

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 МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ  
КОМПАНИИ «ГУЛЛИВЕР» Г. НОВОСИБИРСК**

Выпускная квалификационная работа  
обучающегося по направлению подготовки 11.03.02 Инфокоммуникационные  
технологии и системы связи  
очной формы обучения, группы 07001411  
Цветкова Александра Сергеевича

Научный руководитель  
Старший преподаватель кафедры  
Информационно-  
телекоммуникационных  
систем и технологий  
НИУ «БелГУ» Пеньков Е.П.

Рецензент  
Ведущий инженер участка  
коммутации №1 Белгородского  
филиала ПАО Ростелеком  
Уманец С.В.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
**БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ  
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ**  
(НИУ «БелГУ»)

ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХ НАУК  
КАФЕДРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ  
Направление 11.03.02 Инфокоммуникационные технологии и системы связи  
Профиль «Эксплуатация технических средств инфокоммуникационных систем»

Утверждаю  
Зав. кафедрой

« \_\_\_\_ » \_\_\_\_\_ 201\_ г.

## **ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ**

Цветкова Александра Сергеевича  
(фамилия, имя, отчество)

1. Тема ВКР «Проектирование мультисервисной сети связи компании «Гулливвер» в г. Новосибирск»

Утверждена приказом по университету от « \_\_\_\_ » \_\_\_\_\_ 201\_ г. № \_\_\_\_\_

2. Срок сдачи студентом законченной работы \_\_\_\_ . \_\_\_\_\_

3. Исходные данные:

объект проектирования – офисные здания компании Гулливер г. Новосибирск  
тип сети связи – проводная мультисервисная сеть связи;

4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов):

- 4.1. Экспликация объекта проектирования
- 4.2. Особенности построения сетей для распределенных филиалов
- 4.3. Разработка корпоративной сети организации
- 4.4. Расчёт характеристик пропускной способности мультисервисных пакетных сетей
- 4.5. Расчёт стоимости внедрения и годовой эксплуатации корпоративной сети
- 4.6. Охрана труда, техника безопасности и экологическая безопасность проекта

5. Перечень графического материала (с точным указанием обязательных чертежей):

- 5.1. Экспликация объекта компания «Гулливвер» (А1, лист 1);
- 5.3. Проектируемая схема организации структурированной кабельной системы для офиса компании «Гулливвер» (А1, лист 1);
- 5.4. Проектируемая схема организации мультисервисной сети связи для компании «Гулливвер» (А1, лист 1);
- 5.5. Технико-экономические показатели проекта (А1, лист 1);

6. Консультанты по работе с указанием относящихся к ним разделов

Раздел	Консультант	Подпись, дата	
		Задание выдал	Задание принял
4.1. – 4.4, 4.6	<i>старший преподаватель кафедры ИТСиТ Пеньков Е.П.</i>		
4.5	<i>канд. техн. наук, доцент кафедры ИТСиТ Болдышев А.В.</i>		

7. Дата выдачи задания \_\_\_\_\_

**Руководитель**

*Старший преподаватель  
кафедры Информационно-телекоммуникационных  
систем и технологий»  
НИУ «БелГУ»*

*Е.П. Пеньков*

\_\_\_\_\_  
(подпись)

Задание принял к исполнению \_\_\_\_\_  
(подпись)

## СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1 ЭКСПЛИКАЦИЯ ОБЪЕКТА ПРОЕКТИРОВАНИЯ	5
1.1 Анализ структуры организации	5
1.2 Концепции реализации корпоративной сети	8
2 ОСОБЕННОСТИ ПОСТРОЕНИЯ СЕТЕЙ ДЛЯ РАСПРЕДЕЛЕННЫХ ФИЛИАЛОВ	11
2.1 Особенности проектирования распределенных сетей VPN	11
2.2 Концепция Cisco Easy VPN	15
2.3 Компоненты VPN сети	17
3 РАЗРАБОТКА КОРПОРАТИВНОЙ СЕТИ ОРГАНИЗАЦИИ	20
3.1 Организации сети через VPN/MPLS сеть	20
3.2 Адресное пространство VPN сети	23
3.3 Выбор сетевого оборудования	25
3.3.1 Пограничный маршрутизатор сети	26
3.3.2 Выбор коммутаторов третьего уровня	27
3.3.3 Выбор абонентского оборудования	29
3.4 Организация VPN сети для компании Гулливер	31
4 РАСЧЕТ ХАРАКТЕРИСТИК ПРОПУСКНОЙ СПОСОБНОСТИ МУЛЬТИСЕРВИСНЫХ ПАКЕТНЫХ СЕТЕЙ	34
5 РАСЧЁТ СТОИМОСТИ ВНЕДРЕНИЯ И ГОДОВОЙ ЭКСПЛУАТАЦИИ КОРПОРАТИВНОЙ СЕТИ НА БАЗЕ FTTO	39
5.1 Расчёт затрат на внедрение	39
5.2 Расчет стоимости годовой эксплуатации сети	41
6 ОХРАНА ТРУДА, ТЕХНИКА БЕЗОПАСНОСТИ И ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРОЕКТА	47
ЗАКЛЮЧЕНИЕ	49
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	50

					<i>11070006.11.03.02.321.ПЗВКР</i>			
Изм.	Лист	№ докум.	Подпись	Дата				
Разработал		Цветков А.С.			Проектирование мультисервисной сети связи компании «Гулливер» в г. Новосибирск	Лит.	Лист	Листов
Проверил		Пеньков Е.П.					2	52
Рецензент		Уманец С.В.				<i>НИУ «БелГУ» гр. 07001411</i>		
Н. Контроль		Пеньков Е.П.						
Утвердил		Жиляков Е.Г.						

## ВВЕДЕНИЕ

Появление мультисервисных сетей оказывает решающее влияние на развитие индустрии телекоммуникаций и передачи данных. Доставка по единой сетевой инфраструктуре, базирующейся на коммутации пакетов или ячеек, такого разнородного трафика, как данные, голос и видео, является перспективным решением для корпораций и сервис-провайдеров. Исторически корпоративные сети передачи данных, голоса и видео строились независимо, базировались на разных инфраструктурах и технологиях. Обычно в качестве каналов связи использовались выделенные линии, а технологиями передачи данных служили Frame Relay и АТМ. Очевидно, что эксплуатация и сопровождение разнородных структур весьма неэффективны, в большей мере нуждам бизнеса соответствуют сети следующего поколения, имеющие возможность передавать все типы пользовательских трафиков на базе сетей с коммутацией пакетов (ячеек), таких, как Frame Relay, АТМ или IP.

Современные телекоммуникационные сети используют технологию коммутации каналов и TDM (Time Division Multiplexing) в качестве схемы мультиплексирования. Они проектировались для передачи голосовых потоков и не могут эффективно поддерживать нерегулярный трафик данных. В то же время сегодня темпы роста трафика данных несоизмеримо выше голосового, и операторы столкнулись с проблемой замены неэффективной TDM-инфраструктуры с сохранением необходимого качества передачи голоса, решением которой стала постепенная замена TDM-сетей с коммутацией каналов на инфраструктуру пакетных сетей.

Для создания корпоративной территориально распределенной коммуникационной инфраструктуры необходима современная технологическая сеть предприятия, предназначенная для трансляции разнородных видов трафика - данных, IP-телефонии, видео, сигналов телеметрии и телеуправления. Требования по пропускной способности каналов передачи данных и

						Лист
					<b>11070006.11.03.02.321.ПЗВКР</b>	3
Изм.	Лист	№ докум.	Подпись	Дата		

возможности предоставления услуг с необходимым уровнем качества обслуживания QoS (Quality of Service) являются наиболее важными в такой сети.

Выбор физической среды передачи данных во многом определяет функциональные возможности всей корпоративной сети предприятия. Для создания масштабируемой, надежной сети необходимо произвести анализ существующих вариантов реализации сетей, а так же оценить перспективные пути развития и заложить во вновь создаваемую структуру сети пути для ее модернизации.

Волоконно-оптическая линия связи на сегодняшний день стала практически единственной средой передачи данных, отвечающей всем требованиям, предъявляемым к современным вычислительным сетям. Возросшие скорости передачи, объемы данных, количество интегрируемых услуг, транспортом для которых стала волоконно-оптическая сеть, все это в совокупности с надежностью, отказоустойчивостью снижением стоимости реализации самой волоконно-оптической сети диктует очевидный вариант организации КИС с использованием волоконно-оптической средой передачи данных.

Целью выпускной квалификационной работы является предоставление гибкой сетевой инфраструктуры для безопасной и быстрой передачи разнородного трафика для компании «Гуливер» в г. Новосибирск. Для достижения поставленной цели необходимо решить следующие задачи:

- Провести анализ структуры организации;
- Сформировать требования к проектируемой сети связи;
- Выработать стратегию модернизации сетевой инфраструктуры;
- Осуществить выбор телекоммуникационного оборудования и кабелей в соответствии с выбранной стратегией модернизации сети;
- Составить технико-экономическое обоснование принятых решений;
- Разработать рекомендации по внедрению разработанного проекта.

						Лист
					<b>11070006.11.03.02.321.ПЗВКР</b>	4
Изм.	Лист	№ докум.	Подпись	Дата		

# 1 ЭКСПЛИКАЦИЯ ОБЪЕКТА ПРОЕКТИРОВАНИЯ

## 1.1 Анализ структуры организации

Компания «Гуливер» г. Новосибирск представляет собой сеть из центрального офиса и пяти филиалов. Филиалами являются точки турагенства для работы с клиентами (так же Call-центры). Центральный офис занимается оформлением путёвок для клиентов.

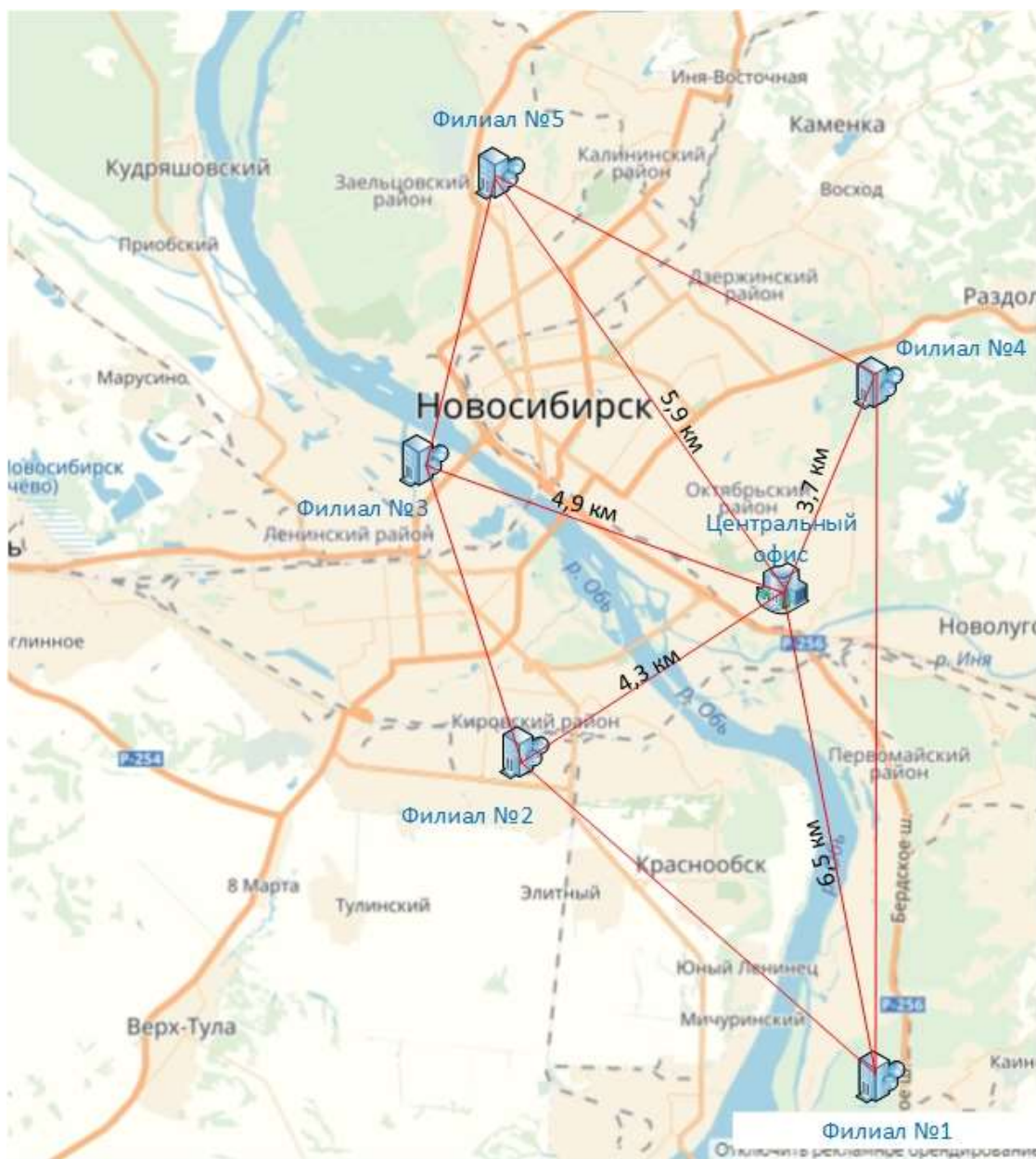


Рисунок 1.1 – Расположение филиалов компании Гуливер на карте г. Новосибирска

Филиалы распределены по районам города. Все структурные подразделения логически связаны в одну корпоративную информационную систему. Каждый филиал имеет собственную базу данных и ряд специальных программных продуктов для работы.

