге}$$

Величина амортизационных отчислений (А) рассчитывается как:

$$A = \sum_{i=1}^{n} H_{ai} \Phi_a \tag{4.12}$$

где H_{ai} - норма амортизационных отчислений от среднегодовой стоимости основных производственных фондов, в процентах;

Φ_a - среднегодовая стоимость основных фондов (капитальных вложений).

Так как компьютеры были ранее установлены, то мы рассчитываем амортизационные отчисления только для программного обеспечения.

Нормы амортизационных отчислений для отрасли связи (до 25% в год), кроме компьютерной техники (до 40% в год).

$$А = К \cdot 0,25 \tag{4.13}$$

$$А = 375\,648 \cdot 0,25 = 93\,912 \text{ тенге}$$

Накладные расходы рассчитываются по формуле:

$$Н = К \cdot 0,75 \tag{4.14}$$

$$Н = 375\,648 \cdot 0,75 = 281\,736 \text{ тенге}$$

Таким образом, согласно формулы (4.5) эксплуатационные расходы до внедрения составят:

$Э_0$ = 1 872 000 +185 328 +1 878,16 +42 100,56 +281 736 =2 383 042,72 тенге

После внедрения:

$Э_1$ = 1 872 000 +185 328 +1 878,16 +42 100,56 +281 736+93 912=2 476 954,72 тенге

4.4 Расчет финансовых результатов реализации проекта

Экономический эффект можем рассчитать по формуле:

$$E = (Пб – Пп)/К \quad (4.15)$$

где Е - экономический эффект;

Пб – затраты базового варианта включая годовые расходы ММТС;

Пп – затраты проектируемого варианта включая годовые расходы ММТС.

Пб = 331 500+2 383 042,72 = 2 714 542,72 тенге;

Пп = 52 000+2 476 954,72= 2 528 954,72тенге;

Экономическая эффективность равна:

$$E = (2\ 714\ 542{,}72 – 2\ 528\ 954{,}72)/375\ 648 = 0{,}49. \quad (4.16)$$

Срок окупаемости данного проекта равен:

$$T = 1/E \quad (4.17)$$

$$T = 1/0{,}49 = 2{,}05$$

4.5 Расчет абсолютной величины чистого дохода с учетом дисконтирования

Коэффициент дисконтирования (PV) – это норматив приведения, при установлении которого следует учитывать инфляционное изменение покупательной способности денег в течение рассматриваемого периода времени, необходимость обеспечения минимального гарантированного уровня доходности и риск инвестора.

Величина расчетного срока окупаемости составляет 2,05 года, что, в свою очередь, ниже величины нормативного срока окупаемости, который составляет 5 лет.

Так как деньги имеют временную ценность, то в расчетах проекта следует их учесть. Ставка дисконтирования составляет r_0 =20%

Коэффициент дисконтирования рассчитывается по формуле:

$$PV = \frac{ОЧДП}{(1+0{,}2)^1} \quad (4.18)$$

где r – ставка дисконты, r = 0,20;

n – год.

1 год $\quad PV = \frac{185588}{(1+0{,}2)^1} = 154\ 656{,}67$ тг

2 год $PV = \frac{185588}{(1+0,2)^2} = 128\ 880,56$ тг

3 год $PV = \frac{185588}{(1+0,2)^3} = 107\ 400,46$ тг

Определим капитальные вложения методом расчета абсолютной величины чистого дохода NPV. Чистая приведенная стоимость проекта будет определяться следующей формулой:

$$NPV = \sum_{t=1}^{n} PV - K, \quad (4.19)$$

где NPV – чистая приведенная стоимость, тг;

PV_t – текущая стоимость доходов за t-ый год, тг;

K – капиталовложения, тг.

$$NPV = (154656,67 + 128880,56 + 107400,46) - 375648 = 15\ 289,69 \text{ тг}$$

Значение NPV получилось больше нуля, поэтому можно сделать вывод, что проект может возместить первоначальные траты, также приносить прибыль.

Теперь необходимо определить индекс рентабельности данного проекта, то есть отношение суммарного дисконтированного дохода к суммарным дисконтированным затратам. Индекс рентабельности вычисляется по следующей формуле:

$$PI = \sum_{t=1}^{n} PV/K \quad (4.20)$$

$$PI = \frac{154656,67 + 128880,56 + 107400,46}{375648} = 1,04$$

Индекс рентабельности получился больше единицы, это значит, что проект можно принять.

Теперь вычислим дисконтированный период окупаемости(DPP) по формуле:

$$DPP = t + \frac{K-(П_1+П_2+\cdots+П_{n-1})}{П_n} \quad (4.21)$$

где t – количество лет, за которые капиталовложения окупятся без учета дисконтирования, t = 2;

К – капиталовложения;

$П_n$ – прибыль по годам (возьмем значение чистой прибыли с учетом дисконтирования).

$$DPP = 2 + \frac{375\,648 - (154656{,}67 + 128880{,}56)}{107400{,}46} = 2{,}8 \text{ года}$$
$$\approx 2 \text{ год}a\ 10 \text{ месяцев}$$

4.6 Ожидаемые результаты внедряемого проекта

За счет внедрения IP телефонии упрощается администрирование маршрутизации звонков (таблица 4.4)

Таблица 4.4 - Потенциальный эффект применения проекта

Сфера воздействия	Дает возможность совершать междугородние и международные телефонные звонки с телефонов ЦАТС компании и с IP телефонов ЛВС компании
Управление	Уменьшение издержек на междугородние и международные переговоры. Усиление контроля за переговорами. Простота настройки маршрутизации звонков
Информационная система	Совершенствование структуры потоков информации Со временем замена телефонной сети, что приводит к уменьшению морального устарения технологии и оборудования. Обмену информации посредством сети.

