

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»**
(Н И У « Б е л Г У »)

ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХ НАУК

Кафедра информационно-телекоммуникационных систем и технологий

**ПРОЕКТИРОВАНИЕ ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ
ГРУППЫ КОМПАНИЙ «МЕТАЛЛОТОРГ» В ЦЕНТРАЛЬНОМ ФЕДЕРАЛЬНОМ
ОКРУГЕ, С РАЗРАБОТКОЙ ИМИТАЦИОННОЙ МОДЕЛИ СЕТИ**

Выпускная квалификационная работа студентки

очной формы обучения

**направления подготовки 11.03.02 Инфокоммуникационные технологии и системы связи
4 курса группы 07001208**

Лазарак Евгении Алексеевны

Научный руководитель
канд. техн. наук, доцент,
доцент кафедры информационно-
телекоммуникационных систем и
технологий
НИУ «БелГУ» С.Н. Девицына

Рецензент
Ведущий инженер Белгородского
районного линейно-технического
цеха Белгородского городского
центра технической эксплуатации
телекоммуникаций г. Белгород
Белгородского филиала ПАО
«Ростелеком» П.М. Старченко

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	4
1 АНАЛИЗ СОСТОЯНИЯ СУЩЕСТВУЮЩЕЙ ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ ГРУППЫ КОМПАНИЙ «МЕТАЛЛОТОРГ».....	6
1.1 Описание объектов группы компаний «Металлоторг».....	7
1.2 Анализ существующей сети связи группы компаний «Металлоторг»...9	
1.3 Постановка задач проектирования.....	11
2 РАЗРАБОТКА КОНЦЕПЦИИ РЕАЛИЗАЦИИ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ ГРУППЫ КОМПАНИЙ «МЕТАЛЛОТОРГ».....	12
2.1 Проектирование транспортной сети связи.....	13
2.2 Проектирование сетей доступа в филиалах компании.....	17
2.3 Расчет нагрузок.....	19
2.3.1 Расчет трафика телефонии.....	19
2.3.2 Расчет трафика передачи данных	21
2.3.3 Расчет трафика предоставления услуг доступа к сети Internet.....	26
3 ПРОЕКТИРОВАНИЕ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ ГРУППЫ КОМПАНИЙ «МЕТАЛЛОТОРГ».....	29
3.1 Разработка сценария VPN.....	29
3.2 Разработка сети абонентского доступа в филиалах.....	30
3.2.1 Выбор оборудования.....	30
3.2.2 Расчет объема оборудования.....	43
4 РАЗРАБОТКА МОДЕЛИ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ ГРУППЫ КОМПАНИЙ «МЕТАЛЛОТОРГ».....	45
4.1 Выбор среды моделирования	45

					11070006.11.03.02.116.ПЗВКР			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		<i>Лазарак Е.А.</i>			Проектирование информационной инфраструктуры группы компаний «Металлоторг» в Центральном Федеральном округе, с разработкой имитационной модели сети	Лит.	Лист	Листов
Провер.		<i>Девыцына С.Н.</i>					2	79
Рецензент		<i>Старченко П.</i>				<i>НИУ «БелГУ», гр. 07001208</i>		
Н. контр.		<i>Девыцына С.Н.</i>						
Утв.		<i>Жилияков Е.Г.</i>						

4.1	Разработка плана IP-адресации.....	46
4.2	Разработка модели сети в среде Cisco Packet Tracer.....	47
5	ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ.....	53
5.1	Расчет капитальных вложений.....	53
5.2	Калькуляция эксплуатационных расходов.....	55
6	РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО РАЗМЕЩЕНИЮ СЕТЕВОГО ОБРУДОВАНИЯ.....	61
6.1	Выбор серверного помещения.....	61
6.2	Рекомендуемые размеры серверного помещения и конфигурация.....	61
6.3	Электропитание и электрические розетки.....	63
6.4	Заземление.....	64
6.5	Прокладка магистральных кабелепроводов к серверному помещению. Средства распределения кабелей и организация кабельных потоков.....	64
7	ОХРАНА ТРУДА И ТЕХНИКА БЕЗОПАСНОСТИ.....	65
7.1	Микроклимат (температура, влажность, вентиляция) в помещении серверной.....	65
7.2	Защита от вредных веществ.....	66
7.3	Вибрация.....	67
7.4	Освещение серверного помещения.....	67
7.5	Электромагнитные помехи.....	67
	ЗАКЛЮЧЕНИЕ.....	68
	СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	69

ВВЕДЕНИЕ

В современном телекоммуникационном мире очень важную роль имеет планирование сетей связи. Планирование сетей позволяет обеспечить развитие сетей связи. В последнее время в мире телекоммуникаций наблюдается повышенный интерес к виртуальным частным сетям. Это обусловлено необходимостью снижения расходов на содержание корпоративных сетей за счет более дешевого подключения удаленных офисов и удаленных пользователей через сеть Internet. При сравнении стоимости услуг по соединению нескольких сетей через Internet можно заметить существенную разницу в стоимости. Однако необходимо отметить, что при объединении сетей через Internet, сразу же возникает вопрос о безопасности передачи данных, поэтому возникла необходимость создания механизмов, позволяющих обеспечить конфиденциальность и целостность передаваемой информации. Сети, построенные на базе таких механизмов, получили название «виртуальные частные сети» - VPN. Преимущества технологии VPN в том, что организация удалённого доступа делается не через телефонную линию, а через Internet, что намного дешевле и лучше. В данном проекте разработаны рекомендации по созданию инфокоммуникационной инфраструктуры группы компаний «Металлоторг» в Центральном Федеральном округе. Компания является одним из самых больших предприятий по доставке металлопроката строительным и металлоперерабатывающим предприятиям, а так же предприятиям нефтегазовой и энергетической отраслей России, Казахстана и Белоруссии. Так как у компании «Металлоторг» достаточно большое количество филиалов, необходимо организовать безопасную связь внутри компании, а для этого отлично подходит такая технология, как VPN.

Цель проекта – разработка инфокоммуникационной платформы, способствующей улучшению процесса обмена информацией и взаимодействия между территориально-распределенными подразделениями группы компаний

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		4

«Металлоторг» в Центральном Федеральном округе, а также его клиентами и поставщиками.

Задачи проекта:

1. Анализ состояния существующей инфокоммуникационной инфраструктуры группы компаний «Металлоторг»
2. Разработка концепции реализации мультисервисной сети связи группы компаний «Металлоторг»
3. Проектирование мультисервисной системы связи группы компаний «Металлоторг»
4. Разработка модели мультисервисной системы связи группы компаний «Металлоторг»
5. Техничко-экономическое обоснование проекта
6. Охрана труда и техника безопасности.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		5

1 АНАЛИЗ СОСТОЯНИЯ СУЩЕСТВУЮЩЕЙ ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ ГРУППЫ КОМПАНИЙ «МЕТАЛЛОТОРГ»

На территории компании «Металлоторг» функционирует корпоративная сеть, позволяющая обеспечить связь между сотрудниками данной компании. Корпоративная сеть, как правило, является территориально распределенной, т.е. объединяющей офисы, подразделения и другие структуры, находящиеся на значительном удалении друг от друга. Узлы корпоративной сети очень часто оказываются расположенными в разных городах. Принципы, по которым строится такая сеть, достаточно сильно отличаются от тех, что используются при создании локальной сети. Основное отличие заключается в том, что территориально распределенные сети используют арендованные линии связи. При создании локальной сети затраты приходится на прокладку кабеля и закупку оборудования, а в территориально-распределенных сетях очень большое влияние имеет стоимость аренды за использование каналов. Корпоративные сети не оказывают услуг другим организациям или пользователям.

Так как телекоммуникации не стоят на месте и развиваются с достаточно большой скоростью, существующая сеть компании «Металлоторг» требует усовершенствования, т.к. появляются дополнительные подразделения, и объем передаваемой информации растет, также требуется обеспечение безопасной передачи конфиденциальных данных. Существующая сеть, организованная более 20 лет назад, не справляется с новыми задачами. Возникла потребность в обеспечении филиалов современными инфокоммуникационными услугами и технологиями, а так же обеспечении возможности управления информационными и другими ресурсами с главного офиса компании, который находится в г. Москва. Таким образом, проектирование транспортной сети связи для ГК «Металлоторг» является актуальной задачей.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		6

1.1 Описание объектов сети связи группы компаний «Металлоторг»

У компании ЗАО «Металлоторг» насчитывается около 38 филиалов по всей стране. Из них 14 филиалов находятся в Центральном Федеральном округе [1]:

1. Москва – это центральный офис, в котором размещаются: генеральный директор, главный бухгалтер, учетно-платежный отдел, бухгалтера, с которыми согласовываются менеджерами возникающие вопросы клиентов, транспортный отдел, товароведческий и рекламный отделы, системные администраторы; отдел по кадрам; управляющие складами; координаторы производства; юридический отдел; отдел сбыта и многие другие отделы и сотрудники для слаженной работы по всей сети металлобаз компании ЗАО «Металлоторг» - 3076 абонентов
2. Москва – Лобня - самый крупный филиал в России, с которого началась работа всего предприятия, как филиала, находящегося вне Москвы - 1752 абонентов
3. Москва – Чехов – открыт в 2006г., имеет хорошие подъездные пути с Симферопольского шоссе и доступна для потребителей металлопроката южной части Москвы и Подмосковья - 1531 абонент
4. Москва – Электроугли – работает с 2004г. Предлагает юридическим или физическим лицам широкий выбор материалов для строительства - 1230 абонентов
5. Белгород – работает с 1999 года. В Белгороде находятся два филиала по адресам: ул. Чичерина, д. 1 и Почтовый 4-ый пер., д.16. На Крейда есть 2 площадки - основная и мелкооптовая – абонентская емкость сети составляет 1102 абонента и 1011 абонентов соответственно.
6. Брянск – филиал расположен в поселке городского типа Большое Полпино по адресу пер. Октябрьский, 2 - 716 абонентов
7. Владимир – работает с июня 2004 года. Филиал состоит из административного здания и базы - 989 абонентов

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		7

8. Воронеж – работает с 24 февраля 1999 года. База располагается на территории бывшего ОАО «Воронежводкомплект» - 1122 абонента
9. Калуга – с 01 августа 2004г. начала работу новая металлобаза, расположенная в районе Железняки, в сложившейся промышленной зоне, на территории бывшего предприятия «Аромосинтез». Оснощена база достаточным количеством оборудования, что способствует оперативной работе по погрузке-выгрузке металла клиентам - 906 абонентов
- 10.Курск – Начал свою работу в ноябре 2006 года. Металлобаза расположена на территории бывшего завода по адресу г. Курск, Магистральный проезд, 24 В. Сегодня база ЗАО Металлоторг представляет собой открытую бетонную площадку в 3400 кв. м. с двумя мостовыми кранами, что позволяет осуществлять погрузку одновременно двух машин, крытый склад для холоднокатаного проката и оцинковки с мостовым краном и цех по производству гнутого швеллера - 729 абонентов
- 11.Липецк – Металлобаза ЗАО «Металлоторг» в г. Липецк начала свою работу в мае 2002 года, склад и офис находятся на территории бывшего угольного склада в с.Подгорное Липецкого района (на трассе Липецк-Воронеж) - 800 абонентов
- 12.Орел – Филиал ЗАО «Металлоторг» в городе Орёл открылся в июне 1996г., база располагается по адресу: ул. Северный парк, 1, в районе завода Силикатного кирпича - 993 абонента
- 13.Тверь – Тверской филиал ЗАО «Металлоторг» был открыт 1 марта 2005 г., металлобаза находится в промзоне Лазурной - 1032 абонента
- 14.Тула – с апреля 1996 года начал свою деятельность филиал в Тульской области, в городе Тула, по адресу Проспект Ленина, д. 57 офис 104. В 2010 году открылся сервисный металлоцентр в северном районе Тулы, по адресу Ленинский район, Плеханово, ул. Ленина, 1А. Склад имеет железнодорожное сообщение, а также хорошие подъездные автодороги как со стороны Октябрьской улицы, так и со стороны объездной дороги на Белгород - 690 абонента

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		8

15. Старый Оскол – База ЗАО «Металлоторг» в г. Старый Оскол открылась в октябре 2012 г., офис и склад находятся на станции Котел, промузле, промплощадке Столярная, Проезде Ш-3. - 1002 абонента.

На рисунке 1 показана экспликация объекта, включающая филиалы Центрального Федерального округа, в том числе и Белгородский филиал.

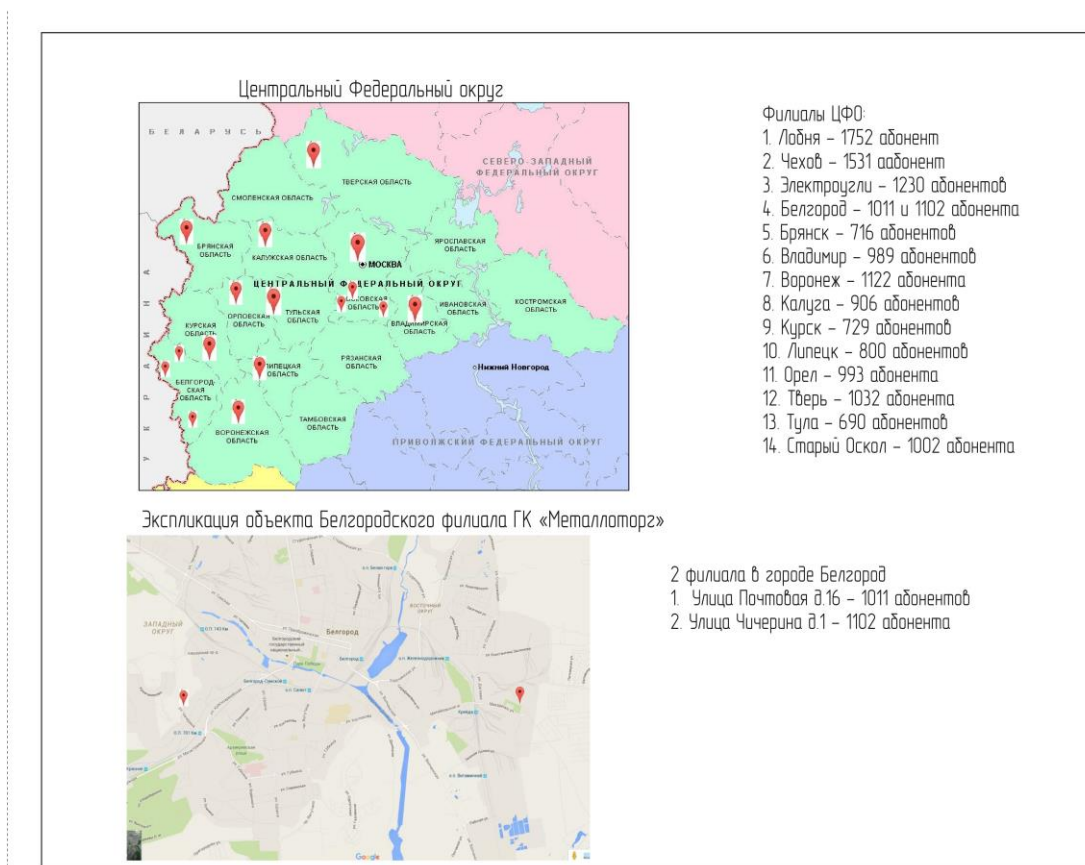


Рисунок 1 – Экспликация объекта

Итого 14 филиалов и 14503 абонента, для которых в проекте предусмотрено предоставление следующих услуг: IP телефония, беспроводной WiFi доступ, IP- камеры видеонаблюдения, доступ в Интернет.