В виду того что филиалы расположены на большом расстоянии от центрального офиса компании, было решено купить у провайдера «Ростелеком» отдельные узлы VPN-сети, т.к. прокладывать оптоволокно от филиалов до центрального офиса (и между ними) слишком дорого.

В таблице 1.1 сводные данные о количестве служащих компании, а также минимальные числа запланированных точек подключения по технологии FTTO.

**Таблица 1.1 - Сводные данные организации**

Филиал	Число служащих	Количество абонентских портов
1 Филиал (Советский р-н)	60	50
2 Филиал (Кировский р-н)	45	35
3 Филиал (Ленинский р-н)	55	50
4 Филиал (Дзержинский р-н)	48	36
5 Филиал (Заельцовский р-н)	50	40
Центральный офис (Октябрьский р-н)	100	120
<b>ИТОГО</b>	<b>338</b>	<b>331</b>

Fiber to office (FTTO) является альтернативной концепцией кабельных сетей для построения локальной сети (LAN). Технология сочетает в себе пассивные элементы (волоконно-оптические кабели, коммутационные панели, соединительные коробки, разъемы и стандартные медные 8P8C патч-корды) и активные мини-коммутаторы (называемые переключателями FTTO) для обеспечения конечных устройств с помощью Gigabit Ethernet. FTTO включает в себя централизованные технологии волоконно-оптических кабелей для создания комбинированного магистрального / горизонтального канала; этот канал предоставляется от рабочих зон до централизованного кросс-соединения или



межсоединения, позволяя использовать сквозные кабели или сращивания в телекоммуникационной комнате.

В настоящее время в каждом филиале используются локальные вычислительные сети построенные по технологии Fast Ethernet. Если рассматривать существующую сетевую архитектуру, то она представляет собой совокупность разрозненных сетей масштаба одной инспекции. Взаимодействие инспекций осуществляется посредством сети Internet (корпоративный сайт, корпоративный почтовый сервер), с использованием ADSL канала шириной 216 Кбит/с .

Существующая организация сети не отвечает современным требованиям безопасности IP трафика, также не считается возможным создание видеоконференций, работы в WEB приложениях, снижена общая производительность корпоративной сети.

Необходимо разработать вариант корпоративной информационной сети, отвечающей следующим требованиям:

- безопасность и конфиденциальность трафика;
- возможность легкой масштабируемости сети;
- объединение разнородного трафика;
- обеспечение высокой скорости передачи данных.

Следовательно требуется разработать план модернизации сети для компании Гуливер в г. Новосибирск.

						Лист
						7
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.321.ПЗВКР</b>	

## 1.2 Концепции реализации корпоративной сети

Существуют две концепции предоставления доступа согласно концепции FTTO: 1) Концепция с использованием медножильного кабеля и активного оборудования передачи на горизонтальном уровне структурированной кабельной системы – рисунок 1.2; 2) Концепция оптической распределительной сети на горизонтальном уровне структурированной кабельной системы – рисунок 1.3.

Среди преимуществ такого подхода к организации связи следует отметить следующие:

Из-за характеристик передачи сигнала волокна и устойчивости к электромагнитным помехам (ЕМП) сигналы могут передаваться на расстояния более 100 м (100 м - это ограничение канала в традиционных структурированных кабельных сетях).

Многомодовые волоконные кабели охватывают расстояния до 550 м и одномодовые до 10 км для Gigabit Ethernet и дальше. Это идеальное решение для крупных пространственно распределенных объектов, обычно находящихся в государственной администрации, университетах, больницах, аэропортах, торговых центрах и военных.

FTTO характеризуется отсутствием сетевой иерархии, которая может упростить развертывание и управление установкой.

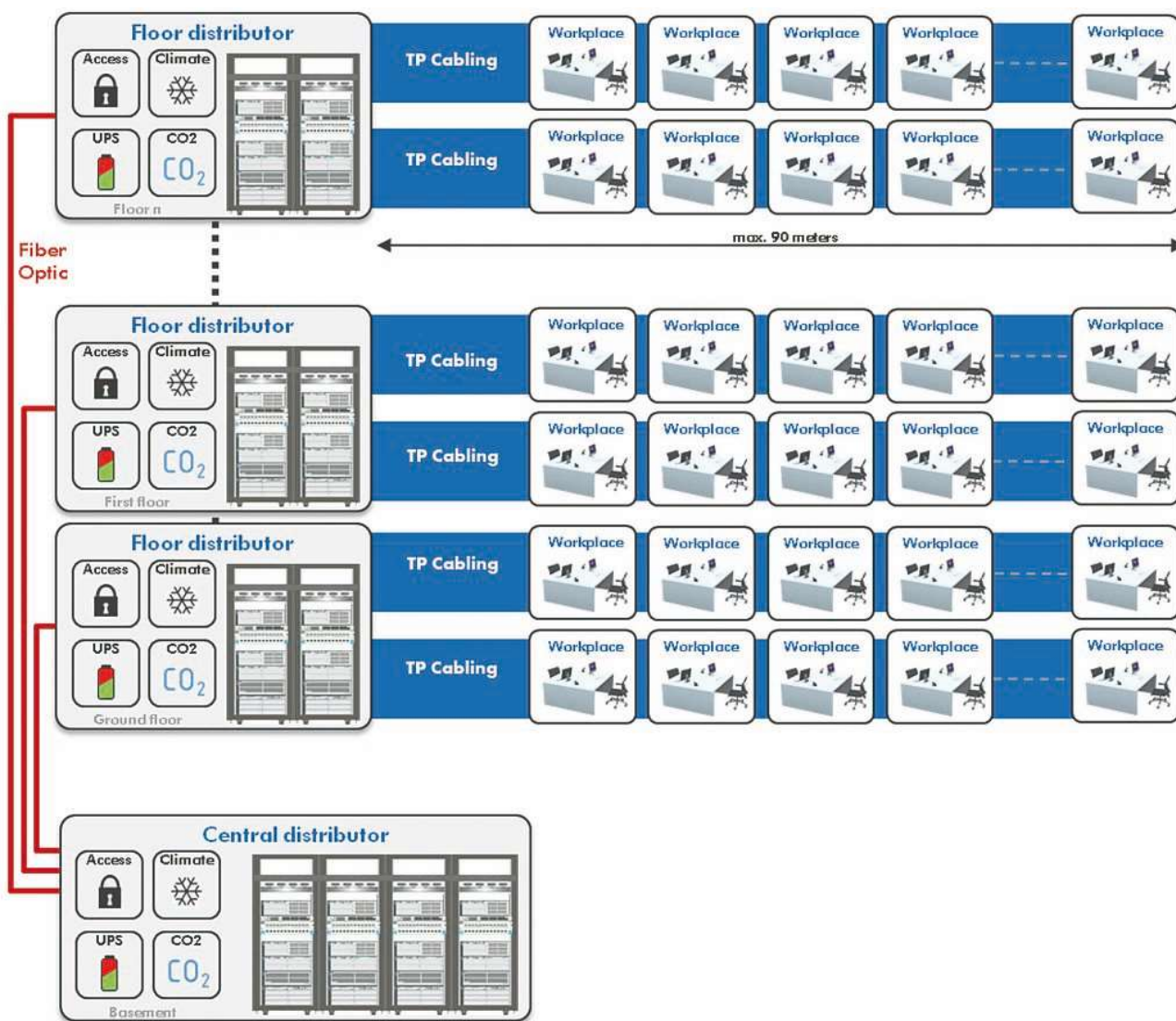
В некоторых конструкциях FTTO нет необходимости в горизонтальных распределителях (рисунок 1.3), а инвестиции которые могли бы быть потрачены на оборудование для охлаждения, электропитание и безопасность можно сохранить для других целей.

Для волоконных инфраструктур требуется меньше кабелей, чем традиционные медные витые пары. Как правило, одна оптоволоконная линия заменяет четыре витых пары кабелей без потери пропускной способности. Это делает концепции избыточного резервирования финансово осуществимыми. Кроме того оптоволоконные кабельные системы не знают проблем с

						Лист
					<b>11070006.11.03.02.321.ПЗВКР</b>	8
Изм.	Лист	№ докум.	Подпись	Дата		

заземлением. Оптическое волокно - очень безопасная среда. Нет проблем с изношенной или поврежденной изоляцией, неправильной или недостаточной защитой цепи, короткого замыкания и перенапряжения.

Пожарная безопасность волоконно-оптических кабелей чрезвычайно высокая, что хорошо для исторических зданий с особыми потребностями в области противопожарной защиты и безопасности.



**Рисунок 1.2 – Концепция СКС FTTO с использованием медножильного кабеля**

Горизонтальное распределительное оборудование может размещаться в помещениях с другим техническим оборудованием (размеры помещения при этом должны составлять 6-18 м<sup>2</sup>). Еще одним преимуществом инфраструктур FTTO является их гибкость. Новые пользователи, службы или приложения могут

быть легко добавлены в сеть. Кроме того, сетевые настройки, обновления и физические изменения легко интегрируются в существующую сеть без приостановки работы. Также, развертывание FTTO сети может быть реализовано на в среднем на 60% быстрее, чем их традиционные аналоги. Исследования показывают, что использование переключателей с поддержкой EEE позволяет сэкономить до 70% потребляемой мощности по сравнению с традиционными сетями не EEE (Energy Efficient Ethernet). Кроме того, большинство передовых инфраструктур FTTO помогают сэкономить до 40% совокупной стоимости владения.