Таблица 4.5 – Итоговая таблица показателей экономической эффективности

Наименование	Сумма, тыс. тг
Капитальные затраты	375 648,00
Экономический расчет	2 476 954,72
Условная прибыль	185 588,00
Экономическая эффективность	0,49
Срок окупаемости до дисконтирования, год	2,05
Срок окупаемости после дисконтирования, год	2,8

5 Безопасность жизнедеятельности

5.1 Анализ условий труда

Аппаратно-программный комплекс для работы IP-телефонии включает в себя оборудование:

а) телефонный шлюз;

б) управляющий сервер;

в) сервер адресов;

г) транспортная сеть IP,

которое питается от сети напряжением 220 В, частотой 50 Гц, полная мощность 1,5 кВт и состоит из восьми штативов размером 185 м×87 м×80 м (высота×длина×ширина) и двух стоек размером 185 м×261 м×80 м.

Данное оснащение располагается в помещении автоматного зала размером 10 м×5 м×4,5 м, объемом 175 м^3. В комнате находятся два световых проема размером 3,7 м×2,5 м, выходящие на запад.

Под операторской имеется помещение с размерами 10 м×5 м×4,5 м, где также находятся два световых проема размером 3,7 м×2,5 м, выходящие на восток. В помещении имеется семь рабочих мест операторов, оснащенных персональными компьютерами. Сообразно санитарным нормам на одного человека рабочая зона составляет 5 м^2. Размеры помещения удовлетворяют вышеуказанным условиям.

Каждое рабочее место организовано с учетом ГОСТ 21958-76 “Система “человек-машина”. Зал и кабины операторов. Расположение рабочих мест. Общие эргономические требования” [11].

Функционирование машины ориентировано на преобразование информации и состоит в упорядоченной совокупности машинных операций, предназначенных для решения предписанной задачи.

Расположение технических средств и кресла оператора в рабочей зоне обязано гарантировать удобный доступ к основным функциональным узлам и блокам аппаратуры, исключение случайного приведения в действие средств управления и ввода информации, комфортную рабочую позу и позу отдыха [12].

Режим труда и отдыха

В согласовании с требованиями СНиП режим труда и отдыха организовывается в зависимости от вида и категории трудовой деятельности при работе на персональном компьютере (ПК).

Виды трудовой деятельности приведены в таблице 5.1.

Таблица 5.1 – Виды трудовой деятельности

Группа	Вид трудовой деятельности
А	Работа по считыванию информации с экрана предварительным запросом;
Б	Работа по вводу информации;
В	Работа в режиме диалога с ПК

Большую часть рабочего времени операторы прибывают в помещении операторской, однако временами операторам приходится находиться в помещении автоматного зала. Для снабжения оптимальной работоспособности и сохранения здоровья пользователей на протяжении рабочей смены устанавливаются регламентированные перерывы, продолжительность которых зависит от длительности рабочей смены, вида и категории трудовой деятельности. Продолжительность работы с ПК без перерыва не превышает двух часов.

Рабочий день операторов составляет восемь часов. При работе с ПК в ночную смену (с 22 до 6 часов) суверенно от категории и вида трудовой занятии, длительность перерывов увеличивается на 60 минут.

Помещение IP-телефонии соответствует категории 1а – легкая физически, так как работа производится сидя и не требует физического напряжения, а энергозатраты организма (расход энергии при выполнении работы) составляют менее 138 ккал/ч [12].

Помещение автоматного зала, где размещается оборудование, считается помещением с повышенной опасностью, так как имеет следующие признаки:

а) температура воздуха до 30^0С;

б) влажность до 60%;

в) присутствие токопроводящего пола

Таблица 5.2 – Категория условий труда

Категория работы с ПК	Уровень нагрузки за рабочую смену			Суммарное время регламентированных перерывов	
	Группа А, кол. знак.	Группа Б, кол. знак.	Группа В, час.	При 8-ми часовой смене	При 12-ти часовой смене
1а	до 20000	до 15000	до 2,0	30	60

Микроклимат помещения

Снабжение характеристик микроклимата в помещении операторов IP-телефонии. Для обеспечения нормальных условий труда для персонала и надежности технологического процесса установлены нормы производственного микроклимата, которые приведены в таблице 5.3.

Поскольку в помещении операторской производится наиболее 60%, а также исходя из категории работы, температура воздуха превосходит возможные допустимые нормы, т.е. в помещении все время находится обслуживающий персонал, который выделяет тепло.

Чтобы восстановить микроклимат используют системы вентиляции и кондиционирования воздуха. Однако эти системы представляют дополнительную пожарную угрозу для помещения, так как с одной стороны они гарантируют подачу кислорода во все помещения, а с другой - при происхождении пожара быстро распространяют огонь и продукты горения.

Таблица 5.3 – Нормы микроклимата

Период года	Категория работ	Температура, ^{0}C				Относительная влажность			Скорость движения воздуха		
		Оптимальная	Допустимая на раб.месте		Фактическая	Оптимаьная	Допустимая на рабочем метсе	Фактическая	Оптималная	Допустимая на рабочем месте	Фактическая
			Постоянных	**Непостоянных**							
Холодный	1а	22-24	21-25	18-26	25-28	40-60	75 при 28^{0}C	60-65	0,1	0,1	0,1
Теплый	1а	23-25	22-28	28-30	28-30	40-60	55 при 28^{0}C	40-45	0,1	0,1-0,2	0,1

Таблица 5.4 – Допустимые уровни звукового давления.

Помещение	Среднестатистические частоты активных полос, Гц								Уровни звука и эквивалентные уровни звука, дБ
	63	125	250	500	1000	2000	4000	8000	
• Комната ПК	71	61	54	49	45	42	40	38	50

Оборудование IP-телефонии относится к разряду шумных. Шум согласно ГОСТ 12.1.003-83 ССБТ “Шум. Общие требования безопасности” [20] должен соответствовать требованиям, представленным в таблице 5.4.