1.2 Анализ существующей сети связи группы компаний «Металлоторг»

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		9

На предприятии Металлоторг уже более 20 лет существует собственная корпоративная сеть. За 20 лет использования этой сети в мире телекоммуникационных технологий появились новые тенденции, новое, более усовершенствованное оборудование, а так же возможность аренды оптоволоконной линии связи у провайдера, с наибольшей скоростью передачи информации и наилучшей эффективностью среди всех представителей данной сферы деятельности. В настоящее время в существующей сети связи группы компаний «Металлоторг» использовано оборудование, которое уже не позволяет с такой точностью и скоростью передать информацию из одного филиала, в другой, находящийся в разных городах.

Данная сеть связывает главный офис со складскими помещениями и офисами во всех других городах России. Однако использование различных технологий (витая пара, симметричный кабель и услуги провайдера) в данной сети нецелесообразно и это увеличивает время на обслуживание и ремонт. Именно устаревшее сетевое оборудование не позволяет просто модернизировать данную сеть. В частности, пропускная способность коммутаторов составляет 10 Мбит/с, что не обеспечивает требуемый результат. Серверы на предприятии используют разные сетевые протоколы и операционные системы, часть из которых уже устарела и не имеет поддержки производителями современного программного обеспечения, что так же указывает на необходимость разработки новой сети связи.

Связь главных офисов в каждом городе со складским помещением этого же города осуществляется с использованием технологий ADSL, либо используя в качестве среды передачи данных кабель UTP по сети Ethernet. А связь между филиалами осуществляется через арендуемые каналы. Такая технология не соответствует современным потребностям предприятия. Именно поэтому необходимо усовершенствование корпоративной сети группы компаний «Металлоторг» с дальнейшим изменением устаревшего оборудования на новое, более усовершенствованное, с использованием VPN соединения на базе поставщика интернет-услуг «Ростелеком».

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		10

1.3 Постановка задач проектирования

Целью данного проекта является разработка инфокоммуникационной инфраструктуры группы компаний «Металлоторг», поддерживающая интеграцию в единое сетевое пространство удаленных филиалов компании.

Задачи проекта:

7. Анализ состояния существующей инфокоммуникационной инфраструктуры группы компаний «Металлоторг»
8. Разработка концепции реализации мультисервисной сети связи группы компаний «Металлоторг»
9. Проектирование мультисервисной системы связи группы компаний «Металлоторг»
10. Разработка модели мультисервисной системы связи группы компаний «Металлоторг»
11. Технико-экономическое обоснование проекта
12. Охрана труда и техника безопасности.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		11

2 РАЗРАБОТКА КОНЦЕПЦИИ РЕАЛИЗАЦИИ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ ГРУППЫ КОМПАНИЙ «МЕТАЛЛОТОРГ»

Мультисервисная сеть — это сеть, способная передавать голос, видеоизображения и данные на базе единой инфраструктуры. Основным стимулом появления и развития мультисервисных сетей является стремление уменьшить стоимость владения, поддержать сложные, насыщенные мультимедиа прикладные программы и расширить функциональные возможности сетевого оборудования. [2]

Для создания корпоративной мультисервисной среды с интеграцией в ней IP-телефонии, необходимо:

- создать условия для дальнейшего развития сети без существенных инвестиций.
- обеспечить прозрачную интеграцию технологий IP-телефонии, полностью сохранив функциональность действующих решений компании в области традиционной телефонии;
- создать защищенные каналы передачи данных и предотвратить возможность несанкционированного доступа в сеть;

Преимущества корпоративной сети являются сокращение расходов на междугороднюю и международную связи, требования к квалификации персонала не высокие, достаточно просто осуществляется подключение новых филиалов к сети, а так же использование полосы пропускания наземных каналов.

В данном проекте были выбраны продукты Huawei, которые создают интеллектуальную сетевую инфраструктуру и обеспечивает поддержку основных сервисов корпоративной сети, такие как: передача данных и голоса, безопасность, сетевое управление и механизмы гарантирования качества

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		12

сервиса. Каналами передачи данных могут быть традиционные наземные линии связи ССОП и цифровые каналы Frame Relay, арендуемые у оператора связи.

Основные компоненты мультисервисной корпоративной сети:

- IP-телефоны, подключенные в локальную сеть каждого офиса и обеспечивающие как традиционную функциональность телефонов, так и ряд новых функций;
- сервер, позволяющий управлять телефонными соединениями и предоставлять дополнительные сервисы IP-телефонии;
- голосовые шлюзы, предназначенные для подключения к ССОП и стыковки с существующими УАТС;
- коммутаторы, необходимые для подключения активных сетевых устройств: рабочих станций, IP-телефонов и серверов.

Построение мультисервисной сети связи позволит обеспечить последующие важные параметры, такие как:

- Надежность передачи информации;
- Безопасность передачи;
- Масштабируемость сети и предоставляемых услуг;
- Управляемость корпоративной сети;
- Возможность и готовность сети к внедрению последующих новых услуг и приложений и др.

Все эти условия накладывают определенные ограничения на выбор оборудования, применение того или иного решения для реализации решения, сопровождение сети и, в конечном итоге, на выбор поставщика услуг не только оборудования, но и различных дополнительных сервисов.

2.1 Проектирование транспортной сети связи

Транспортная сеть связи — это совокупность всех ресурсов, выполняющих функции транспортирования в телекоммуникационных сетях.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		13

Она включает не только системы передачи, но и относящиеся к ним средства контроля, оперативного переключения, резервирования, управления. В проектируемой сети транспортная сеть является сегментом между ядром сети, расположенным в г. Москва, и подсетями филиалов.

Для построения распределенных сетей часто используется такой вид подключения, как VPN. Виртуальные частные сети (VPN) представляют собой подключения типа «точка-точка» в частной или публичной сети, например в Интернете. VPN-клиент использует для виртуального обращения на виртуальный порт VPN-сервера специальные протоколы на основе TCP/IP, которые называются туннельными протоколами. При обычной реализации VPN клиент инициирует по Интернету виртуальное подключение типа «точка-точка» к серверу удаленного доступа. Сервер удаленного доступа отвечает на вызов, выполняет проверку подлинности вызывающей стороны и передает данные между VPN-клиентом и частной сетью организации.

Для эмуляции канала типа «точка-точка» к данным добавляется заголовок (выполняется инкапсуляция). Этот заголовок содержит сведения маршрутизации, которые обеспечивают прохождение данных по общей или публичной сети до конечного пункта. Для эмуляции частного канала и сохранения конфиденциальности передаваемые данные шифруются. Пакеты, перехваченные в общей или публичной сети, невозможно расшифровать без ключей шифрования. Такой канал, по которому частные данные передаются в инкапсулированном и зашифрованном виде, и называется VPN-подключением.

Существует два типа VPN-подключений:

1. VPN-подключение удаленного доступа;
2. VPN-подключение типа «сеть-сеть»

VPN-подключение удаленного доступа дает пользователям возможность работать дома или в дороге, получая доступ к серверу частной сети с помощью инфраструктуры публичной сети. С точки зрения пользователя, VPN-подключение представляет собой подключение типа «точка-точка» между компьютером (VPN-клиентом) и сервером организации. Реальная

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		14

инфраструктура общей или публичной сети не имеет значения, поскольку данные передаются подобно тому, как если бы они передавались по выделенному частному каналу.

VPN-подключения типа «сеть-сеть» (также называются VPN-подключения типа «маршрутизатор-маршрутизатор») позволяют организациям устанавливать маршрутизируемые подключения между отдельными офисами (или между другими организациями) по публичной сети, при этом обеспечивая безопасность связи. Маршрутизируемое VPN-подключение по Интернету логически подобно выделенному каналу глобальной сети (WAN). В случае, когда сети соединены по Интернету, маршрутизатор переадресует пакеты другому маршрутизатору через VPN-подключение. С точки зрения маршрутизаторов VPN-подключение работает как канал уровня передачи данных.

VPN-подключение типа «сеть-сеть» связывает два сегмента частной сети. VPN-сервер обеспечивает маршрутизируемое подключение к сети, к которой прикреплен VPN-сервер. Вызывающий маршрутизатор (VPN-клиент) проходит проверку подлинности на отвечающем маршрутизаторе (VPN-сервере) и, в целях взаимной проверки подлинности, отвечающий маршрутизатор проходит проверку подлинности на вызывающем маршрутизаторе. При VPN-подключении типа «сеть-сеть» пакеты, отсылаемые с любого из маршрутизаторов через VPN-подключение, обычно формируются не на маршрутизаторах.

Свойства VPN-подключений

VPN-подключения, использующие протоколы PPTP, L2TP/IPsec и SSTP, имеют следующие свойства:

1. Инкапсуляция
2. Проверка подлинности
3. Шифрование данных

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		15

Инкапсуляция

VPN-технология обеспечивает инкапсуляцию частных данных с заголовком, содержащим сведения маршрутизации для передачи этих данных по транзитной сети.

Проверка подлинности

Существует три различные формы проверки подлинности для VPN-подключений.

1. Проверка подлинности на уровне пользователя по протоколу PPP. Для установления VPN-подключения VPN-сервер выполняет проверку подлинности VPN-клиента, пытающегося установить подключение, на уровне пользователя по протоколу PPP и проверяет, имеет ли VPN-клиент требуемую авторизацию. При взаимной проверке подлинности VPN-клиент также выполняет проверку подлинности VPN-сервера, что гарантирует защиту от компьютеров, выдающих себя за VPN-серверы.
2. Проверка подлинности на уровне компьютера по протоколу IKE. Для установления сопоставления безопасности IPsec VPN-клиент и VPN-сервер используют протокол IKE для обмена сертификатами компьютеров или предварительным ключом. В обоих случаях VPN-клиент и VPN-сервер выполняют взаимную проверку подлинности на уровне компьютера. Настоятельно рекомендуется выбирать проверку подлинности по сертификату компьютера из-за большей безопасности этого метода. Проверка подлинности на уровне компьютера выполняется только для подключений L2TP/IPsec.
3. Проверка подлинности источника данных и обеспечение целостности данных. Чтобы убедиться в том, что источником отправленных по VPN-подключению данных является другая сторона VPN-подключения и что они переданы в неизменном виде, данные содержат контрольную сумму шифрования, основанную на ключе шифрования, который известен только отправителю и получателю. Проверка подлинности источника данных и

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		16

обеспечение целостности данных доступны только для подключений L2TP/IPsec.

Шифрование данных

Для обеспечения конфиденциальности данных при передаче по общей или публичной транзитной сети они шифруются отправителем и расшифровываются получателем. Успешность процессов шифрования и расшифровки гарантируется в том случае, когда отправитель и получатель используют общий ключ шифрования. Содержание перехваченных пакетов, отправленных по VPN-подключению в транзитной сети, понятно только владельцам общего ключа. Длина ключа шифрования - это важный параметр безопасности. Для определения ключа шифрования можно использовать вычислительную технику. Однако при возрастании размера ключей шифрования использование подобной техники требует большей вычислительной мощности и большего времени для выполнения этих вычислений. Поэтому для гарантии конфиденциальности данных рекомендуется использовать наибольший возможный ключ. [3]

2.2 Проектирование сетей доступа в филиалах компании

Для того чтобы спроектировать сеть доступа в филиалах группы компаний «Металлоторг», необходимо выбрать оборудование и описать условия создания сети связи. В качестве производителя оборудования выбрана фирма Huawei (Китай), которая на данное время является одним из хорошо зарекомендовавших себя на рынке лидеров в разработке оборудования для телекоммуникационных услуг.

Принято решение использовать следующее оборудование:

1. Маршрутизатор главного офиса Huawei AR3260
2. Маршрутизатор среднего офиса Huawei AR2220
3. Коммутатор Huawei S5700-28P-LI-AC
4. VoIP шлюз Huawei U-SYS IAD 132

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		17

5. Платформа Quidway® CX380 Metro.
6. IP-телефон серии eSpace 7900
7. Видеокамеры AHD
8. Принтер
9. Сканер
10. Точка доступа WiFi
11. Персональный компьютер
12. Ноутбук

На рисунке 2 представлена проектируемая схема организации связи в Белгородском филиале.

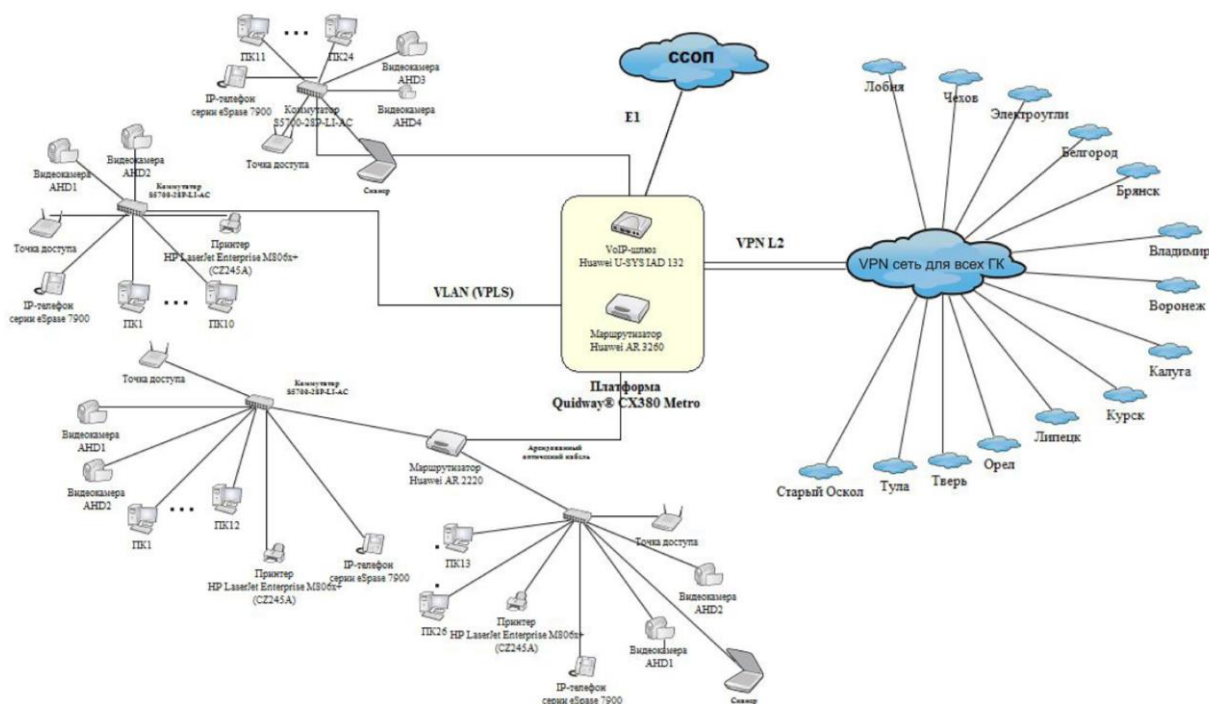


Рисунок 2 – Проектируемая схема организации связи Белгородского филиала

На данном рисунке главным компонентом является платформа Quidway® CX380 Metro, которая включает маршрутизатор главного офиса и VoIP шлюз. Эта платформа находится на площадке филиала, находящегося по адресу: улица Почтовая д.16. От платформы организован выход на сеть связи общего пользования, на маршрутизатор среднего офиса, который находится на

площадке по улице Чичерина, а так же по VPN сети на сеть остальных филиалов. Описание оборудования и его характеристики представлены ниже.