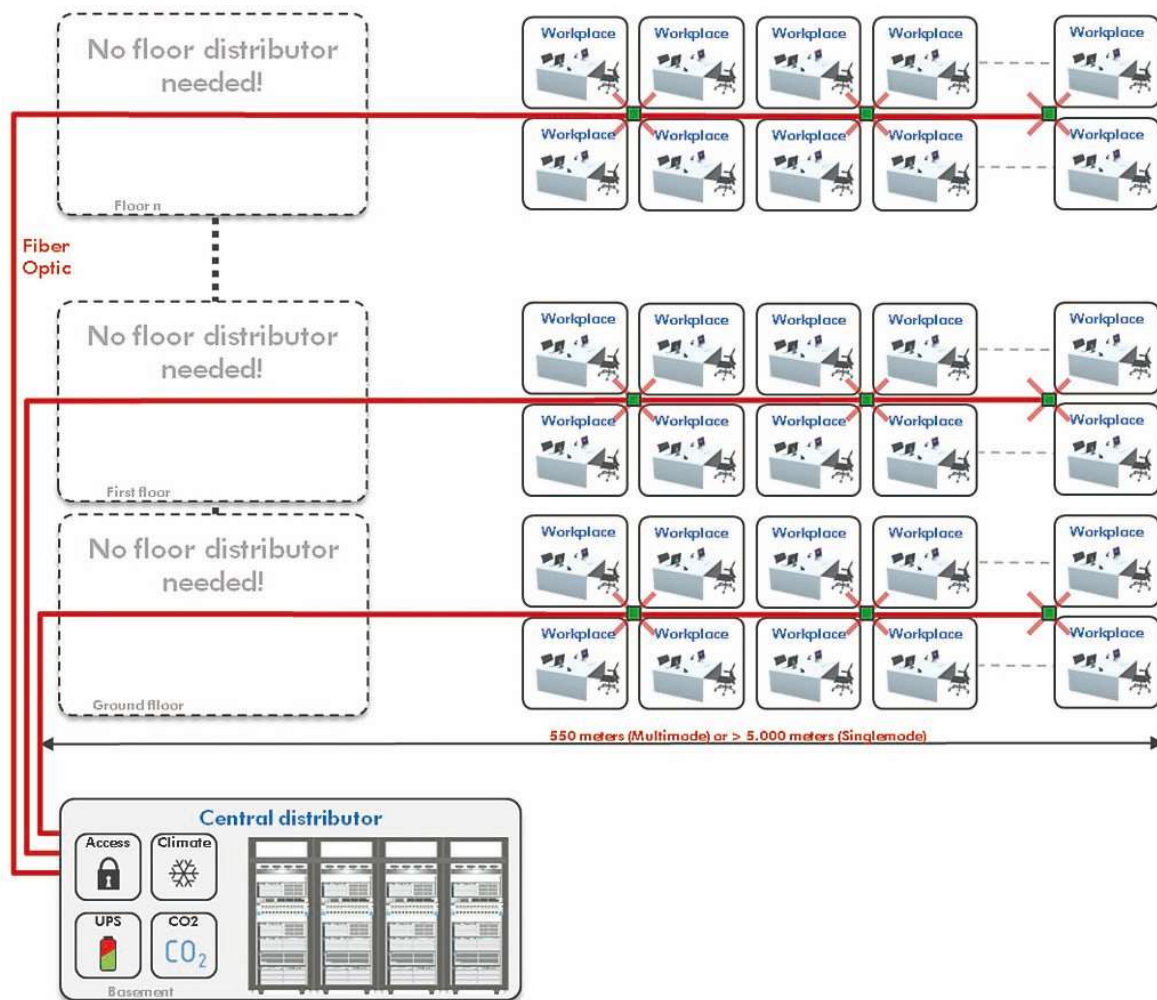


Рисунок 1.3 – Концепция СКС FTTO с использованием оптического кабеля

## 2 ОСОБЕННОСТИ ПОСТРОЕНИЯ СЕТЕЙ ДЛЯ РАСПРЕДЕЛЕННЫХ ФИЛИАЛОВ

### 2.1 Особенности проектирования распределенных сетей VPN

VPN - это зашифрованное соединение между частными сетями через сеть общего доступа, например Интернет. V значит Virtual (виртуальная), N - Network (сеть). Данные частной сети безопасно передаются через сеть общего доступа (Интернет), формируя виртуальный канал. Концептуальная схема VPN сети представлена на рисунке 2.1.



Рисунок 2.1 – Концептуальная схема VPN сети

Буква P обозначает Private. Для сохранения конфиденциальности трафик шифруется. Вместо выделенной линии второго уровня VPN использует виртуальные подключения, которые маршрутизируются из частной сети компании к удаленной площадке или хосту служащего компании.

Преимущества VPN приводятся ниже:

Сокращение затрат: VPN позволяет организациям использовать экономичный сторонний транспорт - сеть Интернет - для подключения удаленных офисов и пользователей к главной корпоративной площадке и устраняет потребность в дорогих выделенных каналах РВС и модемных пулах.

Более того, с появлением экономичных технологий широкополосного доступа, таких как DSL, организации могут использовать VPN для снижения затрат на связь и повышения полосы пропускания удаленных подключений.

**Безопасность:** VPN обеспечивают самый высокий уровень безопасности благодаря передовым протоколам шифрования и аутентификации, которые защищают данные от несанкционированного доступа.

**Масштабируемость:** VPN позволяют корпорациям использовать инфраструктуру и устройства поставщиков услуг Интернета, что упрощает добавление новых пользователей. Таким образом, корпорации могут значительно увеличивать полосу пропускания без наращивания инфраструктуры.

**Совместимость с технологией широкополосного доступа:** VPN позволяет мобильным работникам, удаленным работникам и людям, которые хотят продлить свой рабочий день, получить доступ к корпоративной сети, воспользовавшись широкополосным подключением, например DSL или кабельным модемом, что обеспечивает значительную гибкость и эффективность. Более этого, высокоскоростные широкополосные каналы предлагают экономичное решение для связи удаленных офисов – рисунок 2.2.



**Рисунок 2.2 – Сравнительные преимущества VPN сети над традиционной WAN сетью**

Существует два типа виртуальных частных сетей:

1. VPN для соединения площадок (site-to-site).
2. VPN удаленного доступа, которая реализуется двумя типами решений VPN: а) Cisco Easy VPN; б) Cisco IOS IPsec/SSL VPN, другое название - WebVPN.

VPN для соединения площадок (site-to-site) - расширение классической распределенной сети. Такие VPN используются для соединения полноценных сетей. Например они могут служить для подключения сети филиала к сети штаб-квартиры компании. В прошлом для связи площадок использовались арендованные каналы и каналы Frame Relay. Теперь, когда у большинства компаний есть доступ в Интернет, эти каналы можно заменить на site-to-site VPN, что проиллюстрировано на рисунке 2.3.



**Рисунок 2.3 – VPN для расширения площадок (соединение филиалов) как расширение классической WAN сети**

В site-to-site VPN хосты не используют ПО Cisco VPN Client, они отправляют и принимают обычный трафик TCP/IP через «шлюз» VPN. В качестве шлюза может использоваться маршрутизатор, брандмауэр, VPN-концентратор Cisco и адаптивное устройство безопасности Cisco ASA 5500. Шлюз VPN выполняет инкапсуляцию и шифрование всего исходящего трафика площадки и отправляет его через туннель VPN в сети Интернет в аналогичный

шлюз VPN на площадке назначения. При получении трафика шлюз VPN отделяет заголовки, расшифровывает контент и передает пакеты узлу назначения внутри частной сети.

Удаленный доступ представляет собой усовершенствование сетей с коммутацией каналов, таких как аналоговая телефонная линия или ISDN. VPN удаленного доступа предназначены для удаленных работников, мобильных пользователей и обмена данными между потребителем и организацией. VPN удаленного доступа обеспечивают безопасное подключение отдельных хостов к корпоративной сети через Интернет.

В прошлом корпорации работали с удаленными пользователями с помощью коммутируемого доступа через телефонную сеть и ISDN. С появлением VPN мобильные пользователи нуждаются только в доступе в Интернет для подключения к центральному офису. Удаленные работники, как правило, используют широкополосное соединение, DSL или кабельный модем для доступа в Интернет.

В VPN удаленного доступа (рисунок 2.4) каждый хост работает под управлением ПО Cisco VPN Client. Каждый раз, когда хост пытается передать трафик, ПО Cisco VPN Client инкапсулирует и шифрует его перед отправкой через Интернет в шлюз VPN на периферии сети назначения. При получении трафика шлюз VPN выполняет те же действия, что аналогичный шлюз в site-to-site VPN.



**Рисунок 2.4 – VPN удаленного доступа как развитие сетей коммутируемого доступа и сетей с интеграцией обслуживания**



## 2.2 Концепция Cisco Easy VPN

При внедрении VPN для удаленных работников и малых офисов, простота развертывания крайне важна. Решение Cisco Easy VPN (рисунок 2.5) упрощает развертывание VPN в сетях малых, средних и крупных предприятий, содержащих продукты Cisco. Cisco Easy VPN - экономичное решение, идеальное для удаленных офисов с низким уровнем ИТ-поддержки.



Рисунок 2.5 – Концепция Cisco Easy VPN

Cisco Easy VPN состоит из двух компонентов:

**Cisco Easy VPN Server:** в качестве сервера может служить специализированный шлюз VPN, например VPN-концентратор Cisco, брандмауэр Cisco PIX, адаптивное устройство безопасности Cisco ASA или маршрутизатор Cisco IOS. Шлюз VPN, использующий ПО Cisco Easy VPN Server, может терминировать туннели VPN, инициированные мобильными и удаленными пользователями с компьютерами под управлением ПО Cisco VPN Client. Кроме того, шлюз VPN может терминировать туннели VPN от удаленных устройств, работающих в качестве узлов Cisco Easy VPN Remote в сети site-to-site VPN.

**Cisco Easy VPN Remote:** Cisco Easy VPN Remote позволяет маршрутизаторам Cisco IOS, брандмауэрам PIX, адаптивным устройствам безопасности Cisco ASA и аппаратным клиентам Cisco VPN получать политики от Cisco Easy VPN Server. Это сводит к минимуму требования к настройке VPN на удаленном объекте. Cisco Easy VPN обеспечивает принудительную передачу таких параметров VPN, как внутренние IP-адреса, внутренние маски подсети, адреса DHCP-серверов, адреса WINS-серверов и флаги разделения туннелей (split-tunneling), с Cisco Easy VPN Server на удаленные устройства

#### **Преимущества Cisco Easy VPN:**

- Централизованное хранение конфигураций обеспечивает динамическую настройку политик конечных пользователей и снижает потребность в ручной настройке.
- Локальная конфигурация VPN не зависит от IP-адреса удаленного узла. Эта функция позволяет поставщику услуг изменять конфигурацию оборудования и сети с минимальной перенастройкой оборудования конечных пользователей или вообще без нее.
- Cisco Easy VPN обеспечивает централизованное управление политиками безопасности.
- Cisco Easy VPN обеспечивает развертывание в больших масштабах с быстрым добавлением пользователей.
- Cisco Easy VPN не требует установки и настройки ПО Cisco Easy VPN Remote конечными пользователями.

#### **Ограничения Easy VPN**

Для решения Cisco Easy VPN характерны следующие ограничения:

- Ручная настройка преобразования NAT и PAT не допускается: Cisco Easy VPN Remote автоматически создает необходимые конфигурации NAT и PAT для туннеля VPN.
- Поддерживается только один узел назначения: 1) Cisco Easy VPN Remote поддерживает конфигурации только с одним узлом назначения и

						Лист
					<b>11070006.11.03.02.321.ПЗВКР</b>	16
Изм.	Лист	№ докум.	Подпись	Дата		

туннельным подключением; 2) Если приложение требует создания нескольких туннелей VPN, необходимо вручную настроить параметры IPsec VPN, NAT и PAT на сервере и удаленном клиенте.

- Cisco Easy VPN требует серверов назначения: Для работы Cisco Easy VPN Remote необходимо, чтобы узел назначения был сервером удаленного доступа Cisco Easy VPN.

- Цифровые сертификаты не поддерживаются: 1) Поддерживается аутентификация на основе предварительных общих ключей (PSK); 2) Расширенную аутентификацию (XAUTH) можно использовать в дополнение к PSK для обеспечения аутентификации на уровне пользователей в дополнение к аутентификации на уровне устройств.

- На серверах IPsec поддерживается только группа политик 2 протокола ISAKMP: Cisco VPN Client и Cisco VPN Server поддерживает политики ISAKMP, использующие согласование группы 2 (1024-битный алгоритм Диффи-Хеллмана [DH]).

- Некоторые наборы преобразований не поддерживаются: 1) Функция Cisco Easy VPN Remote не поддерживает наборы преобразований, обеспечивающие шифрование без аутентификации (ESP-DES и ESP-3DES) и наборы преобразований, обеспечивающих аутентификацию без шифрования (ESP-NUL, ESP-SHA-HMAC и ESP-NUL ESP-MD5-HMAC); 2) Cisco VPN Client и Cisco VPN Server не поддерживают протокол AH, но поддерживают протокол ESP.

### 2.3 Компоненты VPN сети

Компания Cisco предлагает семейство маршрутизаторов, оптимизированных для VPN. ПО Cisco IOS, работающее на маршрутизаторах Cisco, объединяет многофункциональные службы VPN и ведущую в отрасли

						Лист
					<b>11070006.11.03.02.321.ПЗВКР</b>	17
Изм.	Лист	№ докум.	Подпись	Дата		

маршрутизацию в единое комплексное решение. ПО Cisco VPN обеспечивает высокий уровень безопасности за счет шифрования и аутентификации. Маршрутизаторы с поддержкой Cisco VPN поддерживают высокую производительность решений VPN для интрасетей, экстрасетей и site-to-site.



**Рисунок 2.6 – Концепция построения VPN на базе маршрутизаторов Cisco**

Адаптивные устройства безопасности Cisco ASA 5500 предлагают гибкие технологии для создания специализированных решений, удовлетворяющих различным требованиям к удаленному доступу и связи площадок site-to-site. Адаптивные устройства безопасности ASA 5500 предоставляют простой в управлении удаленный доступ через IPsec и связь площадок через VPN, учитывающей особенности сети. Это позволяет организациям создавать безопасные подключения для мобильных пользователей, удаленных площадок и бизнес-партнеров.

ASA 5500 предлагает функции IPsec и SSL VPN на одной платформе, устраняя потребность в параллельных решениях. Помимо служб VPN ASA 5500 предлагает брандмауэр для анализа приложений и службы предотвращения вторжений.

Службы безопасности IPsec выполняют 4 важные функции.

**Конфиденциальность (шифрование):** Отправитель шифрует пакеты перед тем, как передать их через сеть. Это предотвращает возможность перехвата сообщений. Если сообщение перехвачено, злоумышленник не сможет прочитать его.