Действительное значение превосходит допустимый уровень на 15 дБ. Для борьбы с шумом применяют следующие мероприятия:

– рациональное размещение оборудования и рабочих мест;

– использование в качестве изоляции и снижения специальных крышек;

– своевременная замена изношенных деталей.

Естественное и искусственное освещение

Так как в помещении операторской непрерывно располагается обслуживающий персонал, следовательно, согласно СНиП II–4-79 “Естественное и искусственное освещение” обладаем естественное освещение, которое реализовывается через окна (боковое освещение).

Ввиду узких окон освещение рабочих мест операторов мало и составляет – 1,7%. Нормированное значение КЕО должно составлять 2,5% . Нормированное значение КЕО выбирается в зависимости от характеристики и разряда работы. Для данного объекта выполняемые работы – работы очень высокой точности. Так как освещение рабочих мест операторов от оконных проемов недостаточное, установлены светильники местного освещения для подсветки документов.

Исходя из данного анализа условий труда в помещении операторской произведем расчет параметров, не соответствующих нормированным значениям (таблица 5.5).

Таблица 5.5 – Сравнение нормированных и фактических параметров

		Нормированное значение	Фактическое значение
Освещение (КЕО), %		2,5	1,7
Температура, ^{0}С	Холодный период года	22-24	25-28
	Теплый период года	23-25	28-30

5.2 Расчет естественного освещения

Помещение, в котором непрерывно находятся операторы, требует наличие естественного освещения. При недостаточном естественном освещении требуется присутствие искусственного освещения.

В помещении используется естественное боковое освещение, которое характеризуется коэффициентом естественной освещенности (КЕО).

Размеры помещения: длина L = 10 м., ширина B = 5 м., высота H = 4,5 м.

Данное помещение находится в операторской с высотой рабочей поверхности h_p = 0,8 м., окна начинаются с высоты 0,8 м., высота окна h_o = 2,5 м. Освещение одностороннее.

Расчет естественного освещения заключается в определении площади световых проемов. При боковом освещении определяют площадь световых проемов (окон), S_o обеспечивающую нормированные значения КЕО, по формуле [20]:

$$100\,\frac{S_o}{S_n} = \frac{e_н \cdot \eta_o}{\tau_o \cdot \tau_1} \cdot K_{зд} \cdot K_з, \qquad (5.1)$$

где S_0 – площадь световых проемов при боковом освещении, м^2;

S_n – площадь пола помещения, м^2;

$e_н$ – нормированное значение КЕО (таблица 1.2);

η_o – световая характеристика окон (таблица 1.3);

$K_{зд}$ – коэффициент, учитывающий значение окон противостоящими зданиями (таблица 1.7);

$K_з$ – коэффициент запаса (таблица 1.10);

τ_o – общий коэффициент светопропускания, определяется по формуле:

$$\tau_o = \tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4, \qquad (5.2)$$

где r_1 – коэффициент, учитывающий повышение КЕО при боковом освещении благодаря свету, отраженному от поверхностей помещения и подстилающего слоя, прилегающего к зданию (таблица 1.2);

τ_1 – коэффициент светопропускания материала (таблица 1.5);

τ_2 – коэффициент, учитывающий потери света в переплетах светопроема (таблица 1.5);

τ_3 – коэффициент, учитывающий потери света в несущих конструкциях (таблица 1.5 (при боковом освещении $\tau_3 = 1$);

τ_4 – коэффициент, учитывающий потери света в солнцезащитных устройствах (таблица 1.5).

В качестве светопропускного материала используются пустотелые стекла двойных блоков, вид несущих покрытий – железобетонные. Из таблицы 1.5 [18] значения:

$$\tau_1 = 0{,}8; \quad \tau_2 = 0{,}7; \quad \tau_3 = 0{,}8; \quad \tau_4 = 0{,}8;$$

$$\tau_0 = 0{,}8 \cdot 0{,}7 \cdot 0{,}8 \cdot 0{,}8 = 0{,}36$$

$$S_0 = \frac{S_п \cdot e_н \cdot \eta_о \cdot K_{зд} \cdot K_з}{100 \cdot \tau_о \cdot r_1}, \qquad (5.3)$$

Определим значения всех составляющих, пользуясь таблицами.

$$S_п = B \cdot L = 10 \cdot 5 = 50 \text{ м}^2$$

а) $l_п^{IV} = e_н^{III} \cdot m \cdot c$;

б) $m = 0{,}9$;

в) $c = 0{,}75$;

г) $e_п^{III} = 2$ т.к. для работ высокой точности;

д) $l_п^{Iv} = 2 \cdot 0{,}9 \cdot 0{,}75 = 1{,}35$.

Определим $\eta_о$ из таблицы 1.3 [20].

Отношение длины к глубине (т.е. наиболее удаленной точки от окон):

$$L : B = 10 : 5 = 2$$

Отношение $B : h_1 = 5 : 3{,}3 = 1{,}51$,

где $h_1 = h_p + h_o = 0{,}8 + 2{,}5 = 3{,}3$ м

Таким образом, $\eta_о = 9$

Средний коэффициент отражения в цехе $\rho_{ср} = 0{,}4$, т.к. одностороннее боковое освещение.

Определяем значение r_1 из таблицы 1.6

$$B : h_1 = 1{,}51, \qquad l : B = 2{,}5 : 5 = 0{,}5 \quad (l = \frac{B}{2})$$

принимаем $r_1 = 1{,}2$;

$К_{зд}$=1, т.к. рядом нет зданий, затеняющих окна;

$К_з$= 1,3.

Тогда

$$S_0 = \frac{50 \cdot 1{,}35 \cdot 9 \cdot 1 \cdot 1{,}3}{100 \cdot 0{,}36 \cdot 1{,}2} = \frac{789.75}{43.2} = 18.3 \text{ м}^2$$

Так как высота оконных проемов 2,5 м, то, следовательно, ширина их составит 18,3 : 2,5 = 7,32 м.