2.3 Расчет нагрузок

Для расчета нагрузок взяты филиалы, находящиеся в г. Белгород на улице Чичерина и Почтовой, ёмкость которых 1011 и 1102 абонента соответственно. В проектируемой сети связи основную полосу пропускания занимают услуги IP – телефонии, передачи данных внутри сети, IPTV и доступа к глобальной сети Internet (услуги Triply Play). Для предоставления остальных услуг требуется полоса пропускания существенно меньшая. Исходя из этого, рассчитаем требуемую полосу пропускания для услуг Triply Play и учтем необходимый запас для предоставления оставшихся услуг.

Для правильной оценки характеристик и расчета требуемой пропускной способности для предоставления комплексной услуги Triply Play используем параметры, основанные на статистических данных, адаптированные к российскому рынку услуг связи. Проектируемая сеть должна быть надежной и на ней не должно быть перегрузок. Поэтому все необходимые расчеты трафика будем производить для часа наибольшей нагрузки для одного оптического сетевого узла.

2.3.1 Расчет трафика телефонии

Для организации услуг IP телефонии необходимо рассчитать требуемую полосу пропускания. Исходными данными для расчета являются:

1. количество источников нагрузки – абоненты, использующие терминалы SIP и подключаемые в пакетную сеть на уровне мультисервисного абонентского концентратора , $N_{SIP}=1011$ абонентов и , $N_{SIP}=1102$ абонентов;
2. тип кодека в планируемом к внедрению оборудовании, G.729A;

					11070006.11.03.02.116.ПЗВКР	Лист
						19
Изм.	Лист	№ докум	Подпись	Дата		

3. длина заголовка IP пакета, 58 байт.

Транспортный ресурс, который должен быть выделен для передачи в пакетной сети телефонного трафика, поступающего на концентратор, при условии использования кодека определяется следующим образом:

Полезная нагрузка голосового пакета G.729A CODEC составит

$$Y_{\text{полезн}} = \frac{t_{\text{звуч.голоса}} \cdot v_{\text{кодирования}}}{8 \text{ бит} / \text{байт}} = \dots \text{байт}, \quad (1)$$

где $t_{\text{звуч.голоса}}$ - время звучания голоса (мс), $v_{\text{кодирования}}$ - скорость кодирования речевого сигнала (Кбит/с).

Эти параметры являются характеристиками используемого кодека. В данном случае для кодека G.729A скорость кодирования – 8кбит/с, а время звучания голоса – 20 мс.

$$Y_{\text{полезн}} = \frac{20 \cdot 8}{8} = 20 \text{ байт}.$$

Каждый пакет имеет заголовок длиной в 58 байт.

Общий размер голосового пакета составит:

$$V_{\text{пакета}} = L_{\text{Eth}} + L_{\text{IP}} + L_{\text{UDP}} + L_{\text{RTP}} + Y_{\text{полезн}}, \text{ байт}, \quad (2)$$

где L_{Eth} , L_{IP} , L_{UDP} , L_{RTP} – длина заголовка Ethernet, IP, UDP, RTP протоколов соответственно (байт), $Y_{\text{полезн}}$ – полезная нагрузка голосового пакета (байт).

$$V_{\text{пакета}} = 14 + 20 + 8 + 16 + 20 = 78 \text{ байт}.$$

Использование кодека G.729A позволяет передавать через шлюз по 50 пакетов в секунду, исходя из этого, полоса пропускания для одного вызова определится по формуле:

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		20

$$ППр_1 = V_{\text{пакета}} \cdot 8 \frac{\text{бит}}{\text{байт}} \cdot 50_{\text{pps}}, \text{Кбит/с}, \quad (3)$$

где $V_{\text{пакета}}$ – размер голосового пакета, [байт].

$$ППр_1 = 78 \cdot 8 \cdot 50 = 30 \text{Кбит/с}.$$

В проектируемой МСС устанавливается точка присутствия, в которой имеется 1011 и 1102 голосовых портов. С помощью средств подавления пауз обычный голосовой вызов можно сжать примерно на 50 процентов (по самым консервативным оценкам – 30%). Исходя из этого, необходимая полоса пропускания WAN для нашей точки присутствия составит:

$$ППр_{\text{WAN}} = ППр_1 \cdot N_{\text{SIP}} \cdot VAD, \text{Мбит/с}, \quad (4)$$

где $ППр_1$ – полоса пропускания для одного вызова, (Кбит/с), N_{SIP} – количество голосовых портов в точке присутствия, (шт), VAD (Voice Activity Detection) – коэффициент механизма идентификации пауз (0,7).

$$ППр_{\text{WAN}} = 30 \cdot 1011 \cdot 0,7 = 21231 \text{бит/с}.$$

$$ППр_{\text{WAN}} = 30 \cdot 1102 \cdot 0,7 = 23142 \text{бит/с}.$$

Результаты могли быть другими, если бы использовались другие средства кодирования/декодирования (CODEC), изменилась средняя продолжительность вызова. Кроме того, на конечный результат может повлиять тип используемого приложения. Так, например, передача музыки вызывающему абоненту, который ждет ответа оператора, не позволяет использовать средства подавления пауз.

2.3.2 Расчет трафика передачи данных

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		21

Сети передачи данных предназначены для совместного доступа пользователя к ресурсам компьютеров: приложениям, файлам, принтерам и т.п. а так же для передачи мультимедийного трафика. Трафик, создаваемый этими традиционными службами, имеет свои особенности и существенно отличается от трафика сообщений в телефонных сетях или сетях кабельного телевидения. Трафик компьютерных данных характеризуется крайне неравномерной интенсивностью поступления сообщений в сеть. Коэффициент пульсации трафика отдельного пользователя сети, равный отношению средней интенсивности обмена данными к максимально возможной, может достигать 1:50 и даже 1:100. Но если число абонентов, обслуживаемых коммутаторами, достаточно велико, то пульсации отдельных абонентов в соответствии с законом больших чисел распределяются во времени так, что их пики не совпадают и коэффициент пульсации на магистральных каналах значительно снижается.

Среди всех пользователей сети в час наибольшей нагрузки (ЧНН) в сети будет находиться и передавать данные только часть абонентов (активные абоненты). Даже в час наибольшей нагрузки количество активных абонентов может изменяться, поэтому для их подсчета используется пятиминутный временной интервал внутри ЧНН, и максимальное число активных абонентов за этот период времени определяется параметром Data Average Activity Factor (DAAF), в соответствии с этим количество активных абонентов составит

$$AS = TS * DAAF, \text{ аб}, \quad (5)$$

где TS – число абонентов на одном сетевом узле, (аб), DAAF – процент абонентов, находящихся в сети в ЧНН.

$$AS = (1011/21) * 0,8 = 39 \text{ абонентов.}$$

$$AS = (1102/21) * 0,8 = 42 \text{ абонента}$$

В час наибольшей нагрузки в сети находится 39 человек на ул. Почтовая и 42 абонента на ул. Чичерина с одного сетевого узла, охватывающего 51 абонент.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		22

Абоненты время от времени передают и принимают данные и, как правило, объем передаваемых данных значительно меньше объема принимаемых данных. Каждому абоненту необходимо обеспечить заявленную пропускную способность. Далее определим среднюю пропускную способность сети, требуемой для обеспечения нормальной работы пользователей.

Средняя пропускная способность для приема данных составит:

$$BDDA = (AS * ADBS) * (1 + OHD), \text{ Мбит/с}, \quad (6)$$

где AS - количество активных абонентов, (аб), ADBS – средняя скорость приема данных, (Мбит/с), OHD – отношение длины заголовка IP пакета к его общей длине во входящем потоке.

$$BDDA = (39 * 2) * (1 + 0,1) = 85,8 \text{ Мбит/с}$$

$$BDDA = (42 * 2) * (1 + 0,1) = 92,4 \text{ Мбит/с}$$

Средняя пропускная способность для передачи данных

$$BUDA = (AS * AUBS) * (1 + OHU), \text{ Мбит/с}, \quad (7)$$

где AS - количество активных абонентов, (аб), AUBS – средняя скорость передачи данных, (Мбит/с), OHU – отношение длины заголовка IP пакета к его общей длине в исходящем потоке.

$$BUDA = (39 * 0,5) * (1 + 0,15) = 22,425 \text{ Мбит/с}$$

$$BUDA = (42 * 0,5) * (1 + 0,15) = 24,15 \text{ Мбит/с}$$

Количество абонентов, передающих или принимающих данные в течение некоторого короткого промежутка времени, определяют пиковую пропускную способность сети. Количество таких абонентов в час наибольшей нагрузки определяется коэффициентом Data Peak Activity Factor (DPAF)

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		23

$$PS = AS * DPAF, \text{ аб,} \quad (8)$$

где DPAF – процент абонентов, одновременно принимающих или передающих данные в течении короткого интервала времени.

$$PS = 39 * 0,7 = 28 \text{ абонентов}$$

$$PS = 42 * 0,7 = 30 \text{ абонентов}$$

Пиковая пропускная способность измеряется за короткий промежуток времени (1 секунда), она необходима для приема и передачи данных в момент, когда одновременно несколько пользователей передают или принимают данные по сети. Пиковая пропускная способность, требуемая для приема данных в час наибольшей нагрузки:

$$BDDP = (PS * PDBS) * (1 + OHD), \text{ Мбит/с,} \quad (9)$$

где PDBS – пиковая скорость приема данных, Мбит/с.

$$BDDP = (28 * 3) * (1 + 0,1) = 92,4 \text{ Мбит/с}$$

$$BDDP = (30 * 3) * (1 + 0,1) = 99 \text{ Мбит/с}$$

Пиковая пропускная способность для передачи данных в ЧНН

$$BUDP = (PS * PUBS) * (1 + OHU), \text{ Мбит/с,} \quad (10)$$

где PUBS – пиковая скорость передачи данных, Мбит/с.

$$BUDP = (28 * 1,5) * (1 + 0,15) = 48,3 \text{ Мбит/с}$$

$$BUDP = (30 * 1,5) * (1 + 0,15) = 51,75 \text{ Мбит/с}$$

Из расчета видно, что пиковая пропускная способность для передачи данных выше средней пропускной способности.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		24

Для проектирования сети необходимо использовать максимальное значение полосы пропускания среди пиковых и средних значений для исключения перегрузки сети:

$$BDD = \text{Max} [BDDA; BDDP], \text{ Мбит/с}, \quad (11)$$

$$BDU = \text{Max} [BUDA; BUDP], \text{ Мбит/с}, \quad (12)$$

где BDD – пропускная способность для приема данных, (Мбит/с), BDU – пропускная способность для передачи данных, [Мбит/с].

$$BDD = \text{Max} [85,8; 22,425] = 85,8 \text{ Мбит/с},$$

$$BDU = \text{Max} [92,4; 48,3] = 92,4 \text{ Мбит/с}$$

$$BDD = \text{Max} [92,4; 24,15] = 85,8 \text{ Мбит/с},$$

$$BDU = \text{Max} [99; 51,75] = 92,4 \text{ Мбит/с}$$

Общая пропускная способность для приема и передачи данных, необходимая для нормального функционирования оптического сетевого узла, составит

$$BD = BDD + BDU, \text{ Мбит/с}, \quad (13)$$

где BDD – максимальная пропускная способность для приема данных, (Мбит/с), BDU – максимальная пропускная способность для передачи данных, (Мбит/с).

$$BD = 85,8+92,4 = 178,2 \text{ Мбит/с}$$

Итак, для передачи данных между абонентами сети на одном сетевом узле на улице Почтовая необходима полоса пропускания 178,2 Мбит/с.

$$BD = 92,4+99 = 192,4 \text{ Мбит/с}$$

Итак, для передачи данных между абонентами сети на одном сетевом узле на улице Чичерина необходима полоса пропускания 192,4 Мбит/с.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		25

2.3.3 Расчет трафика предоставления услуг доступа к сети Internet

Все расчеты параметров проектируемой сети приводятся, принимая во внимание следующие исходные данные:

Только 10% из числа пользователей могут находиться в сети одновременно. Из них 20% в час наибольшей нагрузке (ЧНН). Из этих 20% только 25% загружают данные.

Определим число активных пользователей, работающих на средней скорости по формуле:

$$N_{act\ subser} = HHP * DP * DAAF, \text{ аб}, \quad (14)$$

где HHP – общее число абонентов проектируемой сети; DP – характеристика проникновения трафика данных; DAAF – фактор активности.

$$N_{act\ subser} = 1011 * 0,1 * 0,2 = 21 \text{ абонента}$$

$$N_{act\ subser} = 1102 * 0,1 * 0,2 = 23 \text{ абонента}$$

Далее рассчитаем количество абонентов одновременно принимающих и передающих данные по формуле:

$$Peak_{subser} = HHP * DP * DPeakAF, \text{ аб} \quad (15)$$

$$Peak_{subser} = 1011 * 0,1 * 0,1 = 11 \text{ абонентов}$$

$$Peak_{subser} = 1102 * 0,1 * 0,1 = 11 \text{ абонентов}$$

Для определения требуемой полосы пропускания для среднего и пикового трафика необходимо рассчитать среднюю и пиковую полосу пропускания в ЧНН для восходящего и нисходящего трафика и выбрать из них максимальный.

$$BWDA = (N_{act\ subser} * BWA_{per\ subser}) * (1 + OH), \text{ Мбит/с}, \quad (16)$$

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		26

$$BWDPeak = (Peak_{subser} * BWP_{per\ subser}) * (1 + OH), \text{ Мбит/с}, \quad (17)$$

где $BWA_{per\ subser}$ - средняя полоса пропускания, приходящаяся на 1 абонента (1800 кбит/с); $BWP_{per\ subser}$ – пиковая полоса пропускания на 1 абонента (4000 кбит/с); OH – отношение длины заголовка к длине пакета (0,1).

$$BWDA = (21 * 1800) * (1 + 0,1) = 41,58, \text{ Мбит/с},$$

$$BWDA = (23 * 1800) * (1 + 0,1) = 45,54 \text{ Мбит/с}$$

$$BWDPeak = (11 * 4000) * (1 + 0,1) = 48,4, \text{ Мбит/с}$$

$$BWDPeak = (11 * 4000) * (1 + 0,1) = 48,4, \text{ Мбит/с}$$

Для определения требуемой полосы пропускания определим максимальное значение между пиковой и средней пропускной способностью:

$$BWData = MAX[BWDA; BWDPeak], \text{ Мбит/с} \quad (18)$$

$$BWData = MAX[41,58; 48,4] = 48,4 \text{ Мбит/с}$$

$$BWData = MAX[45,54; 48,4] = 48,4 \text{ Мбит/с}$$

Таким образом, для реализации услуги доступа к глобальной сети Internet полоса пропускания каждого проектируемого узла должна составлять 48,4 Мбит/с.