**Целостность данных:** Получатель может проверить, были ли данные изменены во время передачи через Интернет. IPsec гарантирует целостность данных с помощью контрольных сумм, простой проверки по избыточности.

**Аутентификация:** Аутентификация гарантирует, что соединение установлено с нужным партнером. Получатель может аутентифицировать источник пакета, гарантируя и сертифицируя подлинность источника информации.

**Защита от повтора пакетов:** Защита от повтора гарантирует, что каждый пакет уникален и не дублируется. Защита пакетов IPsec обеспечивается за счет сравнения номеров последовательности полученных пакетов со скользящим окном хоста назначения или шлюза безопасности. Пакет с номером последовательности ниже скользящего окна считается запоздавшим или дублированным. Запоздавшие и дублированные пакеты отбрасываются.

						Лист
						19
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.321.ПЗВКР</b>	

### 3 РАЗРАБОТКА КОРПОРАТИВНОЙ СЕТИ ОРГАНИЗАЦИИ

Проектирование компьютерной сетей является сложной задачей. Для облегчения решения эту задачу принято разбивать на части. В соответствии с предложенным фирмой Cisco Systems подходом компьютерные сети удобно представлять в виде модели, которая включает в себя три уровня иерархии:

- 1) Уровень ядра;
- 2) Уровень распределения;
- 3) Уровень доступа.

Уровень ядра (core) отвечает за высокоскоростную передачу сетевого трафика. Первичное предназначение устройств уровня ядра - коммутация пакетов. В соответствии с указанными принципами на устройствах уровня ядра запрещается вводить различные технологии, такие, как, например, списки доступа или маршрутизация по правилам, мешающие быстрой коммутации пакетов.

На уровне распределения происходит суммирование маршрутов и агрегация трафика. Под суммированием маршрутов понимается представление нескольких сетей в виде одной большой сети с короткой маской. Это позволяет уменьшить таблицу маршрутизации в устройствах уровня ядра, а также изолировать изменения, которые происходят внутри большой сети.

Уровень доступа предназначен для формирования сетевого трафика и контроля за доступом к сети. Маршрутизаторы уровня доступа служат для подключения отдельных пользователей (серверы доступа) или отдельных локальных сетей к глобальной вычислительной сети.

#### 3.1 Организации сети через VPN/MPLS сеть

В качестве линий связи между филиалами организации в пределах города используем транспортную сеть одного из субпровайдеров. Условная схема

						Лист
						20
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.321.ПЗВКР</b>	

корпоративной сети филиалов в городе Новосибирск изображена на рисунке 2.1.

Корпоративная сеть основывается на трехуровневой иерархической модели (верхний уровень - ядро (core), средний - уровень распределения(distribution), нижний - уровень доступа (access)).

На уровне ядра располагается центральный офис компании. Он является узлом ядра глобальной корпоративной сети. Центральные маршрутизаторы узлов (соединены между собой (каждый - с каждым) по одной из технологий для глобальных вычислительных сетей, образуют кольцевое ядро сети с избыточными путями. К узловому маршрутизатору ядра подключаются маршрутизаторы филиалов.

В каждом филиале к маршрутизатору уровня распределения подключаются коммутаторы уровня доступа. В соответствии с технологией FTTH на каждом участке сети в пределах города используются оптоволоконные линии связи, вплоть до конечного пользователя.

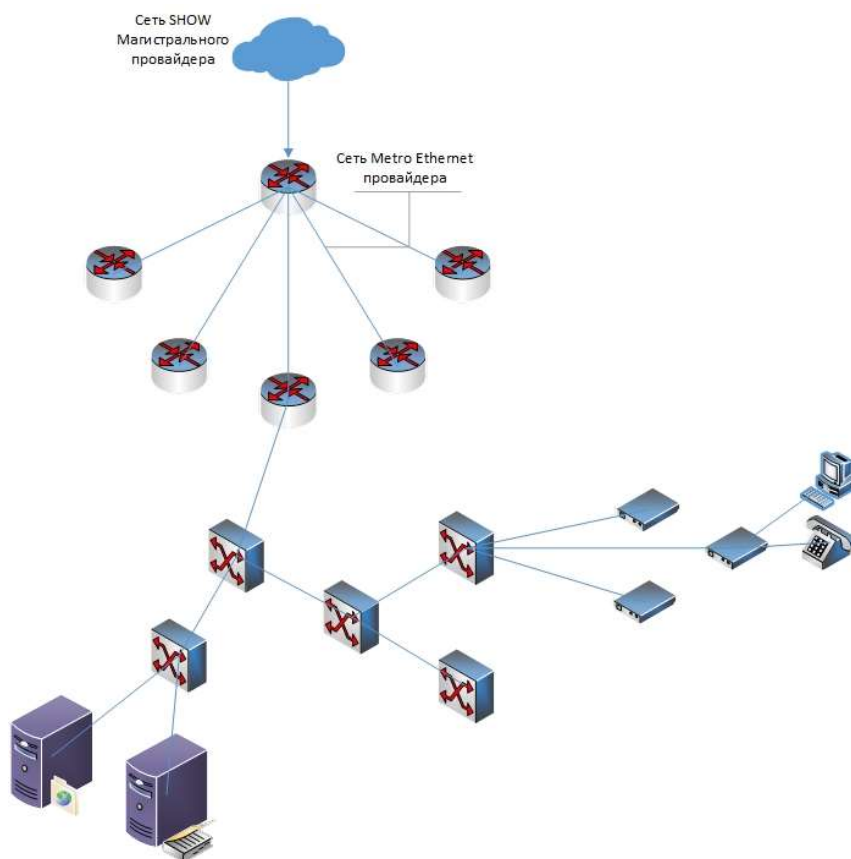


Рисунок 3.1 - Схема организации сети

Маршрутизатор уровня ядра оснащается двумя типами интерфейсов. Для объединения центрального офиса с центральными офисами других субъектов РФ используется сеть DWDM SDH магистрального провайдера.

Для объединения филиалов в пределах Новосибирска, через публичную сеть оператора будет применено построение VPN на базе MPLS.

Определены следующие понятия:

- CE - маршрутизатор со стороны узла клиента, который непосредственно подключается к маршрутизатору оператора;
- PE - граничный маршрутизатор со стороны оператора (MPLS домена), к которому подключаются устройства CE. Устройства PE выполняют функции E-LSR;
- P - маршрутизатор внутри сети оператора (MPLS домена). P устройства выполняют функции LSR.

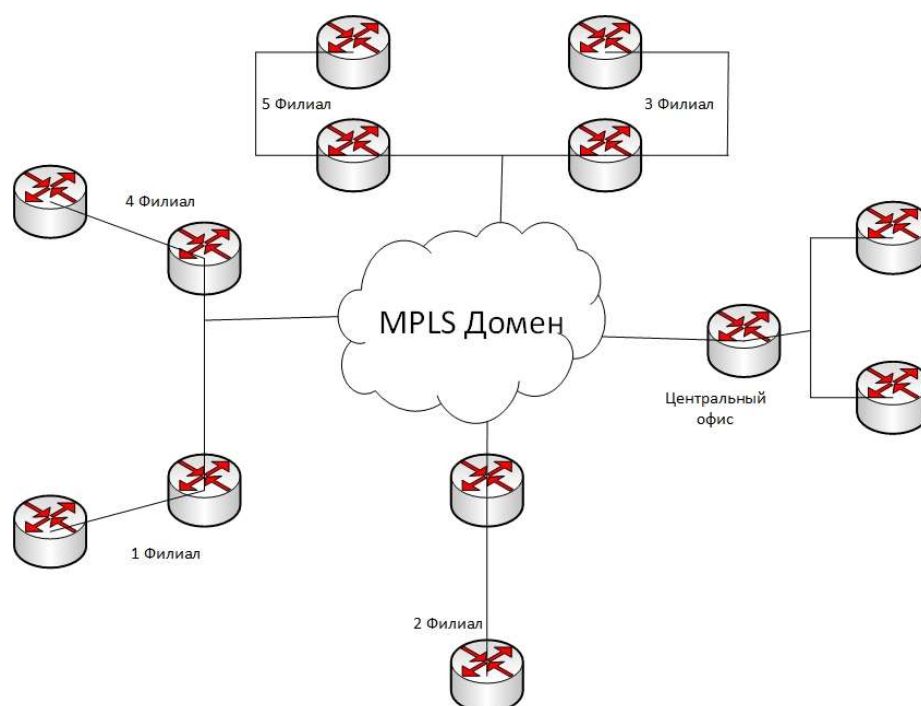
Сеть оператора использует технологию MPLS/VPN. Маршрутизаторы сети оператора образуют MPLS домен. К сети оператора подключены несколько филиалов. Каждому филиалу организован его личный VPN. Список узлов филиалов представлен в таблице 3.1, схема их подключения на рисунке 3.2. Для организации корпоративной сети провайдером транспортной сети MPLS было предложена схема реализации сети как объединение нескольких VPN. Формирование VPN сетей будут осуществляться по принципу «центр - периферия» (hub-and-spoke). Данная схема подразумевает объединение нескольких узлов, один или несколько из которых объявляется центральным, а остальные периферийными. Центральные узлы могут обмениваться IP трафиком друг с другом. Периферийные узлы могут обмениваться трафиком с центральными. Периферийные узлы не могут обмениваться трафиком друг с другом.

						Лист
					<b>11070006.11.03.02.321.ПЗВКР</b>	22
Изм.	Лист	№ докум.	Подпись	Дата		



**Таблица 3.1 - Описание распределения VPN**

Филиал	Обозначение VPN	Тип VPN
Филиал 1	VPN_1	Периферийная сеть
Филиал 2	VPN_2	Периферийная сеть
Филиал 3	VPN_3	Периферийная сеть
Филиал 4	VPN_4	Периферийная сеть
Филиал 5	VPN_5	Периферийная сеть
Центральный офис	VPN_6	Центральная сеть



**Рисунок 3.2 - Схема MPLS домена и подключенных узлов клиента**

В нашем случае центральным узлом VPN будет являться – центральный офис, периферийными VPN (spokes) – филиалы компании.

### 3.2 Адресное пространство VPN сети

Для создания адресного пространства корпоративной сети будем использовать адреса, рекомендованные провайдером для использования -

172.16.0.0 /12, при этом диапазон адресов 172.16.0.0 - 172.31.255.255. При этом для возможного расширения сети и сохранения уникальности адресного пространства разделим сети центрального офиса и филиалов на подсети, используя третий и четвертый октеты. Количество хостов выбирается с существенным запасом.

В таблице 3.2 указано разбиение всего адресного пространства. В таблице 3.3 приведена карта адресного пространства для центрального офиса.

**Таблица 3.2 - Принцип разбиения адресного пространства**

Тип адресуемого пространства	Количество адресуемых элементов	Количество хостов	Диапазон IP-адресов
Филиал 1	50		172.17.1.0 /24
Филиал 2	35		172.17.2.0 /24
Филиал 3	50		172.17.3.0 /24
Филиал 4	36		172.17.4.0 /24
Филиал 5	40		172.17.5.0 /24
Центральный офис	120	1022	172.16.0.0 /22

**Таблица 3.3 – Карта адресного пространства для центрального офиса**

Имя	Значение	16-ричный код	Бинарное значение
Адрес	172.16.0.0	AC.10.00.00	10101100.00010000.000000   00.00000000
Bitmask	22		
Netmask	255.255.252.0	FF.FF.FC.00	11111111.11111111.111111   00.00000000
Wildcard	0.0.3.255	00.00.03.FF	00000000.00000000.000000   11.11111111
Network	172.16.0.0	AC.10.00.00	10101100.00010000.000000   00.00000000
Broadcast	172.16.3.255	AC.10.03.FF	10101100.00010000.000000   11.11111111
Hostmin	172.16.0.1	AC.10.00.01	10101100.00010000.000000   00.00000001
Hostmax	172.16.3.254	AC.10.03.FE	10101100.00010000.000000   11.11111110
Hosts	1,022		

Карты адресации для остальных филиалов приведены в приложении А.

						Лист
						24
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.321.ПЗВКР</b>	

Схема адресного пространства для разрабатываемой сети представлена на рисунке 3.3.