Расчет искусственного освещения

Так как при исполнении в помещении работ высочайшей точности естественного освещения недостаточно, рекомендуется использование комбинированного освещения. При комбинированном освещении к общему добавляется местное освещение, сосредоточивающее световой поток непосредственно на рабочих местах.

Проектирование искусственного освещения заключается в решении задач:

– выбор системы освещения;

– типа источника света;

– расположение светильников;

– выполнение светотехнического расчета;

- определение мощности осветительной установки.

Для искусственного освещения избираем лампы газоразрядные, низкого давления, так как они являются более экономичными:

номинальная мощность, Вт..... 40

номинальный световой поток, лк..... 3120

диаметр, мм..... 40

длина со штырьками, мм..... 1212,6

Расчет производится по двум способом: способу коэффициента использования и точечному способу.

Способ коэффициента применения специализирован для расчета всеобщего равномерного освещения горизонтальных поверхностей при отсутствии больших затеняющих предметов. Способ содержится в определении значения коэффициента η, одинокого отношению светового потока, падающего на расчетную плоскость, к полному потоку осветительного прибора.

Значение η находятся из таблиц, связывающих геометрические параметры помещений (индекс помещений i) с их оптическими характеристиками (коэффициентами отражения потолка $\rho_{пот}$, стен $\rho_{ст}$, пола $\rho_п$).

а) $\rho_{пот}$ = 70% , $\rho_{ст}$ = 50%, $\rho_{пол}$ = 30%;

б) наивыгоднейшее расстояние между светильниками определяется как

$$z = \lambda \qquad h = 1{,}2 \cdot 3{,}2 = 3{,}84\text{м}; \qquad \lambda = 1{,}2 \div 1{,}4, \tag{5.4}$$

в) $$i = \frac{A \cdot B}{h(A+B)} \text{ (формула индекса помещения)}, \tag{5.5}$$

где А – длина помещения – 10 м;

В – ширина помещения – 5 м;

h – расчетная высота – 0,8 м.

Так как высота свеса ламп – 0,5 м, то h = 4,5 – (0,8 + 0,5) = 3,2 м.

Определим индекс помещения

$$i = \frac{10 \cdot 5}{3.2 \cdot (10+5)} = \frac{50}{48} = 1.04$$

Коэффициент использования находим по таблице 2.5 [20] η = 49%, а коэффициент запаса – по таблице 1.10 [20] $К_з$ = 1,3

Подставим в формулу (5.6) эти значения и определим количество люминесцентных ламп.

$$N = \frac{E \cdot K_з \cdot S \cdot Z}{n \cdot \Phi_л \cdot \eta}, \tag{5.6}$$

где Е – заданная минимальная освещенность;

$К_з$ – оэффициент запаса ($К_з$ = 1,3);

S – освещаемая площадь, (S = 50 м^2);

Z – коэффициент неравномерности освещения, Z = 1,1÷1,2;

N – число светильников;

$Ф_л$ – световой поток выбираемой лампы;

n – количество ламп в светильнике, (n = 4).

$$N = \frac{500 \cdot 1{,}3 \cdot 50 \cdot 3.84}{4 \cdot 3120 \cdot 0{,}49} = \frac{124800}{6115{,}2} = 18 \text{ светильников}$$

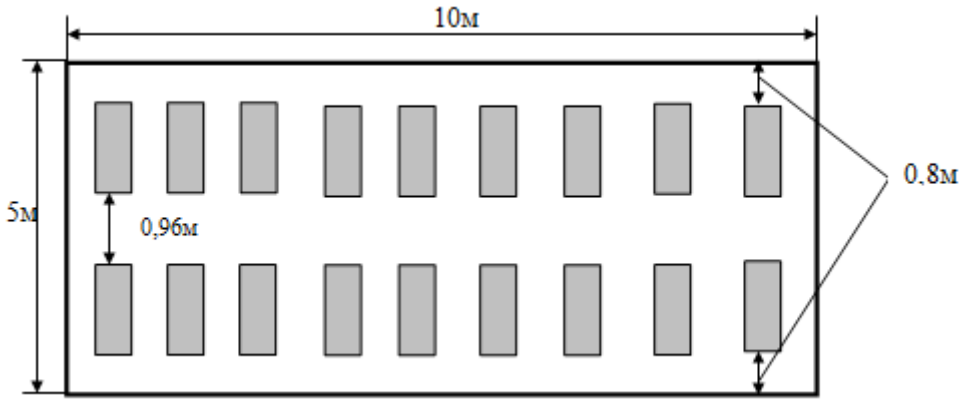

Рисунок 5.1 – План размещения светильников

Светильники располагаем в два ряда с расстоянием между ними 0,96 м (учитывая, что длина лампы 1213,6 мм).

Всего для организации нормируемой освещенности 500 лк достаточно 18 светильников с лампами ЛБ мощностью 40 Вт.

По точечному способу при круглосимметричных точечных излучателях используется, что световой поток лампы (или суммарный световой поток ламп) в каждом светильнике равен 1000лм. Создаваемую таким светильником освещенность называют условной. Световой поток лампы в каждом светильнике определяется по формуле:

$$\Phi = \frac{1000 \cdot E \cdot K_з}{\mu \cdot \sum E_y}, \qquad (5.7)$$

где μ – коэффициент, учитывающий действие “удаленных” светильников (μ = 1,1 ÷1,2);

$\sum E_y$ – суммарная условная освещенность в контрольной точке;

E_y – отдельного светильника определяется по графикам пространственных изолюкс [18].

В качестве контрольных выбираются точки, в которых $\sum E_y$ имеет наименьшее значение.