Общая требуемая пропускная способность узла в Белгороде составит:

$$ППр_{Triply\ play} = ППр_{WAN} + BD + BWData, \text{ Мбит/с}, \quad (19)$$

где $ППр_{WAN}$ – пропускная способность для трафика IP телефонии, (Мбит/с); AB – пропускная способность для видеопотоков, (Мбит/с); BD – пропускная способность для трафика данных, (Мбит/с); $BWData$ - пропускная способность для предоставления услуги доступа к сети Internet, (Мбит/с).

$$ППр_{Triply\ play} = 21,231 + 178,2 + 48,4 = 247,831 \text{ Мбит/с}$$

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		27

$$\text{ППр}_{\text{Triply play}} = 23,142 + 192,4 + 48,4 = 263,342 \text{ Мбит/с}$$

Требования к пропускной способности узлов в сети в филиалах по ул. Почтовая и ул. Чичерина будут удовлетворены при внедрении сетевых решений. [4].

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		28

3 ПРОЕКТИРОВАНИЕ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ ГРУППЫ КОМПАНИЙ «МЕТАЛЛОТОРГ»

3.1 Разработка сценария VPN

VPN сеть позволяет предоставить безопасный удаленный доступ к филиалам сети. С помощью профилей VPN можно настроить любые типы устройств. В таблице 1 показан поддерживаемый тип соединения для каждой из платформ.

Таблица 1 – Поддерживаемые соединения

Тип подключения	iOS и Mac OS	Android	Windows 8.1	Windows RT	Windows RT 8.1	Windows Phone 8.1	Windows 10 Desktop и Mobile
Cisco AnyConnect	Да	Да	Нет	Нет	Нет	Да (OMA-URI)	Да (OMA-URI)
Pulse Secure	Да	Да	Да	Нет	Да	Да	Да
F5 Edge Client	Да	Да	Да	Нет	Да	Да	Да
Dell SonicWALL Mobile Connect	Да	Да	Да	Нет	Да	Да	Да
CheckPoint Mobile VPN	Да	Да	Да	Нет	Да	Да	Да
Microsoft SSL (SSTP)	Нет	Нет	Да	Да	Да	Нет	Нет
Microsoft Automatic	Нет	Нет	Да	Да	Да	Нет	Да (OMA-URI)

Окончание таблицы 1

Тип подключения	iOS и Mac OS X	Android	Windows 8.1	Windows RT	Windows RT 8.1	Windows Phone 8.1	Windows 10 Desktop и Mobile
ИКЕv2	Да (настраиваемая политика)	Нет	Да (OMA- URI)	Да (OMA- URI)	Да (OMA- URI)	Да (OMA- URI)	Да (OMA- URI)
PPTP	Да (настраиваемая политика)	Нет	Да (OMA- URI)	Да (OMA- URI)	Да (OMA- URI)	Нет	Да (OMA- URI)

Для удаленной работы сети требуется компьютер с двумя сетевыми подключениями: к публичной сети и к безопасной. На данном предприятии будет использоваться операционная система Windows Server 2008. Именно Microsoft обеспечивает функции в роли маршрутизации и удаленного доступа. Если клиентский компьютер устанавливает соединение к VPN сети, то оба компьютера будут шифровать все данные, передаваемые между ними.

3.2 Разработка сети абонентского доступа в филиалах

3.2.1. Выбор оборудования

Для построения сети связи в филиале компании «Металлоторг» в городе Белгород было выбрано оборудование, которое отвечает всем тенденциям в современном мире телекоммуникаций:

Корпоративные маршрутизаторы Huawei серии AR G3 - маршрутизаторы нового поколения, предназначенные для корпоративных пользователей. Для нормального функционирования сети были выбраны маршрутизаторы фирмы Huawei. На базе многолетнего опыта Huawei в области телекоммуникаций

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		30

маршрутизаторы AR G3 разработаны с учетом уникальных требований предприятий. С помощью универсальной платформы маршрутизации Versatile Routing Platform (VRP) разработки Huawei, серия AR G3 интегрирует в одном устройстве функции маршрутизации, коммутации, 3G, WLAN, передачи речи и безопасности, посредством многоядерной архитектуры процессора в сочетании с инфраструктурой неблокируемой коммутации.

1. Маршрутизатор главного офиса Huawei AR3260.

Высокая производительность, масштабируемый маршрутизатор доступа с интеграцией коммутации и маршрутизации при низком ТСО, универсальное управление и безопасность для крупномасштабных корпоративных сетей. Неблокируемая архитектура со сдвоенными блоками управления и передачи обеспечивает гибкий доступ для конвергированной передачи голоса, данных и мультимедиа.

Особенности маршрутизатора AR3260:

- Встроенные сервисы обеспечивают голосовую конференцсвязь и поддержку до 500 голосовых почтовых ящиков.
- Мониторинг сети на уровне пакетов и динамическая «горячая» замена обеспечивают быстрое обнаружение отказов и резервное копирование.
- Встроенный брандмауэр, IPS, фильтрация URL; поддержка 802.1x, MAC и аутентификация портала; IPSec VPN, EVPN, DSVPN, Smart VPN и безопасный доступ A2A
- Встроенный ВРХ, SIP-сервер и SIP-шлюз с соединениями NGN/IMS/PBX для голосовых сервисов; функция качества восприятия (Quality of Experience, QoE) Huawei позволяет отслеживать качество услуг передачи голоса в режиме реального времени с функциями управления динамическим буфером джиттера, эхоподавления и компенсации потери пакетов для поддержания высокого качества телефонной связи
- Поддержка высокоскоростного беспроводного режима передачи данных и нескольких режимов 3G/LTE, беспроводных АС и нескольких АР для непрерывной проводной и беспроводной связи

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		31

Основные характеристики оборудования представлены в таблице 2.

Таблица 2 – Характеристики маршрутизатора AR3260 [5]

Характеристики	AR3260
Скорость сети WAN с предоставлением услуг	600 Мбит/с (SRU40), 1 800 Мбит/с (SRU80), 4,5 Гбит/с (SRU200), 5,5 Мбит/с (SRU400)
Производительность брандмауэра	5,5 Гбит/с (с SRU40) 6 Гбит/с (с SRU60) 9,5 Гбит/с (с SRU80)
Фиксированные порты WAN	3 x GE (2 x Combo)/4 x GE Combo + 2 x 10 GE
Емкость коммутации	160Гбит/с
Слоты	Слоты SIC: 4 Слоты WSIC (по умолчанию/максимум): 2/4 Слоты XSIC (по умолчанию/максимум): 4/6
Надёжность	Режим резервирования 1:1 главной платы управления
QoS	Режим Diffserv, MPLS QoS, преобразование приоритета, ограничение трафика (CAR), выравнивание трафика, предотвращение перегрузки (на основе приоритетности IP/DSCP WRED), управление перегрузкой (интерфейс LAN: SP/WRR/SP+WRR; интерфейс WAN: PQ/ CBWFQ), MQC (классификатор трафика, характер трафика и политика трафика), H-QoS, WLAN QoS, FR QoS, интеллектуальное управление приложением (SAC)паратно-ускоренное, иерархическое QoS
Беспроводной контроллер	Интегрирован в программное обеспечение
Память	2Гб
Поддержка	Ethernet, CE1/CT1, E1/T1, ADSL2+, G.SHDSL, последовательный синхронный/асинхронный, ISDN, CPOS Использование U-диска
LAN стандарты	IEEE 802.1P, IEEE 802.1Q, IEEE 802.3, управление VLAN, управление MAC-адресом, MSTP
Базовые услуги	Клиент/сервер DHCP, клиент/сервер PPPoE, клиент/сервер PPPoA, клиент/сервер PPPoEoA, NAT, управление субинтерфейсом
Поддержка голоса	RTP, SIP, SIP AG, IP PBX/TDM PBX, FXO/FXS, VoIP/конференц-связь, BESA, DISA, SBC, контроллер зоны H.323
WLAN контроллер сессий	Управление AP (обнаружение AC/доступ AP/управление AP),CAPWAP, управление пользователем WLAN, управление радиоканалом WLAN (802.11a/b/g/n),WLAN QoS(WMM), безопасность WLAN (WEP/WPA/WPA2/управление ключами)

Окончание таблицы 2

Характеристики	AR3260
Электропитание	AC: 100В ~ 240В, 50/60 Гц DC: -48В ~ -60В Резервный источник питания: внутренний AC и DC
Высота стойки	3 RU

2. Маршрутизатор среднего офиса Huawei AR2220

AR2200 объединяет в себе функции маршрутизации, коммутации, услуги 3G, услуги передачи голоса и обеспечения безопасности. Такой маршрутизатор использует многоядерный процессор CPU и неблокируемую структуру коммутации, обеспечивает ведущее в отрасли быстродействие и расширение системы, отвечая будущим требованиям сервисного обслуживания. AR2200 предлагает комплексное решение для корпоративных сетей, повышает скорость многоканального обслуживания и защищает инвестиции клиентов.

Особенности маршрутизатора AR2220:

- AR2200 использует многоядерный процессор CPU и неблокируемую структуру коммутации и обеспечивает лучшие в отрасли функциональные характеристики, отвечая требованиям расширения сети, а также требованиям в области развития обслуживания предприятий.
- AR1200 не только поддерживает беспроводной режим WLAN, UMTS, LTE, но также и проводной режим оптоволокна и медного провода, что обеспечивает потребителю гибкость методов доступа к сети.
- AR2200 объединяет в себе маршрутизацию, коммутацию, услуги 3G, услуги передачи голоса и выполняет функции обеспечения безопасности.
- AR2200 соединен с основной информационной системой от стороннего производителя при помощи открытой платформы услуг (OSP) и предоставляет унифицированное решение для общения корпоративных пользователей. Клиенты, агенты, представляющие стороннего производителя поставщики и изготовители, по мере необходимости, могут усовершенствовать и использовать маршрутизаторы AR2200.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		33

- Маршрутизатор AR2200 выполняет различные голосовые функции для информационных сетей предприятий, обеспечивая гибкость и эффективность связи.
- В период обслуживания маршрутизатор AR2200 гарантирует безопасную работу корпоративных сетей. Кроме того, он обеспечивает комплексный механизм защиты безопасности, включающим контроль доступа пользователей, распознавание пакетов информации и активную защиту от попыток нарушения защиты.
- Услуги по интеллектуальному развертыванию. По мере роста предприятия растут и требования корпоративных пользователей к службам развертывания. AR2200 предоставляет USB-диск для развертывания устройств и осуществления функций авто-настройки для службы развертывания.
- Упрощенное управление услугами. Корпоративные пользователи заинтересованы в простом управлении услугами. Маршрутизатор AR2200 предоставляет функции iТес, NQA, NetStream для упрощения управления услугами.

Таблица 3 – Характеристики маршрутизатора AR2220 [6]

Характеристики	AR2220
Скорость сети WAN с предоставлением услуг	400Мбит/с
Производительность брандмауэра	1,9Гбит/с
Фиксированные порты WAN	3 x GE (1 x Combo)
Емкость коммутации	32Гбит/с
Слоты	Слоты SIC: 4 Слоты WSIC (по умолчанию/максимум): 2/4 Слоты XSIC (по умолчанию/максимум): 0/2
Надёжность	ACL, брандмауэр, аутентификация 802.1x , аутентификация MAC-адреса, веб-аутентификация, аутентификация AAA, аутентификация RADIUS, аутентификация HWTACACS, подавление широковещательного шторма, безопасность ARP, защита от атак ICMP, URPF, защита IP- источника, отслеживание DHCP, CPICAR, черный список, трассировка IP-источника

Окончание таблицы 3

Характеристики	AR2220
QoS	Режим Diffserv, MPLS QoS, преобразование приоритета, ограничение трафика (CAR), выравнивание трафика, предотвращение перегрузки (на основе приоритетности IP/DSCP WRED), управление перегрузкой (интерфейс LAN: SP/WRR/SP+WRR; интерфейс WAN: PQ/ CBWFQ), MQC (классификатор трафика, характер трафика и политика трафика), H-QoS, WLAN QoS, FR QoS, интеллектуальное управление приложением (SAC)
Память	2Гб
Поддержка	Ethernet, CE1/CT1, E1/T1, ADSL2+, G.SHDSL, последовательный синхронный/асинхронный, ISDN, CPOS
LAN стандарты	IEEE 802.1P, IEEE 802.1Q, IEEE 802.3, управление VLAN, управление MAC-адресом, MSTP
Базовые услуги	Клиент/сервер DHCP, клиент/сервер PPPoE, клиент/сервер PPPoA, клиент/сервер PPPoEoA, NAT, управление субинтерфейсом
Поддержка голоса	RTP, SIP, SIP AG, IP PBX/TDM PBX, FXO/FXS, VoIP/конференц-связь, BESA, DISA, SBC, контроллер зоны H.323
WLAN контроллер сессий	Управление AP (обнаружение AC/доступ AP/управление AP),CAPWAP, управление пользователем WLAN, управление радиоканалом WLAN (802.11a/b/g/n),WLAN QoS(WMM), безопасность WLAN (WEP/WPA/WPA2/управление ключами)
Электропитание	Переменный ток 100 -240В; Частота: 50/60 Гц Постоянный ток -48 ~-60В
Высота стойки	RU
Размеры (В x Ш x Г)	44,5 мм x 442 мм x 420 мм

3. Коммутатор Huawei S5700-28P-LI-AC

S5700-LI – это гигабитный Ethernet-коммутатор второго уровня нового поколения, использующий энергосберегающие технологии, предоставляющий гибкий доступ портов GE и широкий набор сервисов. Он поддерживает функции EEE (Energy Efficient Ethernet, 802.3az) и режим «ожидания», обеспечивая заказчиков энергоэффективным, управляемым, расширяемым и экономически выгодным решением для организации гигабитных подключений устройств доступа.