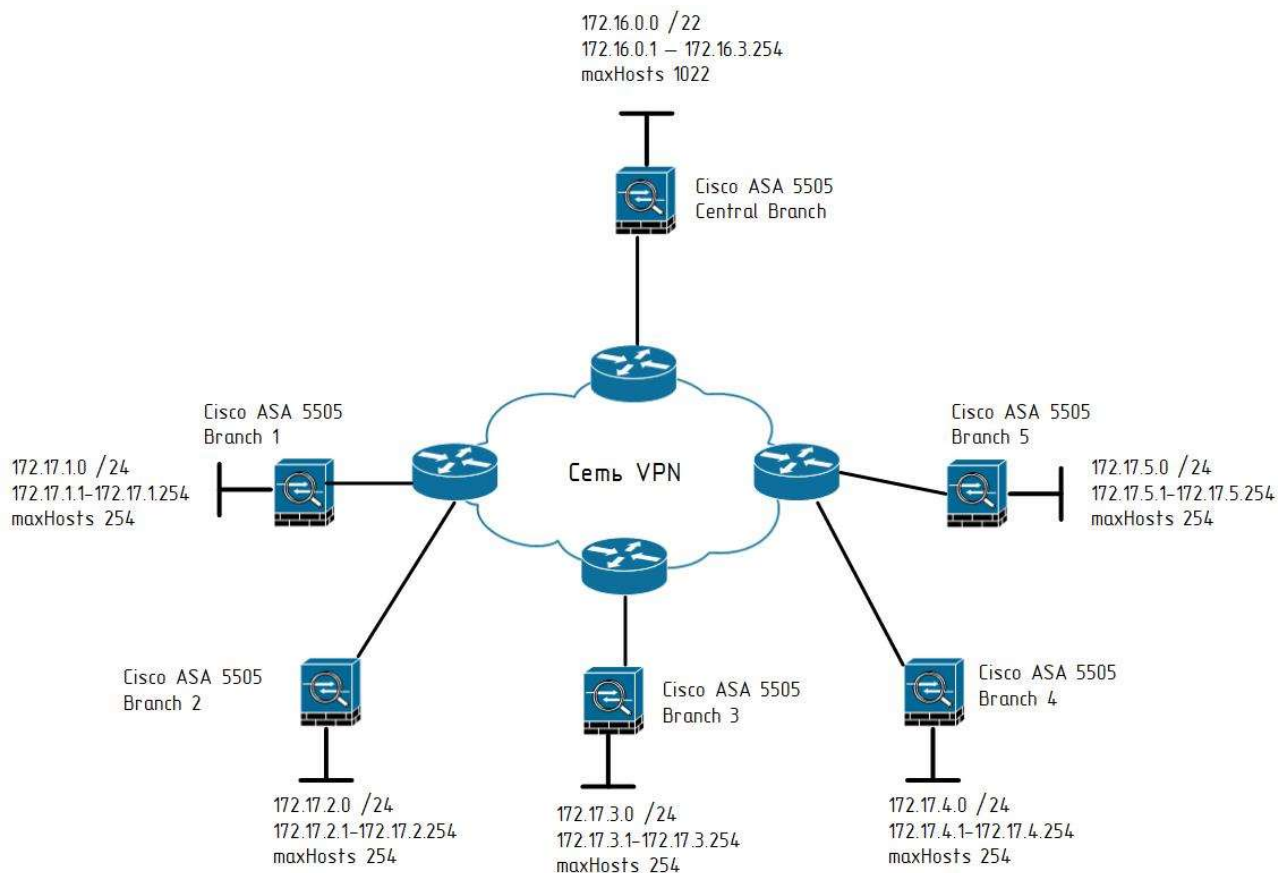


Рисунок 3.3 - Схема адресного пространства VPN сети

### 3.3 Выбор сетевого оборудования

Выбор оборудования для сети абонентского является задачей с неоднозначным решением. Для удобства построения и управляемости сети следует ориентироваться на оборудование единственного поставщика. Практика показывает, что использование оборудование одного поставщика позволяет избежать проблем с совместимостью.

Для проектируемой сети было выбрано оборудование фирмы Cisco Systems (США). Выбор производителя был продиктован его лидирующим положением в области IT.

### 3.3.1 Пограничный маршрутизатор сети

Межсетевой экран CISCO ASA 5505 Sec PLUS appliance with SW, UL users, HA, 3DES/AES

ASA5505-K8 являются полнофункциональным комплексом безопасности для малого бизнеса, офисов и удаленно работающих сотрудников.

Оборудование имеет высокопроизводительный межсетевой экран, SSL и IPsec VPN, а также большое количество сетевых служб в модульном комплексе, поддерживающих "plug-and-play". Данная модель спользует встроенный Cisco ASDM который быстро монтируется и настраивается. Имеет гибкий коммутатор на 8 портов, которые можно динамически сгруппировать для создания 3 отдельных виртуальных сетей, обеспечивая более высокую сетевую фрагментацию и защиту. ASA5505-K8 имеет 2 PoE (Power over Ethernet ) порта, что способствует увеличению сетевой мобильности, облегчению установки IP-телефонии и беспроводных точек доступа. После добавления AIP SSC устройству становится доступно предотвращение вторжений и служба блокирования сетевых червей в системе. Небольшое количество портов USB можно использовать для увеличения дополнительных служб и возможностей.

В дальнейшем, при развитии бизнеса, возможно обновление лицензии до Security Plus, что позволит межсетевому экрану Cisco ASA 5505-K8:

- поддерживать большее количество одновременных подключений до 25 пользователей IPsec VPN;
- объединяться с коммутируемыми сетями при помощи поддержки магистралей виртуальных сетей;
- добавить полную поддержку DMZ.

При следующем обновлении лицензии ASA5505 поможет увеличить эффективность бизнеса путем повышенной доступности служб активности/режима ожидания и поддержки резервирования ISP.

Расширение службы VPN возможно путем улучшения удаленного доступа

						Лист
					<b>11070006.11.03.02.321.ПЗВКР</b>	26
Изм.	Лист	№ докум.	Подпись	Дата		

для поддержки разных бизнес партнеров и мобильных пользователей. Увеличение количество пользователей SSL VPN до 25 на межсетевом экране, обеспечивается установкой Secure Remote-Access Solution, что осуществляется путем обновления лицензии до SSL VPN.

Сочетание высокой защиты и служб VPN, улучшенных сетевых возможностей, гибких возможностей удаленного доступа и будущих расширений делает его замечательным выбором для предпринимателей, требующих верное решение, которое будет лучшим в своем роде для малого бизнеса, офисов, филиалов или корпоративных дистанционных сотрудников.

### 3.3.2 Выбор коммутаторов третьего уровня

В качестве коммутаторов уровня доступа наиболее подходящими можно считать коммутаторы Cisco catalyst 3650. Коммутаторы этой серии применяются для реализации уровня доступа компаний среднего размера. Характеристики моделей коммутаторов данной серии представлены в таблице 3.4.

Таблица 3.4 - Сравнительные технические характеристики коммутаторов

Показатели производительности			
	WS-C3650-24TD-S	WS-C3650-24PD-S	WS-C3650-48TQ-L
Коммутационная ёмкость	88 Гбит/с	88 Гбит/с	176 Гбит/с
Пропускная способность	160 Гбит/с		
Общее количество MAC-адресов	32000		
Общее количество IPv4-маршрутов	24000		
Записи FNF	24000 потоков	24000 потоков	48000 потоков
DRAM	4 Гб		
Флэш-память	2 Гб		
Идентификаторы сети VLAN	4094		
Общее число коммутируемых виртуальных интерфейсов (SVI)	1000		

### Окончание таблицы 3.4

<b>Показатели производительности</b>			
Jumbo frame	9198 байт		
Общее число маршрутизируемых портов на стек 3650	208		
<b>Беспроводные сети</b>			
Число точек доступа на коммутатор/стек	25		
Количество беспроводных клиентов на коммутатор/стек	1000		
Общее число сетей WLAN на коммутатор	64		
Поддерживаемые точки доступа серии Aironet	3700, 3600, 3500, 2600, 1600, 1260, 1140, 1040		
Скорость переадресации	68,45 Мбит/с	130,95 Мбит/с	
<b>Механические</b>			
Размеры (В x Ш x Г)	4,4 x 44,5 x 44,8		
Вес, кг	6,87	7,26	7,21
MTBF	661800	528280	527580
Рабочая температура	-5°C до + 45°C		
Относительная влажность	10% до 95%, без конденсации		

Исходя из особенности построения сети на основе технологии FTTH, моделью, применяемой в нашем случае, будет коммутатор WS-C3650-24TD-S.

Cisco Catalyst серии 3650 коммутаторы, совмещающие в себе основу для конвергенции между проводными и беспроводными сетями .

Одной из инновационных технологий, применяемых на платформе Catalyst 3650, является новая интегральная схема Cisco Unified Access Data Plane (UADP) ASIC, которая обеспечивает поддержку новой архитектуры Cisco Unified Access. Cisco UADP ASIC позволяет объединить обработку проводного и беспроводного трафика на едином уровне (data plane) и обеспечивает высокую производительность и масштабируемость с помощью технологии Cisco StackWise-160. Встроенный WiFi контроллер. Поддерживает установку 2x блоков питания.

										Лист
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.321.ПЗВКР</b>					28

### 3.3.3 Выбор абонентского оборудования

В качестве рабочих станций был выбран офисный компьютер HP 260-a110ur (ZOJ79EA) – рисунок 3.7. Процессор: Intel Celeron J3060; частота процессора: 1.6 ГГц (2.48 ГГц, в режиме Turbo); оперативная память: SO-DIMM, DDR3L 4096 Мб 1600 МГц; видеокарта: Intel HD Graphics 400; HDD: 500 Гб, 7200 об/мин; DVD-RW; Wi-Fi; Bluetooth. Параметры приведены в таблице 3.5.

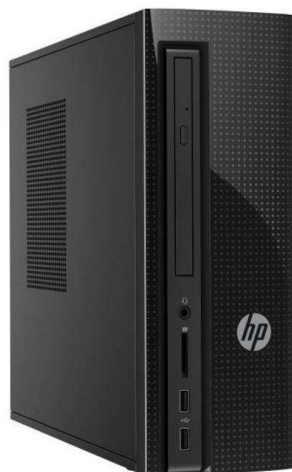


Таблица 3.7 – Офисный ПК

Таблица 3.5 - Характеристики офисного ПК

Модель процессора	Celeron J3060
Размер оперативной памяти	4 Гб
Суммарный объем жестких дисков (HDD)	500 Гб
Модель интегрированной видеокарты	Intel HD Graphics 400

Офисный IP телефон Cisco SPA301 – рисунок 3.8. Однолинейный IP-телефон Cisco SPA301 и трехлинейный IP-телефон Cisco SPA303 с двухпортовым коммутатором, в которых используется протокол SIP, прошли проверку на полную совместимость с оборудованием VoIP ведущих

поставщиков. Обе модели позволяют операторам связи быстро развертывать конкурентоспособные, богатые функциями сервисы для своих заказчиков.



**Таблица 3.8 – Офисный IP телефон Cisco 301**

**Таблица 3.6 - Характеристики офисного IP-телефона**

Порты Fast Ethernet	1 порт 10/100 Мбит/сек
Количество голосовых линий	1
VAD (Voice Activity Detection)	Поддерживается
Безопасность	256-bit Advanced Encryption Standard (AES)
Внутренний свитч	Да

Для размещения различных сервисов предполагается закупка следующего серверного оборудования: сервер HP ProLiant ML350 (рисунок 3.9), Сервер HPE ProLiant ML350 Gen9 E5-2620v4 Tower(5U) / Xeon8C 2.1GHz(20MB)/1x16GbR1D\_2400/ 0/1/10/5/50/6/60)/ noHDD(8/48up)SFF/noDVD/iLOstd/3HPFans/4x1GbEth/1x500wFPlat(2up), analog 765820-421. Параметры сервера приведены в таблице 3.7.



**Таблица 3.9 – Сервер HP ProLiant ML350**



**Таблица 3.7 - Характеристики сервера**

Процессор	Intel Xeon-Silver 4110 (2.1 GHz, 8 core)
Максимальное количество накопителей	48
Сетевой интерфейс	4x1 GibEth
Размер оперативной памяти	16 GB
Блок питания	1x800W HPE FlexSlot Power
RAID-контроллер	Smart Array P408i-a SR

### **3.4 Организация VPN сети для компании Гулливер**

На основе проведенной экспликации объекта и в соответствии с концепцией VPN предлагается использовать оборудование компании Cisco. В качестве пограничных маршрутизаторов использовать платформу Cisco ASA. Данные маршрутизаторы будут выполнять роль входных и выходных узлов в локальные сегменты корпоративной сети. Схема сети представлена на рис. 3.10.

Адаптивные устройства безопасности Cisco ASA 5500 предлагают гибкие технологии для создания специализированных решений, удовлетворяющих различным требованиям к удаленному доступу и связи площадок site-to-site. Адаптивные устройства безопасности ASA 5500 предоставляют простой в управлении удаленный доступ через IPsec и связь площадок через VPN, учитывающей особенности сети.