Нормируемая освещенность – 500лк, разряд зрительной работы – высокой точности, коэффициент запаса $К_з$ – 1,3, полностью пыленепроницаемые светильники установлены на высоте 4,5м, высота рабочей поверхности над полом $h_р$ – 0,8м, высота светильника над освещенной поверхностью

h = 4 – 0,8 = 3,2 м

Выбираем светильник ЛВ001 4х40, для которого

$$\lambda : h = 1{,}7 \text{ м}$$

отсюда

$$\lambda = 1{,}7 \cdot h = 1{,}7 \cdot 3{,}2 = 5{,}44 \text{ м}$$

Устанавливаем два ряда светильников.

Намечаем контрольную точку О. Для нее ближайшие четыре светильника находятся на расстоянии d=2 м., h=4 м.

На рисунке 2.2.б [18] проводим горизонтальную линию от точки h=2 м до пересечения с вертикальной линией, опущенной из точки d=2,5 м.

Точка пересечения А лежит на изолюксе 10 лк. Следовательно, каждый из четырех светильников создает условную освещенность по 10 лк, а всего 40 лк.

Для двух следующих светильников d=2,3 м, они создают условную освещенность по 5лк каждый (точка В), т.о.:

$$\sum E_{у} = 40 + 10 = 50 \text{ лк}$$

.

Световой поток вычислим по формуле:

$$Ф = \frac{1000 \cdot 500 \cdot 1{,}3}{11{,}2 \cdot 50} = 14220 \text{ лм}$$

По таблице 2.3 [18] выбираем люминесцентную лампу ЛБ 20-2 со световым потоком 1060 лм, мощностью 40 Вт.

5.3 Расчет системы кондиционирования

Наиболее актуальным способом и средством, обеспечивающим чистоту и нормальный микроклимат помещения, является кондиционирование, т.е. создание искусственного микроклимата в производственном помещении с помощью кондиционирующих установок. Кондиционирование помещений выполняется в соответствии с требованиями СНиП II-33-75 «Отопление, вентиляция и кондиционирование воздуха» [19].

Количество воздуха L ($м^3$/ч), которое необходимо вывести за один час из производственного помещения (операторской), чтобы вместе с ним удалить избыток тепла $Q_{изб}$ (ккал/ч), определяется по формуле:

$$L = \frac{Q_{изб}}{C_в \cdot t \cdot y_в}, \tag{5.8}$$

где $C_в$ – теплоемкость сухого воздуха ($C_в$ – 0,24 ккал/кг·град);

$t = t_{ух} - t_{вх}$ – разность температур уходящего и входящего воздуха (при расчетах принимаем $t = 5\ ^0C$, т.е. $t_{ух} = 28\ ^0C$, $t_{вх} = 23\ ^0C$);

$y_в$ – плотность уходящего воздуха, определяемая в зависимости от температуры (при расчетах принимаем $y_в = 1{,}2$ кг/м^3).

Избыточное тепло – разность тепловыделений в помещении и теплоотдачи через наружные ограждения в окружающую среду:

$$Q_{изб} = Q_{об} + Q_{осв} + Q_л + Q_р + Q_{отд}, \quad (5.9)$$

где $Q_{об.}$, $Q_{осв.}$, $Q_л$ – тепло, выделяемое производственным оборудованием, системой искусственного освещения и работающим персоналом соответственно, ккал/ч;

$Q_р$ – тепло, вносимое в помещение солнцем (солнечная радиация), ккал/ч;

$Q_{отд}$ – теплоотдача естественным путем, ккал/ч.

Тепло, выделяемое производственным оборудованием:

$$Q_{об} = 860 * P_{об} * \eta, \quad (5.10)$$

где 860 – тепловой эквивалент 1 кВт/ч;

$P_{об}$ – мощность, потребляемая оборудованием, кВт/ч;

$P_{об}$ – 1.98 кВт/ч;

Н – коэффициент перехода тепла в помещение, для данного цеха = 0.75,

$$Q_{об} = 860* 1.98 * 0.75 = 1277.1 \text{ ккал/ч}.$$

Тепло, выделяемое осветительными установками:

$$Q_{осв} = 860 * P_{осв} * \alpha * \beta * \cos \varphi, \quad (5.11)$$

где $P_{осв}$ – мощность осветительных установок, кВт/ч;

$P_{осв}$ – 40 Вт, так как применяются люминесцентные лампы именно этой мощности;

α – КПД перехода электрической энергии в тепловую, $\alpha = 0{,}1$;

β – КПД одновременной работы аппаратуры в помещении. В цехе работает вся аппаратура, $\beta = 1$;

$$\cos \varphi = 0{,}7.$$

$$Q_{осв} = 860*8*0{,}1*0{,}7*1= 2{,}408 \text{ ккал/ч},$$

Тепло, выделяемое людьми:

$$Q_л = К_л(q - q_{шп}), \quad (5.12)$$

где $К_л$ – количество работающих, $К_л$=7 чел.;

$(q - q_{шп})$ – тепловыделение одного человека по графику;

q – тепловыделение одного человека на данной категории работ q =250 ккал/ч ;

$q_{ит}$ – тепло, затрачиваемое на испарение тела, $q_{ит}$= 150 ккал/ч.

$$Q_л = 7 * (250-150) = 7 * 100 = 700 \text{ ккал/ч}$$

Тепло, вносимое солнечной радиацией:

$$Q_р = mFq_{ост}, \quad (5.13)$$

где m – количество окон в помещении, m=2;

F – площадь одного окна, м^2, F=9.13 м^2;

$Q_{ост}$ – солнечная радиация через остекленную поверхность, т.е. количество тепла, вносимое за один час через остекленную поверхность площадью 1м^2, ккал/ч.

$$Q_р=2*9.13*145 =2653.5 \text{ ккал/ч.}$$

Теплоотдачу естественным путем через конструкции помещения принимаем:

а) для холодного периода $Q_{отд}$ = 2000 ккал/ч;

б) для теплого периода $Q_{отд}$ = 0 ккал/ч

Рассчитаем избыточное тепло $Q_я$ для двух периодов и найдем необходимый воздухообмен в помещении:

а) для холодного периода:

$$Q_{изб}= 1277.1+2,408 +2653.5 -2000 = 1933 \text{ ккал/ч,}$$

$$G_{изб} = 1933/(31-28)*1,2 = 1933/3.6= 537 \text{ м}^3\text{/ч.}$$

б) для теплого периода:

$$Q_{изб} = 1933 \text{ ккал/ч,}$$

$$G_{изб}= 1933/(31-23)*1,2 = 1933/9,65 = 200 \text{ м}^3\text{/ч}$$

Необходимый воздухообмен рассчитываем по формуле (5.8):

$$L=\frac{200}{0,24\cdot 5\cdot 1,2}=138,9 \text{ ì}^3/\div,$$

Отношение количества воздуха, поступающего в помещение за один час, к объему помещения называется кратностью воздухообмена [17]:

$$К = L / V_п \text{ , (3.13)}$$

где $V_п$ – объем помещения ($V_п$ = 175 м^3).

$$К = 138,9 / 175 = 0,794$$

В данном помещении можно установить два параллельно подключенных кондиционера типа БК-1500, рассчитанные на площадь не более 25 м^2.

Его потребляемые характеристики:

потребляемый ток, А 5

потребляемая мощность, ВТ 1800

напряжение, В 220

частота, Гц 50

5.4 Выводы по пятой главе

Каждое рабочее место организованно учетом ГОСТ 21958-76 “Система “человек - машина”. Зал и кабинеты операторов. Расположение рабочих мест. Общие эргономические требования”, для удобств выполнения работниками движений и действий.

В соответствие с зависимостью от взрывопожарной и пожарной опасности здания и помещения рассматриваемый объект соответствует категории В пожароопасное. Учитывая высокую стоимость оборудования, а так же в специфику загорания ПК в помещении установлены пять дымовых извещателей.

Производственное освещение удовлетворяет требованиям СНиП 2-4-79. Всего для создания нормируемой освещенности необходимы двадцать ламп ЛБ мощностью 40 Вт.

Заключение

В дипломной работе был дан анализ обеспечения безопасности соединения в сетях IP-телефонии. Были проанализированы возможности протоколов VoIP-телефонии с точки зрения обеспечения безопасности, было приведено сравнение наиболее известных механизмов безопасности для технологии VoIP, проанализирован вариант защиты информации в канале за счет использования технологии виртуальных частных сетей на базе протокола IPSec. Так же были проанализированы кодеки для обеспечения IP-телефонии. Как результат, был выбран кодек с наилучшими показателями. Была выработана рекомендация по обеспечению безопасности соединения в сетях IP- телефонии и представлен сценарий установления безопасного VoIP-соединения. В работе были смоделированы и рассмотрены различные атаки на сеть IP-телефонии и предложены варианты защиты.

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

Список литературы

1 Амато В. Основы организации сетей Cisco. Том 1. М.: издательский дом «Вильямс», 2002.

2 Амато В. Основы организации сетей Cisco. Том 2. М.: издательский дом «Вильямс», 2002.

3 Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP телефония. М.: Радио и связь, 2001.

5 Лукацкий А.В. Атаки на VPN. «Компьютер-Пресс», №3. 2002.

6 Лукацкий А.В. IP-опасность для бизнеса. «Мир связи. Connect», N8. 2002.

7 Лукацкий А.В. Системы обнаружения атак. «Сетевой», №4. 2002.

8 Davidson J., Peters J., Voice Over IP Fundamentals- Cisco Press, 2006

9 Росляков А.В., Самсонов М.Ю., Шибаева И.В. IP телефония. М.: Эко-Трендз, 2003.

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

11 Б.Я Рябко, А. И. Фионов. Криптографические методы защиты информации. Учебное пособие-М, Горячая линия телеком, 2009

12 Уэнстром Майкл. Организация защиты сетей Cisco. М.: издательский дом «Вильямс», 2003.

13 Материалы сайта НПО Информ-защита http://www.infosec.ru

14 Материалы сайта НИИ Телекоммуникационных систем http://www.niits.ru

15 http://www.comptek.ru/iptelephony/articles/index/html

16 http://ixi.ru/voip.html

17 http://www.informsviaz.kz/catalog/addpac/addpac_voip/gateway_VOIP.html

18 Байкенов А.С Технические средства защиты информации в ТКС, для магистрантов спец. 6М050719, АУЭС, 2009,- 17от

19 Practical VoIP Security. Томас Портер, Жан Канклирц, Syngpress, 2010

20 Хакимжанов Т.Е. Безопасность жизнедеятельности. Расчет аспирационных систем. Дипломное проектирование. – Алматы,2002

21 Организация и планирование производства. Управление предприятием: методические указания к экономической части дипломных проектов для специальностей 3803; АИЭС А- ты 2004.-117с

22 Охрана труда на предприятиях связи. /Под ред. Баклашова Н.И. – М.: Радио и связь.-2005. 124с