- 24 порта 10/100/1000Base - T и 4 порта 100/1000Base-X SFP

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		35

•2 модели с питанием от сети переменного и постоянного тока, поддерживающие RPS (резервный источник питания)

• Производительность: 42 млн. пакетов/с

Коммутатор S5700-LI предлагает широкий выбор режимов энергосбережения – стандартный, основной и расширенный – удовлетворяющих большинству требований. Путем установки параметров "port link down/up", "optical-module in-place/out of place", "port shut down/undo shutdown", "idle period", "busy period" возможно увеличение временных интервалов динамического энергосбережения для снижения потребления энергии. В серии S5700-LI использовано множество инновационных энергосберегающих технологий, включая Energy Efficient Ethernet (EEE), определение требуемой энергии на порт, динамическое регулирование частоты ЦПУ и режим "ожидания" устройства, которые значительно сокращают энергопотребление без ущерба для производительности. Кроме протоколов STP, RSTP и MSTP коммутаторы S5700-LI поддерживают улучшенные технологии надежности Ethernet, включая Smart Link и RRPP (Rapid Ring Protection Protocol), которые реализуют защитное переключение каналов в течение миллисекундных интервалов и гарантируют высокую надежность работы сети. Коммутаторы также реализуют варианты Smart Link и RRPP со множеством экземпляров (multi-instance) для балансировки нагрузки между каналами, оптимизируя использование полосы пропускания. S5710-52C-PWR-LI S5700-LI 03 Хорошо спроектированные механизмы политик качества обслуживания (QoS) и безопасности S5700-LI осуществляет сложную классификацию трафика на основе информации пакетов, такой как «5-tuple», IP-приоритет, тип сервиса (ToS), поле DSCP, тип IP-протокола, тип ICMP, порт TCP источника, идентификатор VLAN ID, тип Ethernet-протокола, класс обслуживания CoS. Списки управления доступом ACL могут применяться для входящего и исходящего трафика на интерфейсе. S5700 поддерживает функцию CAR на основе потоков с двумя значениями скорости и трехцветной маркировкой. Каждый порт поддерживает 8 очередей и широкий набор алгоритмов

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		36

диспетчеризации, таких как WRR, DRR, PQ, WRR+PQ и DRR+PQ. Благодаря данным возможностям гарантируется качество голосовых услуг, видео услуг и услуг передачи данных. Серия S5700-LI обеспечивает защиту от атак типа «отказ в обслуживании» (DoS), а также атак на сеть или против пользователей. DoS-атаки включают в себя атаки SYN Flood, Land, Smurf и ICMP Flood. К атакам на сеть относятся атаки STP BPDU / Root. Атаки против пользователей включают в себя атаки поддельного сервера DHCP, атаки с S5700-LI поддерживает интеллектуальный протокол защиты (Smart Ethernet Protection, SEP) – протокол для кольцевых топологий Ethernet, работающий на канальном уровне. SEP может быть использован в разомкнутых кольцевых топологиях и может развертываться на агрегирующих устройствах верхнего уровня для обеспечения быстрого переключения (в пределах 50 мс), обеспечивая непрерывную передачу сервисов.

Таблица 4 – Характеристики коммутатора S5700-28P-LI-AC [7]

Характеристики	S5700-28P-LI-AC
Порт 1000M	24*10/100/ 1000Base-T, 4*100/1000 Base-X SFP
Слот расширения	В S57C имеются 2 слота расширения: один – для дополнительной платы восходящего подключения, другой - для стековой платы
Таблица MAC-адресов	<ul style="list-style-type: none"> • 16K MAC-адресов • Соответствие стандарту IEEE 802.1d • Механизмы обучения и устаревания MAC-адресов • Статические и динамические адреса, а также MAC-адреса типа «черная дыра» • Фильтрация пакетов на основе MAC-адресов источника
VLAN	4K VLAN Виртуальные сети - гостевая (guest), голосовая (voice) Назначение VLAN на основе MAC-адресов, протоколов, IP-подсетей, политик и портов Преобразование VLAN в режиме 1:1 и N:1 SuperVLAN (поддерживается на S5710-LI)
Характеристики	S5700-28P-LI-AC

Окончание таблицы 4

Характеристики	S5700-28P-LI-AC
Надежность	Протокол защиты кольцевой топологии RRPP, в том числе множественные экземпляры RRPP. Протокол защиты древовидной топологии Smart Link, в том числе множественные экземпляры Smart Link, обеспечивающие переключение в течение миллисекундных интервалов .SEP, ERPS(G.8032), STP(IEEE 802.1d), RSTP(IEEE 802.1w) и MSTP(IEEE 802.1s), Защита BPDU, корневого коммутатора STP, защита от петель (loop) , E-Trunk (поддерживается на S5710-LI)
IP- маршрутизация	Статическая маршрутизация, ECMP (поддерживается на S5710-LI)
QoS/ACL	Ограничение скорости передачи пакетов, отправленных и полученных интерфейсом Перенаправление пакетов Политика трафика на основе порта и функция ограничения трафика CAR с двумя граничными значениями и трехцветной маркировкой 8 очередей на каждый порт Алгоритмы диспетчеризации WRR, DRR, PQ, WRR+PQ и DRR+PQ Перемаркировка приоритета 802.1p и приоритета DSCP
Безопасность	Управление уровнями привилегий пользователя и парольная защита Защита от DoS-атак, ARP-атак и ICMP-атак Поддержка привязки IP-адреса, MAC-адреса, интерфейса и VLAN Функции изоляции портов (port isolation), безопасность портов (port security) и закрепления адресов (sticky MAC) MAC-адреса типа "черная дыра" (Blackhole) Ограничение количества изученных MAC-адресов Аутентификация 802.1x и ограничение количества пользователей на интерфейсе Аутентификация AAA, аутентификация RADIUS, аутентификация HWTACACS и NAC SSH v2.0 Протокол защищенной передачи гипертекстов (HTTPS) Защита центрального процессора (CPU) "Черный" и "белый" списки
Входное напряжение	<ul style="list-style-type: none"> • Переменный ток: • Диапазон номинального напряжения: 100 ~ 240В; 50/60 Гц • Диапазон максимального напряжения: 90 ~ 264В; 50/60 Гц • Постоянный ток: • Диапазон номинального напряжения: -48 ~ -60В • Диапазон максимального напряжения: -36 ~ -72В • Примечание: для коммутаторов с функцией PoE источники питания постоянного тока не используются.
Габариты (Ш x Г x В)	442 мм x 220 мм x 43,6 мм
Энергопотребление	25Вт

4. Платформа Quidway® CX380 Metro

Используя обширный опыт в области сетей MAN операторского класса, Huawei разработала платформу Quidway® CX380. Она разворачивается на уровне UPE городской сети Ethernet с возможностью обеспечения до 120 портов GE или 2 портов 10GE и 96 портов GE. CX380 обеспечивает выполнение высокодоходных услуг (доступ, конвергенция и транспорт) на базе технологий MPLS и IP с использованием высокотехнологичной транспортной платформы передачи данных.

Помимо гибкости конфигурирования и хорошего уровня совместимости, унаследованного от современных MAN, CX380 обеспечивает надежность операторского класса, масштабируемость и мультисервисную поддержку, устраняя узкие участки традиционных коммутаторов Ethernet, обеспечивающих лишь возможность соединения. CX380 поддерживает широкий диапазон плат и интерфейсов, обладает высокой плотностью портов и производительностью, предлагает сервис-провайдерам идеальные возможности масштабирования и конфигурирования под конкретные цели.

CX380 поддерживает следующие услуги:

- 1) VPN на основе виртуальной частной линии Ethernet Уровня 2;
- 2) VPN на основе виртуального частного сегмента LAN (VPLS);
- 3) Конвергирование Ethernet высокой плотности;
- 4) Платформа MAN MultiPlay;
- 5) Постепенная модернизация для поддержки мультисервисного L3 VPN, традиционного TDM/ATM и синхронизации Ethernet.

Функции платформы CX380:

- 1) Создан для защиты ваших инвестиций и сокращения эксплуатационных расходов.

Платформа CX380 основана на гибкой программируемой NP-архитектуре. CX380 поддерживает повторное использование плат CX200/300, что поможет защитить ваши инвестиции. CX380 поддерживает коммутационную емкость до 160 Гбит/с. Наличие восьми конфигурируемых сервисных плат позволяет

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		39

операторам конфигурировать оборудование под конкретные цели и поддерживать услуги отдельно, что обеспечивает дополнительную гибкость при их реализации в сфере сети. Благодаря малой глубине корпуса (300 мм), CX380 легко можно установить даже в малых автозалах, что поможет сократить эксплуатационные затраты.

2) Функция иерархического развертывания QoS для обеспечения требований SLA

Реализуя HQoS на CX380, операторы получают возможность обеспечения требований соглашений об уровне обслуживания. CX380 обеспечивает планирование и буферизацию QoS на уровне сети, реализуя требования различных услуг в отношении полосы пропускания, коэффициента потерь пакетов, задержки, искажения, гарантируя таким образом транспортные услуги операторского класса.

- Классификация трафика

CX380 может классифицировать трафик в соответствии с требованиями. Кроме того, данная платформа выполняет повторную разметку, управление трафиком, управление перегрузками в сети, ограничение скорости порта на классифицированных пакетных потоках, обеспечивая таким образом высококлассное сетевое функционирование для таких дополнительных услуг, как NGN, IPTV и услуги широкополосного доступа.

- HQoS

Как правило, QoS выполняет планирование в соответствии с полосой пропускания порта. Компонент QoS учитывает уровень обслуживания, но пользователи при этом не затрагиваются. Кроме того, затруднено выполнение управления потоком на множественных услугах одновременно. Функция HQoS способна обойти эти ограничения.

- MPLS и QoS

С помощью повторной разметки поля EXP в кадре MPLS CX380 может регулировать сопоставление между приоритетами EXP и 802.1p. Это дает

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		40

возможность различать кадры MPLS с различным приоритетом в QoS сети, что гарантирует гибкий доступ MPLS

- 3) Гарантия обслуживания и оперативное устранение неисправностей для поддержки сети операторского класса.

Горячая замена плат и резервирование ключевых компонентов по схеме 1+1 (включая SPU, вентилятор и блок питания) позволяют CX380 обеспечивать расширенную надежность на уровне оборудования.. Благодаря использованию отдельных маршрутов для управления и обслуживания, CX380 защищает оборудование от возникновения ошибок исключения. Защита канала CX380 обеспечивается СЛ кросс-платы порта Ethernet и аппаратными компонентами 8К MPLS OAM/BFD для оперативного обнаружения и переключения между группами защиты LSP в течение 50 мс, гарантируя таким образом комплексное обнаружение сбоев и защиту.

- 4) Развертывание сети MPLS для обеспечения последовательного функционирования.

CX380 поддерживает широкий диапазон функций MPLS, включая основные функции MPLS, LDP/RSVP-TE, MPLS TE и MPLS OAM. С помощью MPLS TE CX380 сочетает MPLS с трафик-инжинирингом для установки туннелей LSP на маршрутах для резервирования ресурсов и запланированной оптимизации. Кроме того, устройство может защищать сеть от сбоев узлов или каналов посредством использования оперативной перемаршрутизации и резервных каналов.

- 5) Привязка и ACL на базе DHCP для оптимизации безопасности сети

CX380 можно развернуть между сервером DHCP и клиентом DHCP для мониторинга пакетов DHCP и предотвращения приема некорректных пакетов таблицей привязки IP+MAC. CX380 также может устанавливать или убирать строку Option82 в пакетах DHCP. До 32К аппаратных L2/L3 ACL могут использоваться для охраны пользователей от злонамеренных пакетов. Устройство также реализует услуги контролируемой многоадресной передачи.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		41

6) Репликация многоадресной передачи и развертывание многоадресной передачи MPLS для поддержки несущей сети Multi-Play .

CX380 поддерживает широкий диапазон функций многоадресной передачи, включая отслеживание IGMP, VLAN многоадресной передачи и мощные функции репликации многоадресной передачи. Устройство предоставляет целый набор функций многоадресной транспортировки по сети VPLS, облегчая развертывание многоадресных видеослужб в сети L2VPN (например, IPTV)

7) Построение MAN на базе CX380.

В качестве UPE MAN CX380 может предоставлять услуги доступа к Internet, VPN, IPTV и VoIP с таких устройств нисходящей передачи данных, как коммутатор LAN, DSLAM, MSAN и CX200. Услуги CX380 можно конвергировать в восходящем направлении на NPE (например, Huawei ME60 или NE40E). В сложных сетях можно также добавить PE-AGG между NPE и CX380 (например, Huawei CX600). При этом услуги CX380 будут конвергироваться непосредственно на CX600. [8]

5. VoIP шлюз Huawei U-SYS IAD 132 (32 порта).

Имеется доступ между пользователями POTS и IP сети, POTS и PTSN. IAD 132 работает в сети с Softswitch посредством H.248 или MDCP. В сети доступа IP (IP Access Network) оборудование может работать с сетью Edge Trunk Gateway (ETG), соединяя звонки между обычным абонентом и абонентом под контролем Softswitch или ETG. Модель имеет конфигурации с фронтальным и задним расположением портов.

Таблица 5 – Характеристики VoIP шлюза Huawei U-SYS IAD 132 (32 порта) [9]

Характеристики	U-SYS IAD 132 (32 порта)
Стандарты	MGCP, SIP, RTP/RTCP, SDP, G.711, G.723, G.729, VAD, CNR, EC, SPC, Fax T.38, transparent fax, PPPoE, DHCP, VLAN
Интерфейс	ТфОП: Модуль ASI обеспечивает 16 FXS-интерфейсов Ethernet: четыре интерфейса 10/100Base-TX Последовательный порт управления RS232 (консоль)

Окончание таблицы 5

Характеристики	U-SYS IAD 132 (32 порта)
Емкость	ASI-модуль поддерживает 16 аналоговых телефонных абонентов. Всего устанавливается до двух ASI-модулей. Один порт передачи данных
Электропитание	100 В – 240 В, 50 Гц – 60 Гц , Переменного тока - 12В, Постоянного тока – 3А
Энергопотребление	74,4Вт
Рабочая температура	0°С – 55°С
Влажность	Длительная: 5% – 85% (без конденсации) Краткосрочная: 0% – 90%
Габариты (Ш x Г x В)	436 мм (Ш) × 365 мм (Г) × 42 мм (В)
Вес	≈5кг

3.2.2 Расчет объема оборудования

В городе Белгород существует два филиала компании «Металлоторг» на улице Почтовая и улице Чичерина. Для каждого филиала была создана схема сети связи, в которой было использовано следующее оборудование, представленное в таблице 6.

Таблица 6 – Объем оборудования

Название оборудование	Количество, шт.
Платформа Quidway CX380 Metro	1
Маршрутизатор малого офиса Huawei AR2220	1
Коммутатор на 24 порта Huawei S5700-28P-LI-AC	4
Камера видеонаблюдения АНД	8
Принтер HP LaserJet M806+	3
Персональный компьютер	48
IP-телефон	4
Точка доступа	4
Сканер	2

Для функционирования сети связи в городе Белгород была выбрана одна платформа Quidway CX380 Metro, в которую уже встроен маршрутизатор и VoIP шлюз, оборудование будет размещено в помещении серверной, на улице Почтовая, в филиале с наибольшим количеством абонентов. На территории филиала будет размещено 2 коммутатора на 1 и 2 этажах. Каждый коммутатор имеет 24 порта, поэтому будет задействовано оборудование: 2 камеры видеонаблюдения, 1 IP-телефон, 1 точка доступа WiFi на двух этажах, а так же на первом этаже будет подключено 10 ПК и принтер, а на втором этаже 13 ПК и сканер. Для первого этажа было оставлено 9 запасных портов в коммутаторе, а на втором 6. На улице Чичерина будет задействован маршрутизатор среднего офиса AR2220, а так же два коммутатора на 1 и 2 этажах. Каждый коммутатор имеет 24 порта, поэтому будет задействовано оборудование: 2 камеры видеонаблюдения, 1 IP-телефон, 1 точка доступа WiFi на двух этажах, а также на первом этаже будет подключено 12 ПК и принтер, а на втором этаже 13 ПК, сканер и принтер. Для первого этажа было оставлено 7 запасных портов в коммутаторе, а на втором 5.