Локальные сегменты сети построены на базе концепции FTTO (Fiber to the Office) и реализованы на базе коммутаторов третьего уровня Cisco Catalyst WS-C3650-24TD-S. Количество абонентских портов на 1 коммутатор в среднем составляет 19 штук. Серверная ферма располагается в центральном офисе и подключена к отдельному коммутатору доступа, который находится в зоне DMZ.

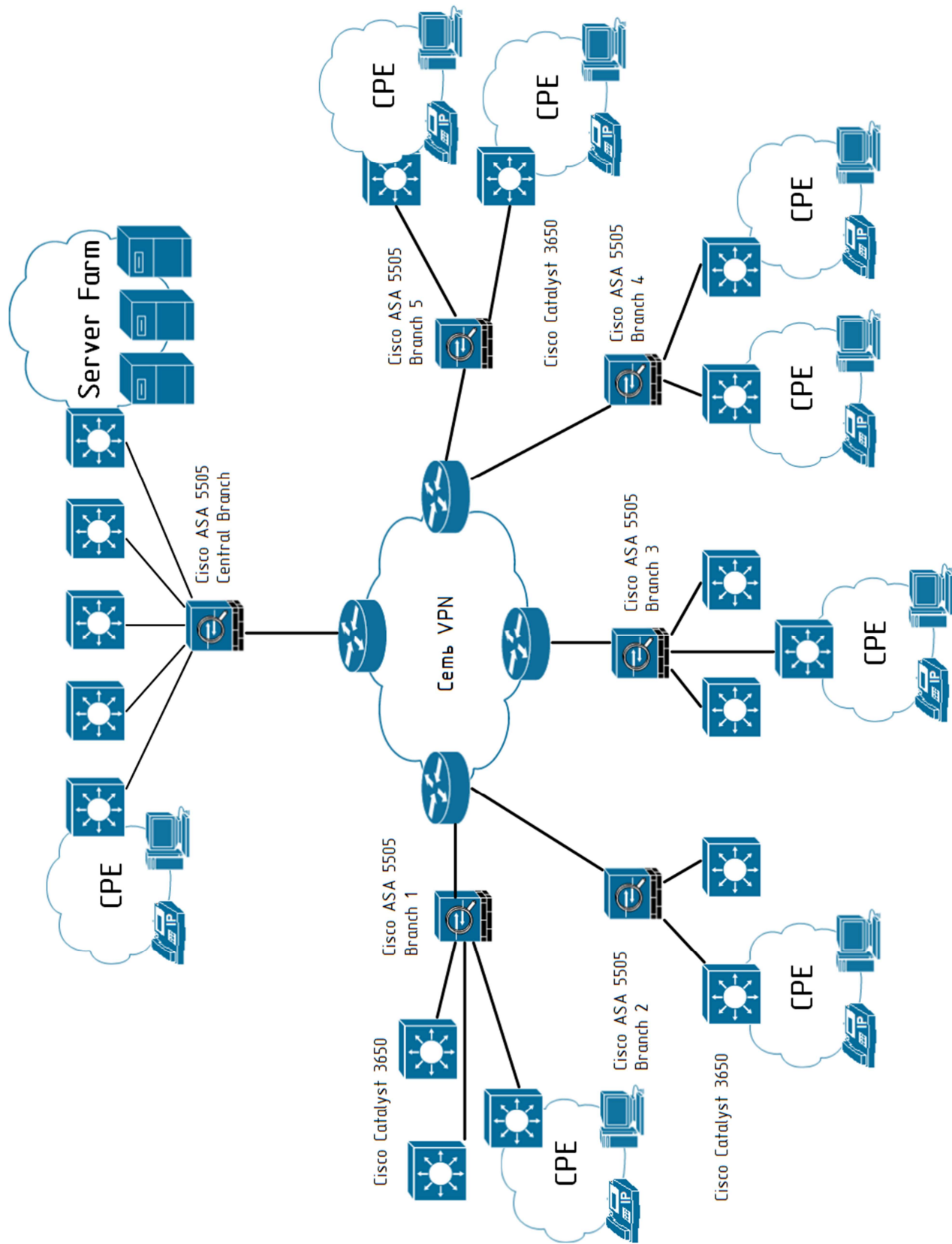


Рисунок 3.10– Проектируемая схема организации сети

Разработанные структурированные кабельные системы для компании Гулливер г. Новосибирск горизонтального уровня представлены на рисунке 3.11, вертикального уровня на рисунке 3.12.

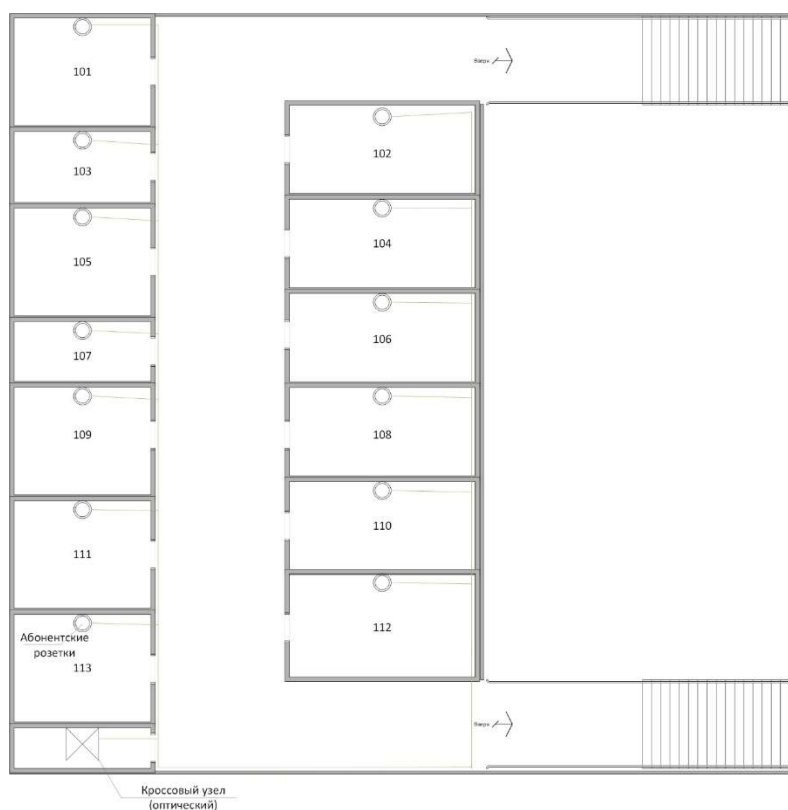


Таблица 3.11 – СКС горизонтального уровня центрального офиса

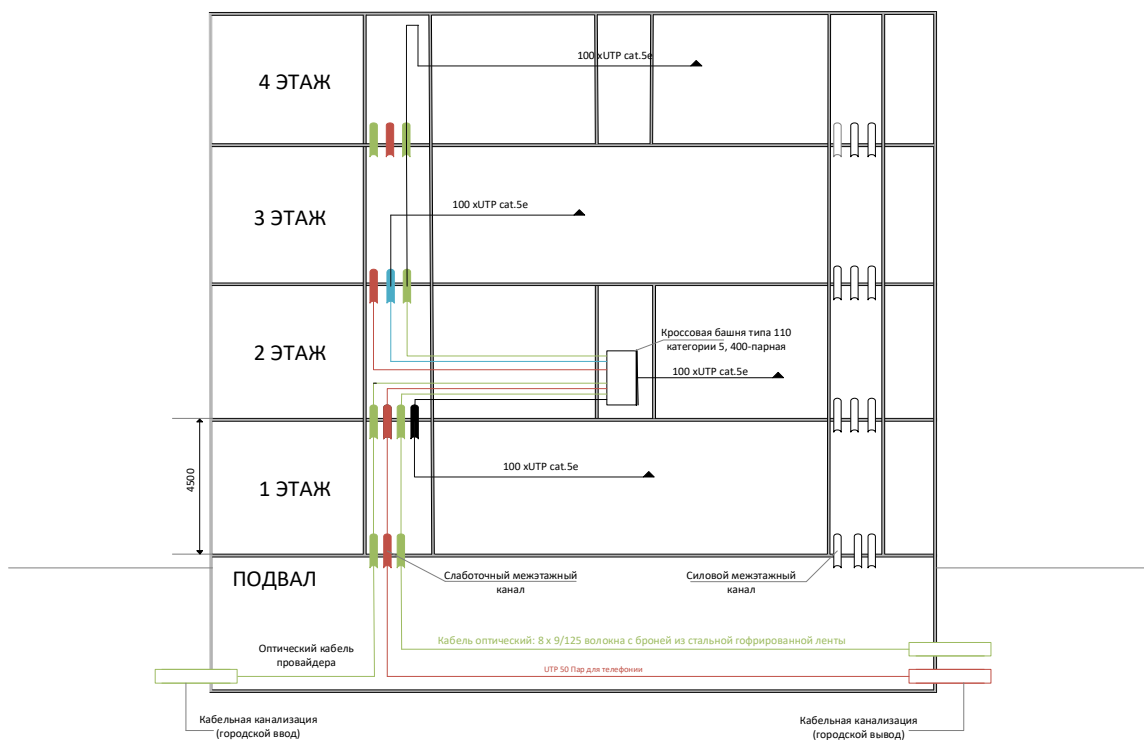


Таблица 3.12 – СКС вертикального уровня центрального офиса

						Лист
						33
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.321.ПЗВКР</b>	

## 4 РАСЧЕТ ХАРАКТЕРИСТИК ПРОПУСКНОЙ СПОСОБНОСТИ МУЛЬТИСЕРВИСНЫХ ПАКЕТНЫХ СЕТЕЙ

Методы обеспечения качества обслуживания (QoS) занимают сегодня одно из важнейших мест в арсенале технологий сетей с коммутацией пакетов, так как без их применения невозможна работа современных мультимедийных приложений, таких как IP-телефония, видео, радиовещание и т.п. Эти методы оперируют параметрами, характеризующими скорость передачи данных, задержку пакетов и потерю пакетов.

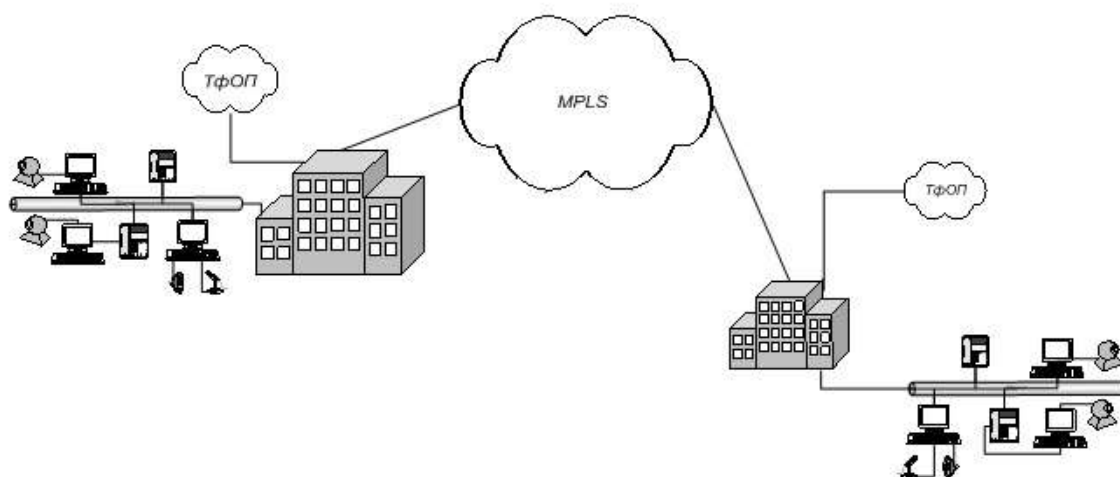


Рисунок 4.1 - Общая структурная схема организации корпоративной сети

Методы обеспечения качества обслуживания фокусируют внимание на влиянии очередей в коммуникационных устройствах на передачу трафика. В них используются различные алгоритмы управления очередями, резервирования и обратной связи, позволяющие снизить негативное влияние очередей до приемлемого для пользователей уровня.

Спроектированный 5 филиал (Заельцовский р-н) сети передачи данных и голосовой информации для Компании «Гуливер» в г. Новосибирск, отдаленный от центрального офиса.