Приложение А

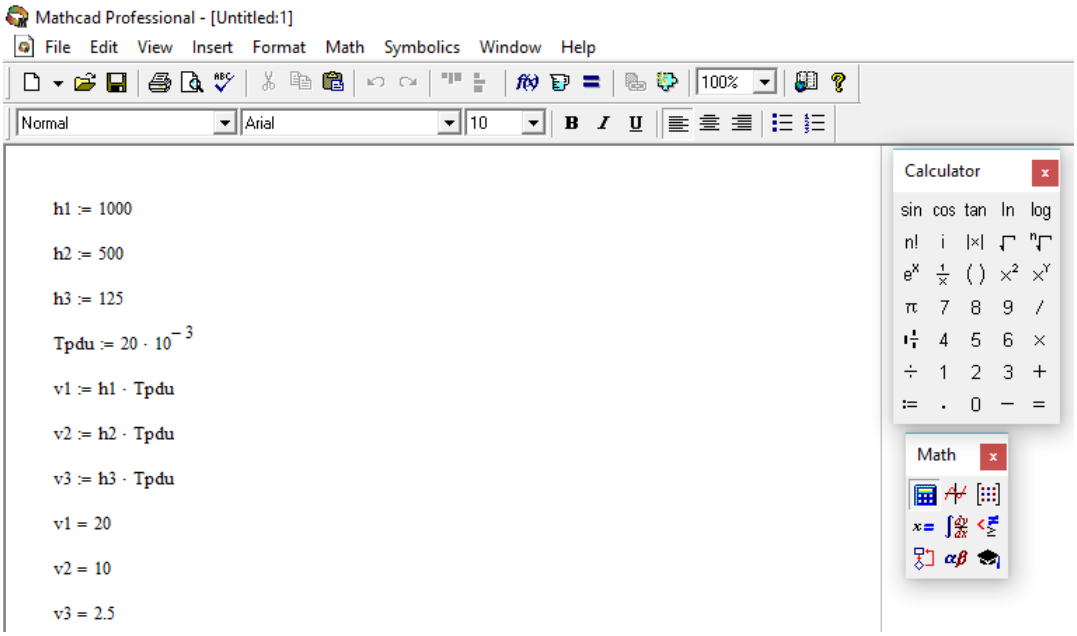

Рисунок А.1 - Расчет размеров пакетированных данных

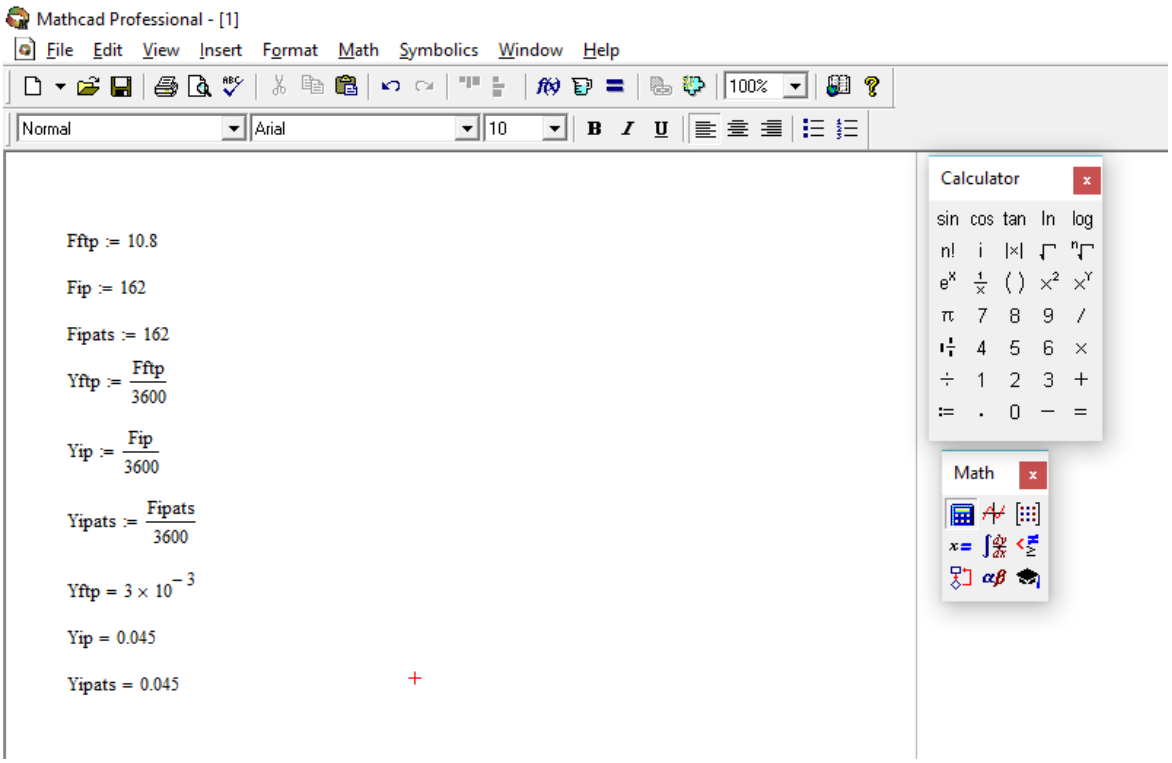

Рисунок А.2 – Расчет число заявок, поступающих от абонента каждой службы

Mathcad Professional - [2]

File Edit View Insert Format Math Symbolics Window Help

$n1j := 50$

$t3 := 1$

$\pi_3 := 0.25$

$N := 40$

$Fftp := 10.8$

$N3tj := n1j \cdot t3 \cdot \pi_3 \cdot N \cdot Fftp$

$N3tj = 5.4 \times 10^3$

$N31d := 4.26 \cdot 10^6$

$N32d := 8.52 \cdot 10^6$

$N33d := 34.08 \cdot 10^6$

$N31 := N3tj + N31d \qquad N31 = 4.265 \times 10^6$

$N32 := N3tj + N32d \qquad N32 = 8.525 \times 10^6$

$N33 := N3tj + N33d \qquad N33 = 3.409 \times 10^7$

Рисунок А.3 – Число пакетов, генерируемое третьей группой

Mathcad Professional - [Untitled:2]

File Edit View Insert Format Math Symbolics Window Help

$N11 := 16.2 \cdot 10^6$

$N21 := 8.755 \cdot 10^6$

$N31 := 4.265 \cdot 10^6$

$N22 := 9.41 \cdot 10^6$

$N32 := 8.525 \cdot 10^6$

$N23 := 13.34 \cdot 10^6$

$N33 := 34.085 \cdot 10^6$

$N1 := N11 + N21 + N31 \qquad N1 = 2.922 \times 10^7$

$N2 := N11 + N22 + N32 \qquad N2 = 3.413 \times 10^7$

$N3 := N11 + N23 + N33 \qquad N3 = 6.362 \times 10^7$

$Nsek1 := \frac{N1}{3600} \qquad Nsek1 = 8.117 \times 10^3$

$Nsek2 := \frac{N2}{3600} \qquad Nsek2 = 9.482 \times 10^3$

$Nsek3 := \frac{N3}{3600} \qquad Nsek3 = 1.767 \times 10^4$

Рисунок А.4 – Расчет суммарное и средное число пакетов

Mathcad Professional - [4]