					11070006.11.03.02.116.ПЗВКР	<i>Лист</i>
<i>Изм.</i>	<i>Лист</i>	<i>№ докум</i>	<i>Подпись</i>	<i>Дата</i>		44

4 РАЗРАБОТКА МОДЕЛИ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ ГРУППЫ КОМПАНИЙ «МЕТАЛЛОТОРГ»

4.1 Выбор среды моделирования

Для того, чтобы проанализировать структуру проектируемой сети связи в Белгородском филиале группы компаний «Металлоторг», а также организовать сеть VPN между филиалами компании, принято решение создать модель сети связи в среде моделирования 10 – Strike.

Программа позволяет создать схему сети, обнаружить сетевые устройства и поместить их на карту-схему, а так же автоматически рисует связь между коммутаторами, если они поддерживают протокол SNMP. Так же в комплекте с этой программой выступают сетевые программы для мониторинга сети, которые помогут в разработке более подробной схемы сети связи и для корпоративной сети и для магистральной.

Это такие программы, как:

- 10-Strike LANState – программа администрирования компьютеров и мониторинга сети ,
- 10 – Strike Network File Search – программа для поиска файлов в локальной сети и на FTP-серверах,
- 10-Strike Connection Monitor - программа для отслеживания и контроля подключений к сетевым ресурсам компьютера.

На рисунке 3 представлена схема сети группы компаний «Металлоторг», которая была создана с помощью программы 10 – Strike.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		45

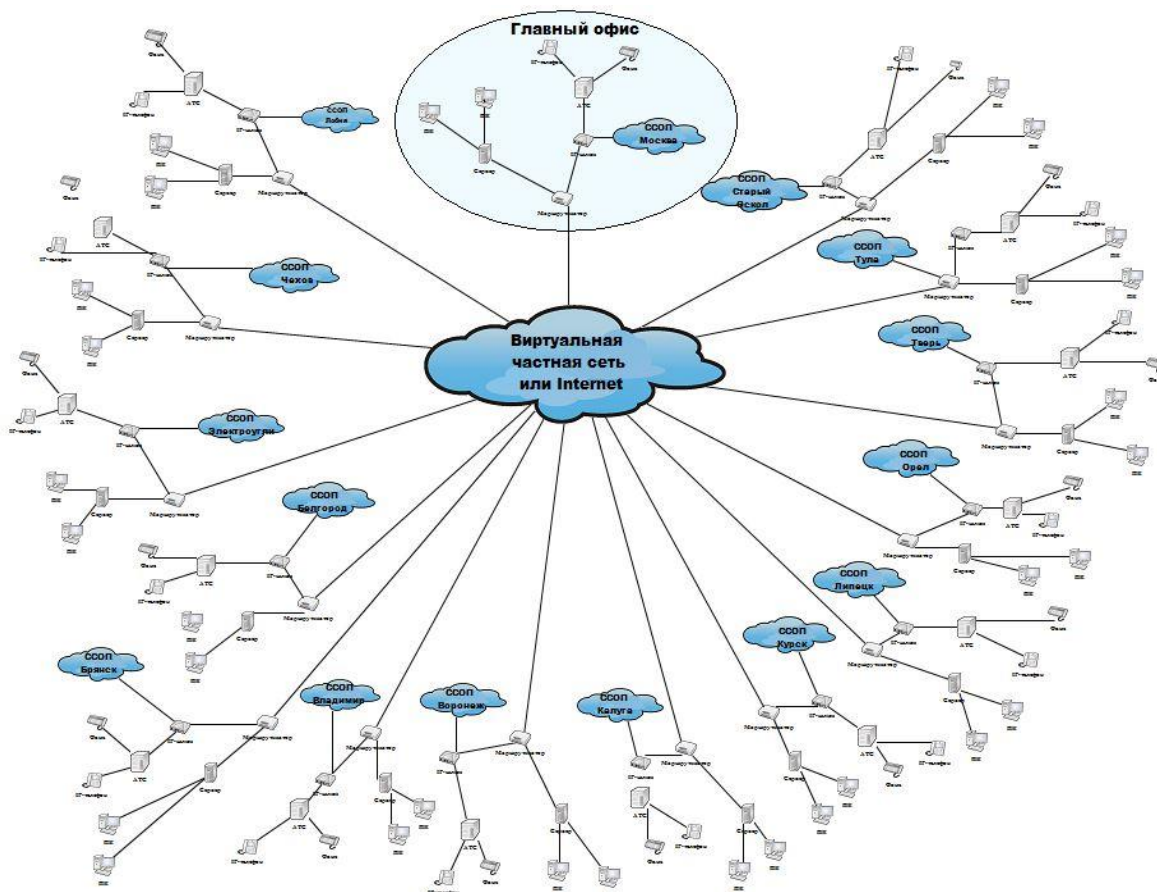


Рисунок 3 – Схема сети группы компаний «Металлоторг» в программе 10 – Strike

Для организации сети VPN была использована программа Cisco Packet Tracer, навыки работы с которой приобретены во время занятий по дисциплине «Сети связи». В данной среде удобно организовывать сеть VPN на базе оборудования, представленного в библиотеке компонентов программы.

4.2 Разработка плана IP-адресации

Для проектирования сети VPN необходимо назначить каждому маршрутизатору, находящегося в сети, IP адрес. В таблице 7 представлен план IP-адресации.

Таблица 7 – План IP-адресации

Название города	IP-адрес
Главный офис г. Москва	172.0.0.1
Лобня	172.1.0.1
Чехов	172.2.0.1
Электроугли	172.3.0.1
Белгород	Ул. Почтовая: 172.4.1.1
	Ул. Чичерина: 172.4.2.1
Брянск	172.5.0.1
Владимир	172.6.0.1
Воронеж	172.7.0.1
Калуга	172.8.0.1
Курск	172.9.0.1
Липецк	172.10.0.1
Орел	172.11.0.1
Тверь	172.12.0.1
Тула	172.13.0.1
Старый Оскол	172.14.0.1
Промежуточные маршрутизаторы	172.0.1.1 – 172.0.1.7

4.3 Разработка модели сети в среде Cisco Packet Tracer

Для разработки сети VPN была взята программа Cisco Packet Tracer. На рисунке 4 изображена схема реализации сети VPN между центральным офисом в городе Москва и филиалом, который находится в городе Белгород.

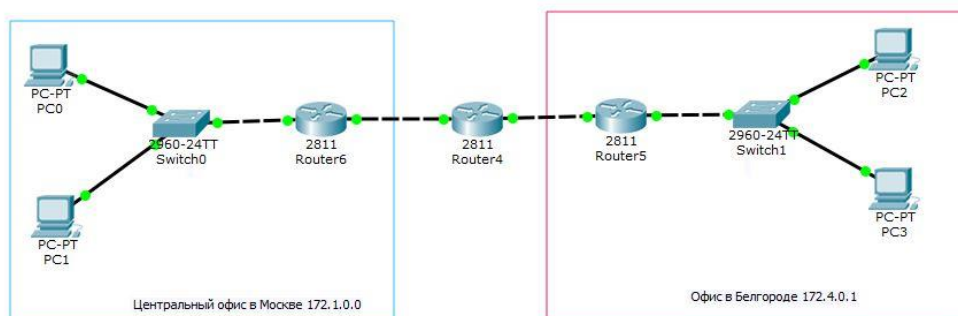


Рисунок 4 – Схема реализации сегмента сети VPN

Сначала были настроены ПК для главного офиса и филиала. Для каждого из ПК был определен свой IP-адрес.

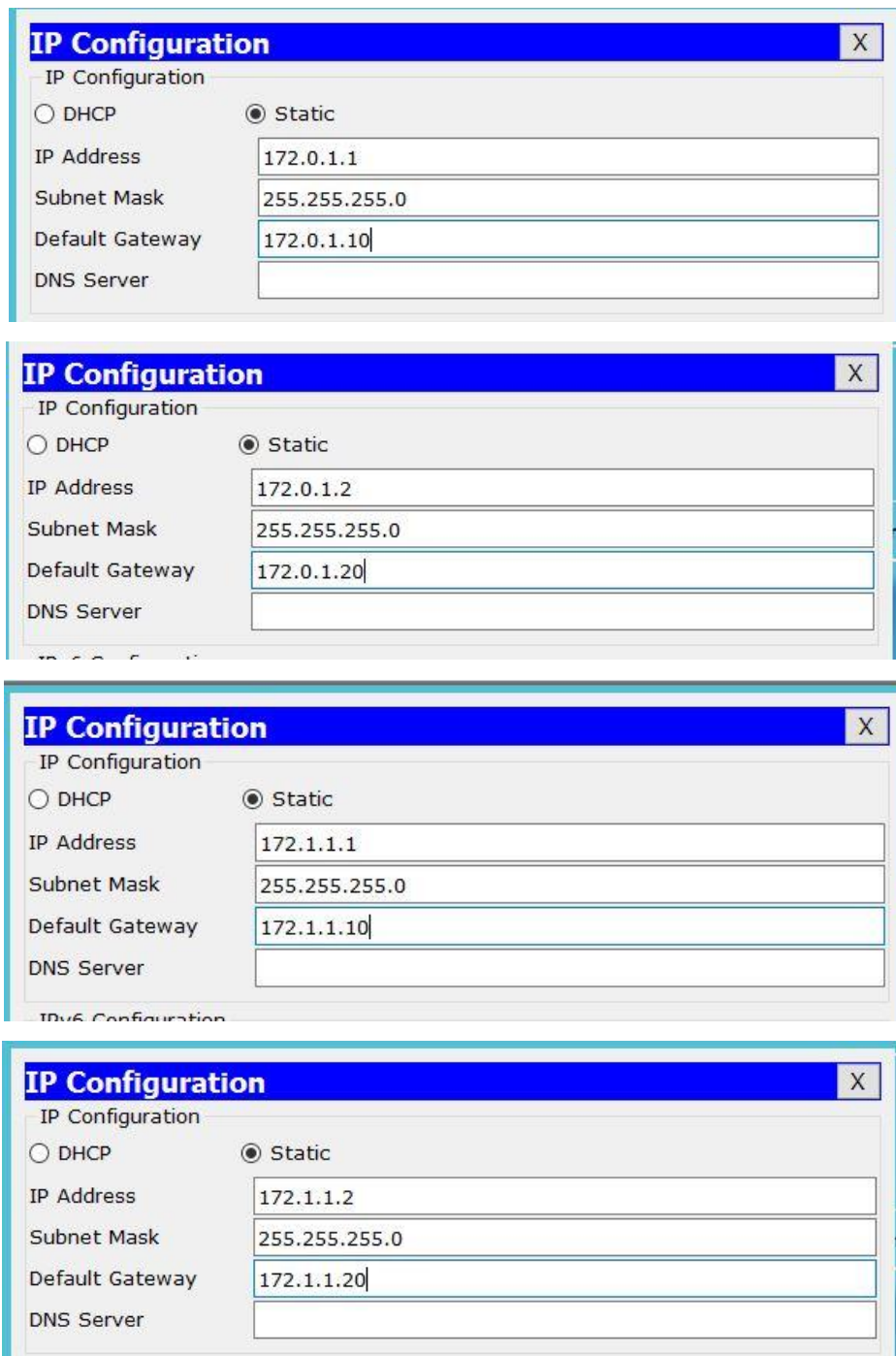


Рисунок 5 – Присвоение ПК IP-адреса

В дальнейшем были произведены все базовые настройки маршрутизатора. Пример был показан на маршрутизаторе R1. Для начала даем имя маршрутизатору, затем выключаем поиск DNS и включаем пароль для привилегированного режима. Далее входим в настройки консоли, назначаем

пароль на вход и включаем запрос пароля перед входом в консоль. Затем входим в режим telnet и так же назначаем и включаем пароль на вход. Для того, чтобы сеть функционировала, необходимо включить интерфейсы и назначить им IP-адрес и маску.

```
Router(config)#hostname R1
R1(config)#no ip domain lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 6 – Базовая настройка маршрутизатора R1

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fa 0/0
R1(config-if)#ip address 200.1.1.0 255.255.255.0
Bad mask /24 for address 200.1.1.0
R1(config-if)#des subnet A
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

R1(config-if)#exit
R1(config)#interface fa 0/1
R1(config-if)#ip address 172.1.0.0 255.255.255.0
Bad mask /24 for address 172.1.0.0
R1(config-if)#des subnet B
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up

R1(config-if)#end
R1#
```

Рисунок 7 – Настройка интерфейсов

Такие же действия были совершены на двух других маршрутизаторах. Далее началась установка VPN соединения между центральным офисом и филиалом. Для начала необходимо настроить протокол NAT, позволяющий преобразовывать IP-адреса транзитных пакетов, то есть обеспечить доступ в Интернет. Был определен интерфейс FastEthernet 0/0 как IP NAT OUTSIDE, а интерфейс FastEthernet 0/1 как IP NAT INSIDE. Далее был создан access-list,

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		49

который будет определять трафик, который будет идти в сеть Интернет. Далее указана сеть (для центрального офиса) с wildcard маской (т.е. 0.0.0.225).