Характеристика отделения организации: 50 пользователей (каждый

						Лист
					<b>11070006.11.03.02.321.ПЗВКР</b>	34
Изм.	Лист	№ докум.	Подпись	Дата		

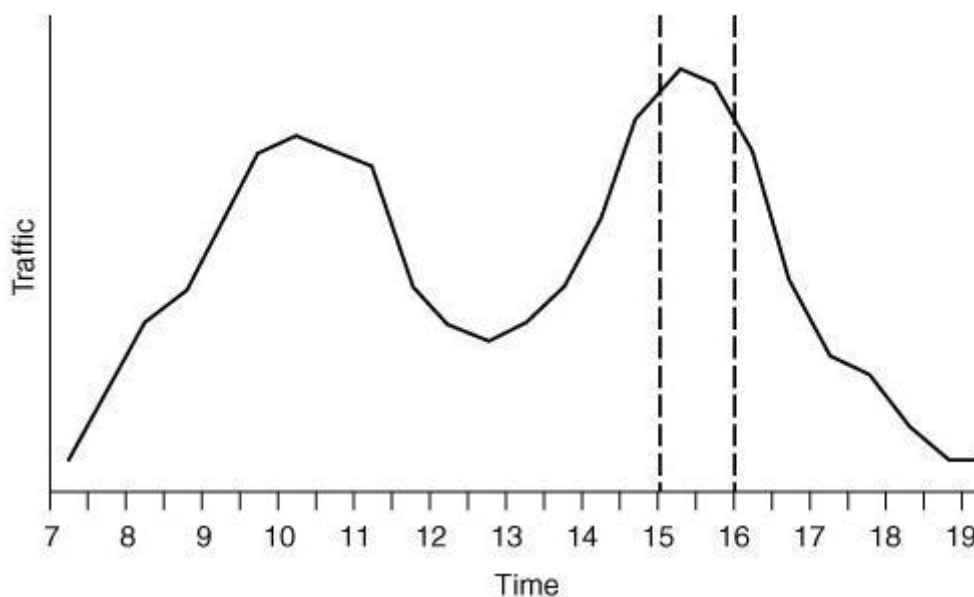
пользователь имеет как персональный компьютер, так и телефонный аппарат).

С целью определения периодов максимальной загруженности сети и объема совершаемых звонков в это время был проведен статистический анализ голосового трафика.

Источниками данной статистики являются:

- оператор ССоП;
- детализация звонков, производимая офисными АТС (PBX CDRs);
- телефонные счета.

Характерное распределение нагрузки представлено на рисунке 4.2.



**Рисунок 4.2 - Распределение нагрузки в зависимости от времени суток**

Произведем расчет нагрузки на сеть в час-пик:

$$Z = \frac{P}{N} \times 1.1 \times 0.15 \quad (4.1)$$

Где, **Z** - загруженность сети в час пик; **P** - продолжительность всех разговоров за месяц, ч; **N** - количество рабочих дней.

Для отделения нового офиса предприятия продолжительность всех разговоров за месяц будет составлять: 880 часов

Количество рабочих дней принимаем равное 22.

Откуда получаем загруженность сети в час-пик:

$$Z = \frac{880}{22} \times 1.1 \times 0.15 = 6.6 \text{ Эрл} \quad (4.2)$$

Одним из основных параметров оценки качества передачи голоса является так называемая вероятность отказа (GoS), определяющий вероятность отказа в предоставлении услуг абоненту. Вероятность отказа принимается равной 0,01. Зная загруженность сети в час-пик и необходимую вероятность отказа, найдем требуемое количество соединительных линий, используя таблицу Эрланга.

**Таблица 4.1 - Таблица Эрланга**

Количество каналов	Вероятность отказа					
	0.003	0.005	0.01	0.02	0.03	0.05
1	0.003	0.005	0.011	0.021	0.031	0.053
2	0.081	0.106	0.153	0.224	0.282	0.382
3	0.289	0.349	0.456	0.603	0.716	0.900
4	0.602	0.702	0.870	1.093	1.259	1.525
5	0.995	1.132	1.361	1.658	1.876	2.219
6	1.447	1.622	1.909	2.276	2.543	2.961
7	1.947	2.158	2.501	2.936	3.250	3.738
8	2.484	2.730	3.128	3.627	3.987	4.543
9	3.053	3.333	3.783	4.354	4.748	5.371
10	3.648	3.961	4.462	5.084	5.530	6.126
11	4.267	4.611	5.160	5.842	6.328	7.077
12	4.904	5.279	5.876	6.615	7.141	7.950
13	5.559	5.964	6.608	7.402	7.967	8.835
14	6.229	6.664	7.352	8.201	8.804	9.730
15	6.913	7.376	8.108	9.010	9.650	10.630

Количество каналов ( $p=0,01$ , загруженность сети 6,6 Эрл) = 13;

Определим количество соединительных линий для связи с АТС, а также количество Интернет-каналов: 70% трафика являются местным, следовательно:

$$K_{ГТС} = 13 \times 0.7 = 9$$

где -  $K_{ГТС}$  – количество соединительных линий с ГТС;

Для связи с ГТС используем 1 плату PRI рассчитанную на 30 каналов

Соответственно 30% трафика является междугородним, следовательно:

$$K_{VoIP} = N \times 30\%$$

где,  $K_{VoIP}$  - количество VoIP шлюзов; N – количество рабочих мест.

Откуда получаем количество VoIP шлюзов:

$$K_{VoIP} = 80 \times 30\% = 24$$

Была рассчитана требуемая полоса пропускания для каналов VoIP:

Требуемая ширина полосы пропускания зависит от используемой комбинации кодеков и интервалов передачи пакетов.

Для обеспечения соответствующего качества речи необходимо учитывать следующие параметры, связанные с типом кодека и интервалом передачи пакетов:

- качество речи кодека G.711 выше качества речи кодека G.729A;
- чем короче интервал передачи пакетов, тем выше качество речи;
- чем выше качество речи, обеспечиваемое платой V-IPGW16, тем большая ширина полосы.

**Таблица 4.2 - Ширина полосы пропускания через локальную сеть**

Кодек	Интервал передачи данных			
	20 мсек	30 мсек	40 мсек	60 мсек
G.711	87.2 Кбит/с	79.5 Кбит/с	75.6 Кбит/с	71.7 Кбит/с
G.729A	31.2 Кбит/с	23.5 Кбит/с	19.6 Кбит/с	87.2 Кбит/с

Требуемая полоса пропускания:

$$PP_{\text{VoIP}} = N_f \times PP_{G.711} + N_t \times PP_{G.729A} , [\text{Кбит/с}]$$

где,  $N_f$  – количество факсимильных аппаратов;  $N_t$  – количество телефонных аппаратов;  $PP_{G.711}$  &  $PP_{G.729A}$  – полосы пропускания кодеков.

$$PP_{\text{VoIP}} = 2 \times 87,2 + 22 \times 31,2 = 860,8 , [\text{Кбит/с}].$$

						Лист
						38
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.321.ПЗВКР</b>	



# 5 РАСЧЁТ СТОИМОСТИ ВНЕДРЕНИЯ И ГОДОВОЙ ЭКСПЛУАТАЦИИ КОРПОРАТИВНОЙ СЕТИ НА БАЗЕ FTTO

## 5.1 Расчёт затрат на внедрение

Произведем экономический расчет стоимости внедрения корпоративной мультисервисной сети компании на базе технологии FTTO. Расчет будет производиться для сети, содержащей 5 филиалов и центральное управление, с общим числом абонентских отводов составляет 1022 подключения.

При проведении расчета на внедрение мультисервисной сети для организации принимаем ряд допущений. Полностью учитывается стоимость активного оборудования всей сети. Стоимость материалов будет определяться из номинальной стоимости материалов для организации мультисервисной сети одного филиала, умноженной на соответствующее число филиалов:

$$C_{Mat} = C_{MatНом} \times 6 \quad (5.1)$$

В таблице 5.1 представлена смета затрат на покупку всей необходимой продукции и оборудования для построения сети одного филиала на примере первого филиала по советскому району, включающей организацию 100 абонентских подключений.

Таблица 5.1 - Затраты на материалы в рублях

Наименование	Ед. изм.	Кол -во	Цена	Сумма.
ВОК для внешней прокладки марки ИК/Д2-Т-А4-1.2, 8 жил	м.	500	15,7	7850
Шнур соединительный UTP, категория 5е, 5м	шт.	993	70	69510
Пигтейл SC SM 9.5/125, 1 м	шт.	10	60	600
Шнур оптический монтажный SM 9/125, SC-SC, duplex, 1 м	шт.	10	330,89	3308,9
ВОК внутриобъектовый марки ИКВА-ПО1-0.05	м.	400 0	18,7	74800
Итого				156069

Цены оборудования и материалов приняты по прайс-листам компаний поставщиков оборудования и актуальны по состоянию на июнь 2018 года, все цены приведены с учетом налога на добавленную стоимость (НДС).

В таблице 5.2 произведен расчет количества и стоимости всего телекоммуникационного оборудования, необходимого для организации сети.

**Таблица 5.2 - Затраты на активное оборудование сети в рублях**

Наименование	Ед. изм	Кол-во	Цена	Сумма.
Серверы	шт.	3	200000	600000
IP телефоны Cisco	шт	331	5990	1982690
Офисные компьютеры (в сборе)	шт.	331	25000	8275000
(PD2W) Модуль вентиляторный, потолочный, 210 x 380 mm, 2 вент.	шт.	6	5000	30000
Маршрутизатор Cisco 3650	шт.	17	110990	1886830
Маршрутизатор Cisco ASA 5505	шт.	6	79990	479940
Розетка UTP	шт.	331	100	33100
Источник бесперебойного питания APC Smart-UPS SC 420VA 230V	шт.	357	4990	1781430
Оптический органайзер 19"	шт.	21	290	6090
Итого				15075080

Для расчета стоимости проведения монтажных работ, тестирования сети, а так же работ связанных с введением сети в эксплуатацию стоимость принимаем равной удвоенной стоимости материалов и стоимости активного и телекоммуникационного оборудования, представленной в таблице 5.2, используемого для организации данной сети:

$$C_{MP} = 2 \times C_{Mat} + C_{Обор} . \quad (5.2)$$

Используя данные таблицы 5.1, произведем расчет стоимости материалов, необходимых для организации мультисервисной сети Центрального офиса:  $C_{Mat}=156069*6=936414$  руб. Стоимость проведения монтажных работ и других видов работ по вводу сети в эксплуатацию составляет:  $C_{MP}=2*936414+15075080=16947908$  руб. Конечная стоимость ввода в эксплуатацию корпоративной сети рассматриваемой организации рассчитывается путем суммированием стоимости материалов, телекоммуникационного оборудования и проведения монтажных работ:

$$C_{КИС} = C_{MP} + C_{Mat} + C_{Обор} . \quad (5.3)$$

Таким образом, стоимость создания сети равна:

$$C_{КИС}=16947908+936414+15075080=32959402 \text{ руб.}$$

## 5.2 Расчет стоимости годовой эксплуатации сети

Расходы по эксплуатации корпоративной мультисервисной сети рассчитываются по формуле:

$$C_{ГЭ} = C_A + C_{ЗП} + C_{ЕСН} + C_{Э} + C_H , \quad (5.4)$$

где:  $C_A$  - амортизационные отчисления, руб.;  $C_{ЗП}$  - расходы на заработную плату, руб.;  $C_{ЕСН}$  - единый социальный налог, руб.;  $C_{Э}$  - расходы на электроэнергию, руб.;  $C_H$  - накладные и прочие расходы, руб.

Значения амортизационных отчислений зависят от принятого на предприятии способа начисления амортизации. Существует несколько способов расчета:

						Лист
					<b>11070006.11.03.02.321.ПЗВКР</b>	41
Изм.	Лист	№ докум.	Подпись	Дата		

- линейный - расчет производится исходя из фактической стоимости предмета и нормы амортизации, исчисленной с учетом срока полезного использования;
- снижение стоимости - расчет производится пропорционально объему продукции (работ), производимой (выполняемой) с использованием предмета, и предполагаемой продукции (работ) за весь срок полезного использования;
- процентный - расчет производится исходя из фактической себестоимости предмета и ставки в 50% или 100% при передаче предмета в производство или эксплуатацию. При этом в первом случае оставшиеся 50% списываются при выбытии предмета из производства или эксплуатации из-за невозможного использования (непригодности).

Для расчета амортизационных отчислений применим линейный способ расчета. Расходы на амортизационные отчисления вычисляются исходя из стоимости используемого телекоммуникационного сетевого оборудования, приведенного в таблице 5.2, стоимость которого составляет 15075080 руб.

Расходы на амортизацию вычисляются по формуле:

$$C_A = K \times \frac{H_A \times T_{Общ}}{T_G}, \quad (5.5)$$

Где К - первоначальная стоимость телекоммуникационного оборудования, рублей;  $H_A$  - норма амортизационных отчислений, процент;  $T_{Общ}$  - время работы оборудования;  $T_G$  - календарный годовой фонд времени, дни (действительный фонд времени работы оборудования за год);

Норма амортизационных отчислений при применении линейного метода определяется по формуле:

$$H_A = \frac{1}{n} \times 100\%, \quad (5.6)$$

где n - срок полезного использования активного сетевого оборудования, лет.