File Edit View Insert Format Math Symbolics Window Help

$N1 := 29.22 \cdot 10^{6}$

$N2 := 34.14 \cdot 10^{6}$

$N3 := 63.63 \cdot 10^{6}$

$N11 := 16.2 \cdot 10^{6}$

$N21 := 8.755 \cdot 10^{6}$

$N31 := 4.265 \cdot 10^{6}$

$N12 := 16.2 \cdot 10^{6}$

$N22 := 9.41 \cdot 10^{6}$

$N32 := 8.525 \cdot 10^{6}$

$N13 := 16.2 \cdot 10^{6}$

$N23 := 13.34 \cdot 10^{6}$

$N33 := 34.085 \cdot 10^{6}$

$N11\% := \frac{N11 \cdot 100}{N1}$ $\quad N11\% = 55.441$

$N21\% := \frac{N21 \cdot 100}{N1}$ $\quad N21\% = 29.962$

$N31\% := \frac{N31 \cdot 100}{N1}$ $\quad N31\% = 14.596$

$N12\% := \frac{N12 \cdot 100}{N2}$ $\quad N12\% = 47.452$

$N22\% := \frac{N22 \cdot 100}{N2}$ $\quad N22\% = 27.563$

$N32\% := \frac{N32 \cdot 100}{N2}$ $\quad N32\% = 24.971$

$N13\% := \frac{N13 \cdot 100}{N3}$ $\quad N13\% = 25.46$

$N23\% := \frac{N23 \cdot 100}{N3}$ $\quad N23\% = 20.965$

$N33\% := \frac{N33 \cdot 100}{N3}$ $\quad N33\% = 53.567$

Рисунок А.5 – Расчет

Mathcad Professional - [5]

File Edit View Insert Format Math Symbolics Window Help

$\tau 1 := 1.214 \cdot 10^{-4}$

$\tau 2 := 1.041 \cdot 10^{-4}$

$\tau 3 := 5.62 \cdot 10^{-5}$

$\beta 1 := \frac{1}{\tau 1}$ $\quad \beta 1 = 8.237 \times 10^{3}$

$\beta 2 := \frac{1}{\tau 2}$ $\quad \beta 2 = 9.606 \times 10^{3}$

$\beta 3 := \frac{1}{\tau 3}$ $\quad \beta 3 = 1.779 \times 10^{4}$

Рисунок А.6 – Расчет интенсивности обслуживания

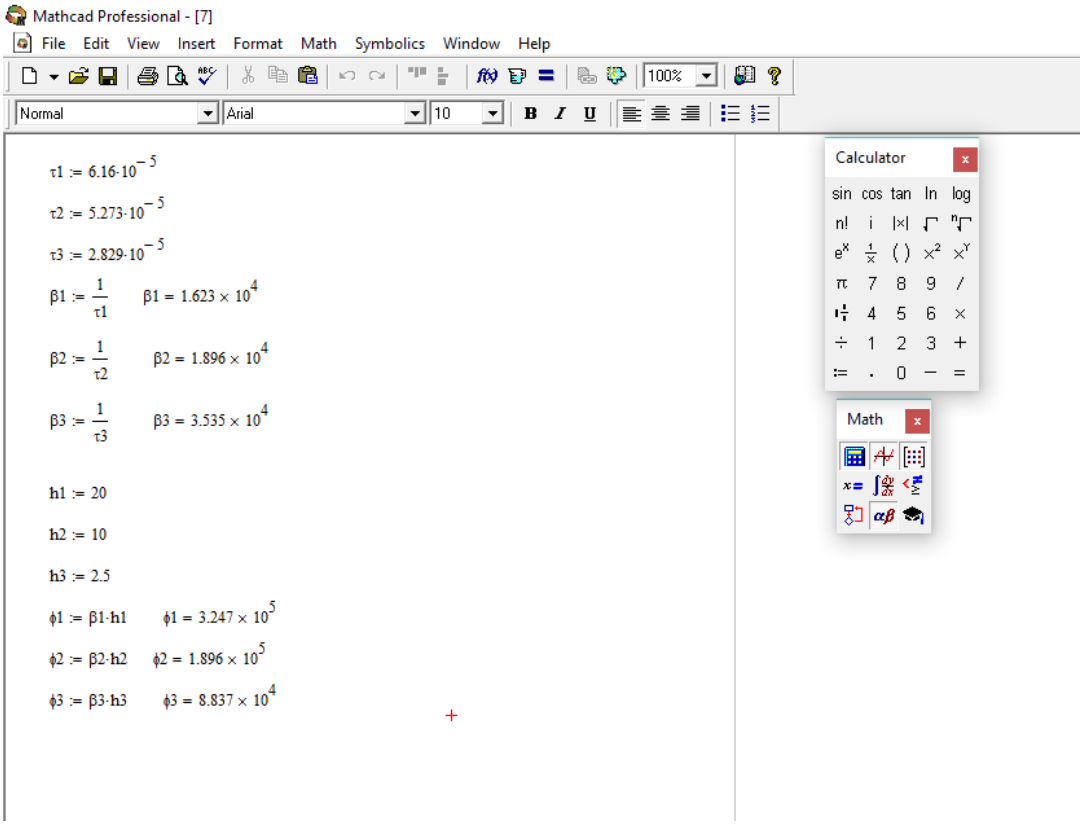

Рисунок А.7 – Расчет интенсивности обслуживания и требуемая полоса пропускания