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fa 0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#int fa 0/1
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#ip access-list standard FOR-NAT
R1(config-std-nacl)#permit 172.1.0.0 0.0.0.255
R1(config-std-nacl)#exit
R1(config)#ip nat ?
    inside      Inside address translation
    outside     Outside address translation
    pool        Define pool of addresses
R1(config)#ip nat inside source list FOR-NAT interface fa0/0 overload
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#wr mem
Building configuration...
[OK]
R1#
R1#
```

Рисунок 8 – Настройка NAT

Такие же действия были совершены на двух оставшихся маршрутизаторах. В дальнейшем была произведена настройка VPN.

Есть несколько этапов настройки виртуальной частной сети:

1 этап – Настройка первой фазы.

Создается политика crypto isakmp в policy 1, где указывается алгоритм шифрования 3des, алгоритм хэширования md5, тип аутентификации pre-share и алгоритм для обмена pre-share ключами group 2 – это параметры, необходимые для построения мини – туннеля isakmp, через который будут передаваться параметры основного ipsec туннеля.

2 этап – Настройка ключа аутентификации и пира.

Производится настройка pre-share key и задается IP адрес пира, то есть маршрутизатора филиала. Секретный ключ – lazarak. А адресом пира является адрес внешнего интерфейса роутера на филиале, т.е. 200.1.1.1.

3 этап – Настройка второй фазы.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		50

Указываются параметры, необходимые для построения ipsec туннеля – имя, алгоритм шифрования и алгоритм хэширования.

4 этап – Определение трафика, который необходимо зашифровать

Необходимо создать access-list, то есть определить какой трафик будет заворачиваться в VPN тоннель. Указывается IP адрес центрального офиса и филиала, в который необходимо передать информацию, в нашем случае в город Белгород. Для того, чтобы не правильно осуществить NAT трафика необходимо изначально указать запрещенный трафик, то есть тот трафик, который не нужно преобразовывать, это трафик от центрального офиса до филиала, а затем указать весь остальной трафик, который можно преобразовывать.

5 этап – Создание криптокарты и привязка к интерфейсу

Создается криптокарта CMAP 10 ipsec. В качестве пира используется внешний адрес маршрутизатора центрального офиса. Указывается access-list и привязывается к интерфейсу FastEthernet 0/0.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
R1(config)#crypto isakmp key lazarak address 200.1.1.1
R1(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
R1(config)#ip access-list extended FOR-VPN

R1(config)#ip access-list extended FOR-NAT
R1(config-ext-nacl)#deny ip 172.1.0.0 0.0.0.255 172.4.0.1 0.0.0.255
R1(config-ext-nacl)#permit ip 172.1.0.0 0.0.0.255 any
R1(config-ext-nacl)#exit
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)#set peer 200.1.1.1
R1(config-crypto-map)#set transform-set TS
R1(config-crypto-map)#match address FOR-VPN
R1(config-crypto-map)#exit
R1(config)#interface fa 0/0
R1(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
R1(config-if)#exit
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#wr mem
Building configuration...
[OK]
R1#
```

Рисунок 9 – Настройка VPN

									Лист
									51
Изм.	Лист	№ докум	Подпись	Дата	11070006.11.03.02.116.ПЗВКР				

Таким образом, применение VPN в компании «Металлоторг» избавит от необходимости строить собственную транспортную инфраструктуру, а также снизит стоимость оплаты за выделенный канал.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		52

5 ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ

5.1 Расчет капитальных вложений

Общая стоимость оборудования определяется в зависимости от проектируемой емкости сети и удельных затрат на одну абонентскую линию. Так как проект реализован на базе импортного оборудования, объемы капиталовложений указаны в рублях и иностранной валюте (при расчетах в иностранной валюте использован курс ЦБ РФ).

Капитальные вложения представляют собой смету затрат на реализацию проекта, и включают в себя все необходимое коммуникационное оборудование (коммутаторы, маршрутизаторы, модемы, абонентские платы), линию связи (кабель, либо стоимость аренды виртуального канала, стоимость аренды частотного ресурса), стоимость лицензионного программного обеспечения и т.д.

Общие капитальные вложения на приобретение оборудования могут быть вычислены по формуле:

$$K_{об} = \sum_{i=1}^N K_i, \text{ руб} \quad (20)$$

где $K_{об}$ - суммарный объем затрат на приобретение оборудования, руб;

K_i – общая стоимость одной позиции (типа оборудования);

N – количество позиций.

В таблице 8 представлена смена затрат на приобретение оборудования.

Цены на оборудование взяты из источников [10,11,12,13,14,15,16,17,18], с учетом курса валют на дату обращения. В реальных условиях на закупку оборудования объявляется тендер, и цены могут отличаться от использованных в проекте.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		53

Таблица 8 – Смета затрат на приобретение оборудования

Наименование	Кол-во единиц	Стоимость (руб)	
		за единицу	всего
Маршрутизатор главного офиса Huawei AR3260	1	430 171	430 171
Маршрутизатор среднего офиса Huawei AR2220	4	86 167	344 668
Коммутатор Huawei S5700-28P-LI-AC	8	81 855	654 840
Платформа Quidway® CX380 Metro*	1	5 329 225	5 329 225
VoIP шлюз Huawei U-SYS IAD 132 (32 порта)	1	68 200	68 200
Двухволоконный модуль, SFP 1000BaseLX	4	816	3 264
ИБП UPS General Electric GT 6000 (UPS & Battery Module are separately packed)	2	251 134	502 268
ОКК-10-0,22-4П (3,5 кН)**	13 000	51,97	675 610
Кабель UTP cat 5e , м	5 690	15	85 350
Оплата разработки проекта			2 000 000
Сертификат на обучение персонала по эксплуатации нового оборудования	8	45 000	360 000
Муфта кабельная 1КВТпО 1х300-400	20	1507,37	30 147,4
Wi-Fi роутер TP-LINK TL-WR940N	8	1959	15 672
Итого:			10 499 244

Примечание* Цена Платформы Quidway® CX380 Metro включает в себя стоимость: стativa, стойки, оборудования, устройства климатехники, модулей электрического питания, в том числе резервного, серверной части.

**ОКК-10-01-1,0-8 - кабель городской на основе одномодового оптического волокна с диаметром модового поля 10 мкм, с коэффициентом затухания 0,22 дБ/км, с числом оптических волокон 4.

При приобретении оборудования обычно предусматриваются следующие расходы: $K_{пр}$ – Затраты на приобретение оборудования; $K_{тр}$ – транспортные расходы в т.ч. таможенные расходы (4% от $K_{пр}$); $K_{смр}$ – строительно-монтажные расходы (20% от $K_{пр}$); $K_{т/у}$ – расходы на тару и упаковку (0,5% от $K_{пр}$); $K_{зср}$ –

заготовительно-складские расходы (1,2% от $K_{пр}$); $K_{пр}$ – прочие непредвиденные расходы (3% от $K_{пр}$).

Общие затраты на прокладку кабеля составят:

$$K_{каб} = L * Y \quad (21)$$

где L – длина трассы прокладки кабеля; Y – стоимость 1 км. прокладки кабеля.

$$K_{каб} = L * Y = 13000 * 250 = 3250000$$

Таким образом, общие капитальные вложения рассчитываются как:

$$KB = K_{об} + (K_{пр} + K_{тр} + K_{смп} + K_{м/у} + K_{зсп} + K_{нпр})K_{об} + K_{каб}, \text{ руб} \quad (22)$$

$$KB = 10499244 + 10499244 * (0.04 + 0.2 + 0.03 + 0.012 + 0.005) + 3250000 = 16762527,028, \text{ руб}$$

5.2 Калькуляция эксплуатационных расходов

Эксплуатационными расходами называются текущие расходы предприятия на производство или предоставление услуг. В состав эксплуатационных расходов входят все расходы на содержание и обслуживание сети. Эти расходы имеют текущий характер. Эксплуатационные расходы по своей экономической сущности выражают себестоимость услуг связи в денежном выражении.

Для определения эксплуатационных расходов по проекту используются следующие статьи:

1. затраты на оплату труда;
2. страховые взносы;
3. амортизация основных фондов;
4. материальные затраты;
5. прочие производственные расходы.

Для расчета годового фонда заработной платы необходимо определить численность штата производственного персонала.

В случае если проект предполагает создание новой сети, то необходимо спланировать количество рабочих, которое позволит своевременно и

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		55

эффективно выполнять задачи по развертыванию сети и подключение новых абонентов к сети. Если проект предполагает модернизацию существующей сети, то возможны два варианта: увеличение персонала, либо его сокращение. Определенный состав персонала представляется в проекте в виде таблицы. Сумма оклада работника зависит от региона, где он работает.

Таблица 9 – Состав персонала по обслуживанию оборудования

Наименование должности	Оклад	Количество, чел.	Сумма з/п, руб.
Ведущий инженер	30 000	1	30 000
Инженер 1 кат.	23 000	2	46 000
Инженер-программист.	25 000	2	50 000
Монтажник	20 000	4	80 000
Итого:		9	206 000

Годовой фонд оплаты труда для персонала рассчитывается как:

$$ФОТ = \sum_{i=1}^K (T * P_i * I_i) * 12, \text{ руб} \quad (23)$$

$$ФОТ = 30000 * 12 + 46000 * 12 + 50000 * 12 + 80000 * 12 = 2472000 \text{ руб}$$

где: I_i – количество работников каждой категории; P_i – заработная плата работника каждой категории, руб; 12 – количество месяцев; T – коэффициент премии (если премии не предусмотрены, то $T=1$).

Каждое предприятие обязано выплачивать налоги на каждого своего сотрудника, ранее этот налог назывался Единый социальный налог, но с 1 января 2010 года единый социальный налог (ЕСН) был заменён страховыми взносами, а его ставка повышена. Ранее ЕСН составлял лишь 26%, затем он был резко увеличен до 34%. Взносы включают в себя отчисления в: Пенсионный фонд (ПФР) — 22 %, Фонд медицинского страхования (ФФОМС) — 5,1 %, Фонд социального страхования (ФСС) — 2,9 %.

Как видно, на сегодняшний день (2016 год) этот показатель составляет порядка **30%** от заработной платы. В случае, если доход работника за 1 год превысит 796 тыс. рублей, то на него вносится дополнительный налог в 10%. При превышении базы в 718 тыс. рублей взносы в ФСС не уплачиваются).

$$CB = \Phi OT * 0,3, \text{ руб} \quad (24)$$

$$CB = 2472000 * 0,3 = 741600, \text{ руб}$$

Амортизация является процессом постепенного переноса стоимости основных средств на производимую продукцию (работы, услуги). Смысл амортизационных отчислений в накоплении средств для модернизации инфраструктуры в перспективе.

Начисление амортизации осуществляется в течение всего срока полезного использования основного средства.

Сроком полезного использования является период, в течение которого использование объекта основных средств приносит экономические выгоды (доход) организации. Срок полезного использования организация устанавливает самостоятельно при принятии объекта основных средств к учету. Таким образом, сумма амортизационных отчислений определяется по формуле:

$$AO = T / F, \text{ руб} \quad (25)$$

$$AO = 7332636 / 25 = 293305,44, \text{ руб}$$

где Т – стоимость оборудования,

F – срок службы этого оборудования.

В России пока еще действует документ (постановление совмина СССР от 22.10.90г 1072 (ред. От 06.04.2001) «о единых нормах амортизационных отчислений на полное восстановление основных фондов народного хозяйства СССР»), в котором предусмотрены все нормы по амортизации для любой из видов деятельности, в том числе и на оборудование отрасли связи. (Обратите

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		57

внимание на то, что под амортизацию не попадает ПО, затраты на транспортировку и т.д., т.е. учитывается только оборудование).

Материальные затраты составляют значительную статью эксплуатационных расходов. В них включена оплата потребляемой электроэнергии при эксплуатации сети, затраты на материалы и запасные части (ЗИП) и другое.

Эти составляющие материальных затрат определяются следующим образом:

а) затраты на оплату электроэнергии определяются в расчете, что все коммуникационные узлы вместе потребляют около 3 кВт/ч, а цена 1 кВт/ч в Белгороде на июнь 2016 года равна 3.53 рубля:

$$Z_{эн} = T * 24 * 365 * P \quad (26)$$

где T – тариф на электроэнергию (руб./кВт · час), P – мощность установок (кВт).

$$Z_{эн} = 3.53 * 24 * 365 * 3 = 92768,4 \text{ руб}$$

б) затраты на материалы и запасные части составляют 3,5% от основных производственных фондов и определяются по формуле:

$$Z_{мз} = KB * 0,035 \quad (27)$$

где KB – капитальные вложения, затраты на оборудование.

$$Z_{мз} = 16762527,028 * 0,035 = 586688,45 \text{ руб}$$

Общие материальные затраты определяются суммой двух статей:

$$Z_{общ} = Z_{эн} + Z_{мз} \quad (28)$$

где $Z_{эн}$ – затраты на оплату электроэнергии; $Z_{мз}$ – материальные затраты.

$$Z_{общ} = 586688,45 + 92768,4 = 679456,85$$

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		58

Прочие расходы предусматривают общие производственные ($Z_{пр.}$) и эксплуатационно-хозяйственные затраты ($Z_{эк.}$):

$$Z_{пр} = \Phi OT * 0,15 \quad (29)$$

$$Z_{эк} = \Phi OT * 0,25 \quad (30)$$

где ΦOT – годовой фонд оплаты труда.

$$Z_{пр} = 2472000 * 0,15 = 370800$$

$$Z_{эк} = 2472000 * 0,25 = 618000$$

Следовательно, прочие расходы равны:

$$Z_{прочие} = 370800 + 618000 = 988800$$

Произведен расчет годовых эксплуатационных расходов, полученные данные внесены в таблицу 10.

Таблица 10 – Годовые эксплуатационные расходы

Наименование затрат	Сумма затрат, руб.	Удельный вес статей, %
1. ФОТ	2472000	39
2. Страховые взносы	741600	11
3. Амортизационные отчисления	293305,44	20
4. Материальные затраты	679456,85	14
5. Расходы на аренду	280 000	5
6. Прочие расходы	988800	11
ИТОГО	5 455 162, 29	100

Выводы по разделу

Таким образом, в данном разделе осуществлена оценка капитальных вложений в предлагаемый проект и калькуляция эксплуатационных расходов.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		59

Определен общий дохода от реализации проекта, рассчитаны основные оценочные показатели проекта, характеризующие финансовый уровень решения задач. Рассчитанные технико-экономические показатели на конец расчетного периода сведены в таблицу 11.

Таблица 11 – Основные технико-экономические показатели проекта

Показатели	Численные значения
Количество абонентов в филиалах компании в г. Белгород Белгородской области, чел	Ул. Почтовая – 1011 абонентов Ул. Чичерина – 1102 абонента
Капитальные затраты, руб	16 762 527
Ежегодные эксплуатационные расходы, руб, в том числе:	5 455 162, 29
Расходы на оплату производственной электроэнергии	92 768
Расходы на материалы, запасные части и текущий ремонт	
Фонд оплаты труда	2 472 000
Страховые взносы	741 600
Амортизационные отчисления	293 305
Аренда VPN в год, руб	600 000
Общие производственные расходы	370 800

Разработанный проект мультисервисной сети связи имеет приемлемые экономические показатели. Капитальные вложения составили 16 762 527 рублей, эксплуатационные расходы - 5 455 162 рубля.

Анализ технико-экономических показателей проекта свидетельствует о достаточной степени эффективности принятых проектных решений и подтверждает их экономическую обоснованность. [19]

6 РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО РАЗМЕЩЕНИЮ СЕТЕВОГО ОБОРУДОВАНИЯ

В данном разделе будут описаны рекомендации по организации серверной, где планируется разместить оборудование проектируемой сети.

6.1 Выбор серверного помещения

Серверное помещение следует размещать как можно ближе к магистральным кабельным каналам. Желательно расположить серверное помещение рядом с главным распределительным пунктом (Main Cross, MC), а если есть возможность, то установить главный распределительный пункт в серверном помещении. Не размещать серверное помещение рядом с лифтовыми шахтами, лестничными пролетами, вентиляционными камерами и другими элементами здания, которые могут ограничить расширение аппаратного помещения в будущем. Серверное помещение рекомендуется размещать так, чтобы была возможность расширения помещения серверного помещения за счет площади смежного помещения.

6.2 Рекомендуемые размеры серверного помещения и конфигурация

Размер серверного помещения выбирается исходя из размера обслуживаемой рабочей области и количества устанавливаемого оборудования. Важно учесть не только размеры самого оборудования, но и способы монтажа, обеспечения доступа и обслуживания оборудования, возможность установки дополнительных устройств.

- 1) Высота серверного помещения должна быть не менее 2,44 метра.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		61

2) Минимально рекомендуемый размер серверной комнаты должен быть не менее 14 м².

3) Рекомендуется выделить под серверное помещение 0,09 м² площади на каждые 10 м² обслуживаемой рабочей площади.

В филиалах ГК «Металлоторг», где невысокая плотность размещения телекоммуникационных розеток, размер серверного помещения выбирается исходя не из площади рабочей области, а в зависимости от количества рабочих зон.

Таблица 12 - Рекомендуемый размер серверного помещения в филиалах с небольшой абонентской емкостью

Количество рабочих зон	Размеры серверного помещения, м2
до 100	14
101-400	37
401-800	74
801-1200	111

Окна

Рекомендуется под серверное помещение использовать помещение без окон. Если в серверном помещении имеются окна, то необходимо заложить окна кирпичом.

Дверь и дверной проем

Дверной проем должен быть в ширину не менее 0.91 м и высотой не менее 2 метров. Дверь должна закрываться на замок, чтобы ограничить доступ в кроссовое помещение. Допускается использование раздвижной двери. Навесная дверь должна открываться наружу, раскрытие двери должно быть не менее 1800. Если планируется внос габаритного оборудования в серверное помещение, то рекомендуется установить двойную дверь с минимальным проемом в ширину не менее 1.82 метра и высотой не менее 2,28 метра.

Подвесной фальшпотолок

Не рекомендуется использовать В серверном помещении подвесной фальшпотолок.

Отделка стен, потолка и пола

Стены, потолок и пол должны иметь покрытие, которое затрудняет выделение, оседание и накапливание пыли на поверхности. Потолок должен иметь гидроизоляцию, чтобы исключить протечку воды. Стены должны быть окрашены светлой краской.

Нагрузка на фальшпол и на перекрытие пола

Если в серверного помещения возможна установка тяжелого оборудования, например, аккумуляторных батарей, большого количества тяжелого оборудования в один монтажный конструктив (свыше 500 кг), то необходимо провести расчеты динамической и статической нагрузки на фальшпол и на перекрытие пола.

6.3 Электропитание и электрические розетки

Рекомендуется установить, как минимум, два отдельных блока двойных электрических розеток. Блоки электрических розеток рекомендуется запитать от разных питающих кабелей, электрические розетки должны быть рассчитаны на переменный ток до 16А. Дополнительно требуется установить блоки с двойными электрическими розетками с интервалом 1,8 метра вдоль стены на высоте не ниже 0,15 метра от уровня пола. Подача электропитания в серверное помещение должна осуществляться по выделенному силовому кабелю, желательно напрямую от главного распределительного щита. Если установлена система резервного электропитания, то серверное помещение должно быть запитано от системы резервного электропитания. Требуется установить отдельный электрический распределительный щит для серверного помещения. Разрешается установка источников бесперебойного питания (ИБП) до 100 кВА в

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		63

серверном помещении. ИБП мощностью свыше 100 кВА должны быть установлены в отдельном помещении. Подробнее вопросы электроснабжения серверного помещения рассмотрены в руководстве «Требования и рекомендации к серверному помещению и системам».

6.4 Заземление

В аппаратном помещении должна быть установлена магистральная телекоммуникационная заземляющая шина, к которой должны быть подключены заземляющие и соединительные проводники от монтажных конструктивов, телекоммуникационного оборудования, металлических кабелепроводов.

6.5 Прокладка магистральных кабелепроводов к серверному помещению. Средства распределения кабелей и организации кабельных потоков

К аппаратному помещению должны быть подведены магистральные кабелепроводы.

Для распределения кабелей и организации кабельных потоков в телекоммуникационном помещении необходимо использовать кабелепроводы и организаторы. Средства распределения и организации кабельных потоков должны быть надежно закреплены, выдерживать вес кабеля, должны обеспечить защиту и распределение кабелей с минимально допустимым радиусом изгиба кабеля. Кабелепроводы должны быть установлены от кабельного ввода в телекоммуникационное помещение до телекоммуникационных шкафов. Кабелепроводы расположенные под потолком, должны быть открыты и доступны для проведения дальнейших работ по прокладке кабелей, шнуров или перемычек. [].

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		64

7 ОХРАНА ТРУДА И ТЕХНИКА БЕЗОПАСНОСТИ

7.1 Микроклимат (температура, влажность, вентиляция) в помещении серверной

Система контроля и управления микроклиматом должна обеспечить в серверном помещении заданный уровень влажности и температуры необходимый для нормального функционирования активного оборудования. Система микроклимата должна обеспечить поддержку температурного режима не только летом, но и зимой и рассчитана на круглосуточную непрерывную работу. Если централизованная система микроклимата в здании не может обеспечить непрерывную работу и заданный уровень температуры и влажности, то необходимо установить автономную систему в серверном помещении.

Таблица 13 - Рекомендуемая температура и влажность в серверном помещении

Рекомендуемая температура, Ос	Рекомендуемая относительная влажность, %
18-27	40-55

При воздушном охлаждении измерение температуры и влажности должно осуществляться при работающем активном оборудовании на высоте 1.5 метра от уровня пола в зоне подачи холодного потока воздуха. При водяном охлаждении измерение температуры и влажности должно осуществляться при работающем активном оборудовании в монтажном конструктиве.

Требуется обеспечить воздушное давление в серверном помещении больше, чем в прилегающих помещениях. Рекомендуется смена воздуха в серверном помещении не реже 1 раза в час, если в помещении постоянно работает обслуживающий персонал. Рекомендуется использовать

систему очистки и фильтрации поступающего воздуха в аппаратное помещение. Если в здании установлена система резервного электропитания, то система поддержки микроклимата в серверном помещении должны быть подключена к системе резервного электропитания. Подробнее вопросы фильтрации воздуха, воздушного охлаждения, электроснабжения в телекоммуникационных помещениях рассмотрены в руководстве «Требования и рекомендации к серверному помещению и системам».

7.2 Защита от вредных веществ

Серверное помещение должно быть защищено от пыли и вредных веществ, которые могут отрицательно воздействовать на работу оборудования и на материалы оборудования. Концентрация вредного вещества в серверном помещении не должна превышать предельно допустимую норму.

Таблица 14 - Предельно допустимая норма вредных веществ в серверном помещении

Вредное вещество	Предельно допустимая норма
Хлор	0.01 ppm (промилле)
Пыль	100 мг/м ³ / в сутки
Углеводороды	4 мг/м ³ / в сутки
Сероводород	0.05 ppm (промилле)
Оксиды азота	0.1 ppm (промилле)
Диоксид серы	0.3 ppm (промилле)

При необходимости нужно использовать систему очистки и фильтрации поступающего воздуха. Применение масляных фильтров в аппаратных не допускается.

7.3 Вибрация

Вибрация отрицательно влияет на работу активного оборудования, контакты и соединения. В диапазоне частот до 25 Гц амплитуда колебаний не должна превышать 0.1 мм.

7.4 Освещение серверного помещения

Необходимо обеспечить освещение в серверном помещении не менее 500 люкс. Уровень освещенности измеряется на высоте 1 метра от уровня пола. Электропитание освещения серверного помещения и электропитание телекоммуникационного оборудования, установленного в серверном помещении, должно подаваться от разных распределительных электрических щитов. Светильники необходимо размещать на потолке. Требуется использовать для управления освещением одним или несколькими выключателями и располагать их рядом с дверью на высоте 1.5м от уровня пола. В серверном помещении запрещается использовать устройства плавного регулирования освещения.

7.5 Электромагнитные помехи

Серверное помещение требуется разместить в стороне от источников электромагнитных помех на таком расстоянии, чтобы напряженность электрического поля в серверном помещении не превышала 3 В/м во всем спектре частот.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		67

ЗАКЛЮЧЕНИЕ

В дипломном проекте поставленные в техническом задании задачи полностью решены, создана инфокоммуникационная инфраструктура группы компаний «Металлоторг» в Центральном Федеральном округе с подробной разработкой схемы организации связи в Белгородских филиалах и с организацией транспортной инфраструктуры на базе технологии VPN. Принято проектное решение. Для реализации сетей выбрано оборудование компании Huawei, такое как: маршрутизатор главного офиса Huawei AR 3260, маршрутизатор среднего офиса Huawei AR 2220, коммутатор Huawei S5700-28P-LI-AC, VoIP шлюз Huawei U-SYS IAD 132, Платформа Quidway® CX380 Metro, которое будет размещено по улице Чичерина и улице Почтовая города Белгород. Сделан расчет нагрузок, который позволил определить количество оборудования для требуемого количества абонентов.

Для того, чтобы проанализировать структуру проектируемой сети связи в Белгородском филиале группы компаний «Металлоторг», а также организовать сеть VPN между филиалами компании, принято решение создать модель сети связи в среде моделирования 10 – Strike.

Далее было сделано технико-экономическое обоснование для Белгородского филиала, которое показало, что при количестве абонентов 2113 капитальное вложение составит 16 762 528 рублей, эксплуатационные расходы составят 5 455 163 рубля.

В целом проект носит рекомендательный характер и может быть использован при построении сетевой инфраструктуры в любой крупной компании.

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		68

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Описание филиалов компании «Металлоторг» [Электронный ресурс] / <http://www.metallotorg.ru/> - официальный сайт компании «Металлоторг» / URL: <http://www.metallotorg.ru/info/nashifiliali/> (дата обращения 25.05.2016 г.)
2. Мультисервисные сети [Электронный ресурс] / <http://compress.ru/article.aspx?id=9404> / (дата обращения 25.05.2016 г.)
3. Что такое VPN [Электронный ресурс] / <https://technet.microsoft.com/ru-ru> - официальный сайт компании TechNet / URL: [https://technet.microsoft.com/ru-ru/library/cc731954\(v=ws.10\).aspx](https://technet.microsoft.com/ru-ru/library/cc731954(v=ws.10).aspx) (дата обращения 27.05.2016 г.)
4. Девицына С.Н., Методические рекомендации по расчету нагрузок [Текст] / С.Н. Девицына - Белгород, 2014
5. Технические характеристики маршрутизатора Huawei AR3260 [Электронный ресурс] / <http://www.huawei.com/ru/> - официальный сайт компании Huawei / Режим доступа: http://www.huawei.com/Eugene/Downloads/Eureca_Huawei%20AR%20G3%20Series%20Enterprise%20Router%20Datasheet_Rus--20130222--view%20low.pdf (дата обращения 30.05.2016 г.)
6. Технические характеристики маршрутизатора Huawei AR2220 [Электронный ресурс] / <http://www.huawei.com/ru/> - официальный сайт компании Huawei / Режим доступа: http://www.huawei.com/Eugene/Downloads/Eureca_Huawei%20AR%20G3%20Series%20Enterprise%20Router%20Datasheet_Rus--20130222--view%20low.pdf (дата обращения 31.05.2016 г.)
7. Технические характеристики коммутатора S5700-28P-LI-AC [Электронный ресурс] / <http://www.dagc.ru> - официальный сайт компании dagc / URL: http://www.dagc.ru/wp-content/uploads/2013/11/Huawei-S5700-LI-Series-Gigabit-Enterprise-Switches-Datasheet_Rus-20130216-view-low.pdf (дата обращения 2.06.2016 г.)

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		69

8. Технические характеристики платформы Quidway® CX380 Metro [Электронный ресурс] / <http://www.expertmark.net/> - официальный сайт компании Expert Mark / URL: <http://www.expertmark.net/index.php/2010-12-08-08-22-24/-huawei/2010-12-08-09-54-36/quidway-cx380> (дата обращения 4.06.2016 г.)

9. Технические характеристики VoIP шлюза Huawei U-SYS IAD 132 [Электронный ресурс] / <http://www.huawei.com/ru/> - официальный сайт компании Huawei / URL: [http://www.huawei.com/ru/products/data-communication /ne-routers/index.htm](http://www.huawei.com/ru/products/data-communication/ne-routers/index.htm) (дата обращения 8.06.2016 г.)

10. Прайс на продукцию источник бесперебойного питания UPS General Electric GT 6000 (UPS & Battery Module are separately packed) [Электронный ресурс] / [http://ziteks.ru/catalog/26898?utm_source=merchant&utm_medium=src&utm_term=%D0%98%D0%91%D0%9F_UPS_General_Electric_GT_6000__\(UPS_&_Battery_Module_are_separately_packed\)&utm_campaign=tovary&gclid=CLvOr7r3p80CFaPDcsgodLwIAqQ](http://ziteks.ru/catalog/26898?utm_source=merchant&utm_medium=src&utm_term=%D0%98%D0%91%D0%9F_UPS_General_Electric_GT_6000__(UPS_&_Battery_Module_are_separately_packed)&utm_campaign=tovary&gclid=CLvOr7r3p80CFaPDcsgodLwIAqQ) (дата обращения 12.06.2016 г.)

11. Прайс на продукцию ОКК-10-0,22-4П (3,5 кН) [Электронный ресурс] / Режим доступа: <http://velcom-s.ru/products/950/4520/> (дата обращения 13.06.2016 г.)

12. Прайс на продукцию Кабель UTP cat 5e [Электронный ресурс] / Режим доступа: <https://5element48.ru/catalog/kabelno-provodnikovaya-produktsiya/vitaya-paga-utp-ftp/57477/?gclid=CNyXvLOAqM0CFYXbcgodMfwJDQ> (дата обращения 14.06.2016 г.)

13. Прайс на продукцию Муфта кабельная 1КВТпО 1x300-400 [Электронный ресурс] / Режим доступа: http://www.elektromaster.ru/price/price_tf.htm (дата обращения 16.06.2016 г.)

14. Прайс на продукцию Wi-Fi роутер TP-LINK TL-WR940N [Электронный ресурс] / Режим доступа: <http://www.eldorado.ru/cat/detail/71151881/?category=1831494> (дата обращения 16.06.2016)

15. Прайс на продукцию двухволоконный модуль, SFP 1000BaseLX [Электронный ресурс] / Режим доступа: <http://shop.nag.ru/catalog/02086.Moduli->

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		70

SFP/06897.Dvuhvolokonnye/00537.SNR-SFP-LX-20 (дата обращения 17.06.2016 г.)

16. Прайс на продукцию маршрутизатор Huawei AR3260 [Электронный ресурс] / Режим доступа: <https://www.srv-trade.ru/catalog/1076965559/AR0M0036SA00/?r1=yandext&r2=> (дата обращения 17.06.2016 г.)

17. Прайс на продукцию маршрутизатор Huawei AR2220 [Электронный ресурс] / Режим доступа: <http://www.insotel.ru/model.php?id=26328> (дата обращения 17.06.2016 г.)

18. Прайс на продукцию коммутатор Huawei S5700-28P-LI-AC [Электронный ресурс] / Режим доступа: https://www.softmagazin.ru/hard/kommutatory/kommutatory_huawei/upravlyaemye_3_go_urovnya_huawei/S5700-28P-LI-AC (дата обращения 20.06.2016 г.)

19. Болдышев, А.В. Методические рекомендации по выполнению технико-экономического обоснования выпускных квалификационных работ [Текст] / А.В. Болдышев – Белгород, 2013

					11070006.11.03.02.116.ПЗВКР	Лист
Изм.	Лист	№ докум	Подпись	Дата		71