						Лист
					<b>11070006.11.03.02.321.ПЗВКР</b>	42
Изм.	Лист	№ докум.	Подпись	Дата		

В разрабатываемом проекте применяется современное, отвечающее всем технологическим требованиям оборудование, с высокими показателями надежности. Учитывая это, предполагается принять срок эксплуатации данного оборудования, без необходимости его замены, равным 5 годам.

Таким образом, норма амортизации составит 20%, а затраты на амортизацию будут равны:

$$CA=15075080*0,2*365*24/365*24=26411540160/8760=3015016 \text{ руб.}$$

Расход на заработную плату осуществляется для обслуживающего персонала корпоративной мультисервисной сети, который состоит из шести инженеров-администраторов сети.

Основная заработная плата работников, в общем случае, рассчитывается по формуле:

$$\Phi ЗП_{осн} = Ч_{яв} \times O \times T_{общ} \times K_{н.д.}, \quad (5.7)$$

где ЧЯВ - явочная численность работников, чел.; O - оклад (месячная тарифная ставка), руб.; T<sub>общ</sub> - общая трудоемкость, чел.-дней; КН.Д. - коэффициент, учитывающий надбавку и доплату.

При расчете примем сумму месячного оклада инженера-администратора равной 25000 руб., а так же размер премиальных выплат равный 10% и коэффициент, учитывающий надбавку и доплату - 15%. Сумма оклада инженера равна 25000 руб. в месяц или 833 руб. в день, районный коэффициент для Новосибирской области равен 15% и также учитывается при расчете заработной платы.

Фонд основной заработной платы рассчитывается как сумма перечисленных составляющих:

$$\Phi ЗП_{осн} = \Phi ЗП_{окл} + \Phi ЗП_{пр} + \Phi ЗП_{рк}, \quad (5.8)$$

						Лист
					<b>11070006.11.03.02.321.ПЗВКР</b>	43
Изм.	Лист	№ докум.	Подпись	Дата		

где ФЗПОКЛ - фонд заработной платы оклада; ФЗППР - фонд заработной платы премиальных выплат; ФЗПРК - фонд заработной платы надбавки районного коэффициента.

$$\text{ФЗПОКЛ} = 6 * 833 * 21 * 12 * 1.2 = 1511395,2 \text{ руб.}$$

$$\text{ФЗППР} = \text{ФЗПОКЛ} * 0,1 = 151139,52 \text{ руб.}$$

$$\text{ФЗПРК} = (\text{ФЗПОКЛ} + \text{ФЗППР}) * 0,15 = (1511395,2 + 151139,52) * 0,15 = 249380 \text{ руб.}$$

$$\text{ФЗПОСН} = 1511395,2 + 151139,52 + 249380 = 1911915 \text{ руб.}$$

Дополнительная заработная плата устанавливается в процентах от основной и может быть принята в размере 10 %.

$$\text{ФЗПДОП} = \text{ФЗПОСН} * 0,1 = 1911915 * 0,1 = 191191,5 \text{ руб.}$$

Таким образом, общий годовой фонд заработной платы шести инженеров-администраторов сети составит:

$$\text{СЗП} = \text{ФЗПОСН} + \text{ФЗПДОП} = 1911915 + 191191,5 = 2103106,5 \text{ руб.}$$

Отчисления по единому социальному налогу (выплаты в пенсионный фонд Российской Федерации, федеральный бюджет, фонд социального страхования, а также в фонд обязательного медицинского страхования) в процентном отношении от общего фонда заработной платы принимаются в размере 26,2%.

Таким образом:

$$\text{СЕСН} = \text{СЗП} * 0,262 = 2103106,5 * 0,262 = 551014 \text{ руб.}$$

Расходы на электрическую энергию рассчитываются по формуле:

$$C_{\text{э}} = C_{\text{э}} \times \text{Э}_{\text{э}}, \quad (5.9)$$

где  $C_{\text{э}}$  - тариф на электрическую энергию, руб/кВт\*ч;  $\text{Э}_{\text{э}}$  - расчетное потребление количества электрической энергии, кВт\*ч.

$$\text{Э}_{\text{э}} = P_{\text{у}} \times P_{\text{у}} \times T_{\text{у}}, \quad (5.10)$$

где,  $P_{\text{у}}$  - количество оборудования данного вида;  $P_{\text{у}}$  - установленная мощность

						Лист
					<b>11070006.11.03.02.321.ПЗВКР</b>	44
Изм.	Лист	№ докум.	Подпись	Дата		

оборудования, кВт;  $T_y$  - фонд работы оборудования, часов.

Разрабатываемая сеть содержит активное коммуникационное оборудование, потребляющее электроэнергию согласно спецификациям предприятия изготовителя, при максимальной нагрузке на сеть, не более 90 Вт/ч. Расчетную нагрузку на активное оборудование примем равным 70 процентам от максимальной - 63 Вт/ч.

Энергопотребление всей корпоративной сети по ориентировочным оценкам составляет приблизительно 6600 Вт/ч.

Расчетное потребление электрической энергии составит :

$$\text{ЭЭ} = 160 * 0,66 * 365 * 24 = 1613066 \text{ кВт/ч.}$$

Следовательно, годовой расход на электрическую энергию при текущем тарифе на электрическую энергию 2,6 руб./кВт\*ч будет равен:

$$\text{СЭ} = 2,6 * 1613066 = 4193972,64 \text{ руб.}$$

Под накладными и прочими расходами принимаем затраты на содержание аппарата управления, проведение технических осмотров оборудования, замену и модернизацию текущего оборудования, а так же затраты на производство мелкого ремонта. Величину накладных расходов условно принимаем равной 25% от суммы всех затрат на содержание и эксплуатацию корпоративной мультисервисной сети и составляет 3418784 руб.

Таким образом, суммарная итоговая стоимость годовой эксплуатации инфраструктуры корпоративной сети составит:

$$\text{СГЭ} = 3015016 + 2103106,5 + 551014 + 4193972,64 + 3418784 = 13281893 \text{ руб.}$$

Результаты расчета основных затрат на эксплуатацию корпоративной мультисервисной сети представлены в таблице 5.3

					<b>11070006.11.03.02.321.ПЗВКР</b>	Лист
Изм.	Лист	№ докум.	Подпись	Дата		45

**Таблица 5.3 - Структура затрат на эксплуатацию сети провайдера связи**

Наименование статьи затрат	Сумма, руб.	Удельный вес, %
Амортизационные отчисления	3015016	77
Фонд основной заработной платы	2103106,5	5
Отчисления по ЕСН	551014	1
Электроэнергия	4193972,64	9
Накладные и прочие расходы	3418784	8
Годовые расходы на эксплуатацию	13281893	100

Таким образом, результирующая стоимость создания корпоративной мультисервисной сети на базе технологии FTTO составляет - СКИС=32959402 руб. Расходы организации связанные с годовой стоимостью эксплуатации разработанной сети составляют - СГЭ=13281893 руб.



## **6 ОХРАНА ТРУДА, ТЕХНИКА БЕЗОПАСНОСТИ И ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРОЕКТА**

Техническое помещение для мультисервисной сети связи является помещением с повышенной опасностью поражения электрическим током, в силу опасности одновременного прикосновения к металлическим корпусам оборудования с одной стороны и к заземлённым металлическим конструкциям с другой. Для предотвращения этого необходимо соблюдать нормы на проектирование эксплуатационных проходов – 1800 мм и размещение оборудования вдали от батарей центрального отопления. Места разъемов должны располагаться в безопасном для человека месте, все провода должны быть изолированы.

Ремонт и техническое обслуживание мультисервисного оборудования необходимо производить в соответствии с правилами техники безопасности при эксплуатации электрических установок до 1 000 В. К обслуживанию должны допускаться лица, имеющие квалификацию четвёртой группы по правилам техники безопасности.

Пожар, возникающий на участке мультисервисной сети, может привести к выходу из строя оборудования, и угрожает жизни и здоровью людей. К основным причинами пожаров относятся: неисправности электрооборудования (короткое замыкание, пробой в цепях электрического тока, перегрузка и так далее); самовозгорание горючих веществ; неправильное хранение пожароопасных материалов (спирт, бензин); курение в не предназначенных для этого местах.

На участке ЭМС заранее разработаны мероприятия, обеспечивающие быструю ликвидацию возникшего пожара. К этим мероприятиям относятся:

1. установка устройств пожарной сигнализации,
2. организация средств пожаротушения, с набором средств пожаротушения. Во всех технических помещениях АТС предусмотрена установка углекислотных огнетушителей ОУ-8, в которых в качестве

									Лист
									47
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.321.ПЗВКР</b>				

огнегасящего вещества используется углекислый газ, не являющийся электропроводным; кроме того, он не портит предметы, подвергающиеся тушению;

3. организация двух выходов из технического помещения - главного и запасного, и наружных пожарных лестниц.

При возникновении аварийной ситуации на рабочем месте, работающий с персональным компьютером обязан работу прекратить, отключить электроэнергию, сообщить руководителю и принять меры к ликвидации создавшейся ситуации. При наличии травмированных:

- - устранить воздействие повреждающих факторов, угрожающих здоровью и жизни пострадавших (освободить от действия электрического тока, погасить горящую одежду и т.д.);
- - оказать первую помощь;
- - вызвать скорую медицинскую помощь или врача, либо принять меры для транспортировки пострадавшего в ближайшее лечебное учреждение;
- - сохранить, по возможности, обстановку на месте происшествия;

Разработанные в разделе мероприятия и рекомендации в полной мере решают вопросы охраны труда. Мероприятия по эргономическому обеспечению (удобное рабочее место оператора, оптимальное размещение оборудования, правильное освещение) способствует созданию наилучших условий работы оператора.

Мероприятия по технике безопасности (заземление и зануление оборудования, применение защитных средств) соответствуют требованиям системы стандартов безопасности труда. Мероприятия по пожарной профилактике (надёжная изоляция токонесущих проводов, оснащение помещений огнетушителями и сигнализацией) позволяют предотвратить возникновение пожара, вовремя его обнаружить и принять меры по его устранению.

					<b>11070006.11.03.02.321.ПЗВКР</b>	Лист
Изм.	Лист	№ докум.	Подпись	Дата		48

## ЗАКЛЮЧЕНИЕ

В ходе дипломного проектирования была разработана корпоративная мультисервисная сеть на базе технологии FTTO.

Мультисервисная сеть была разработана как альтернативный вариант существующей вычислительной сети компании «Гуливер» г. Новосибирск. Разработанный вариант реализации сети отражает современные тенденции интеграции разнородных видов трафика и обеспечивает значительную ширину канала передачи данных, за счет использования на всех участках сети волоконно-оптические линии связи.

В ходе выполнения дипломного проекта была разработана архитектура корпоративной сети, выбрано активное сетевое оборудование. В качестве маршрутизатора центрального офиса был выбран маршрутизатор Cisco ASA 5505-K10/315R, в качестве маршрутизаторов филиалов была выбрана модель Cisco ASA 5505-K8/218R. Для прокладки вертикальной СКС был предложен волоконно-оптический кабель компании «Интегра кабель» марки ИК/Д2-Т-А4.

Был произведен расчет экономической части дипломного проекта: рассчитана стоимость материалов, телекоммуникационного оборудования и стоимость проведения монтажных работ, работ по тестированию сети, а так же работ связанных с вводом сети в эксплуатацию. Общая стоимость построения мультисервисной сети по технологии FTTO составила 32959402 руб.

						Лист
						49
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.321.ПЗВКР</b>	

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Росляков, А.В., Самсонов, М.Ю. Сети следующего поколения NGN [Текст] // А.В. Росляков, М.Ю. Самсонов - М.: Эко-Трендз, 2008.- 449 с. 25.  
Росляков, А.В., Самсонов, М.Ю., Сети следующего поколения NGN [Текст] / А.В. Росляков, М.Ю. Самсонов. - М.: Эко-Трендз, 2008.- 449 с.

2. Интернет вещей. Обзор перспектив [Электронный ресурс] // Официальный сайт компании Cisco Systems / Режим доступа: <http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html> (Дата обращения 10.04.18)

3. Соколов Н.А. Сети доступа FTTx. Принципы построения. [Текст] // Н.А. Соколов -М.: ЗАО “ИГ” Энтер-профи, 2006, 308с.

4. Бакланов, И.Г. Технологии xDSL теория и практика применения [Текст] // И.Г. Бакланов. – М.: Метротек, 2007, 384с.

5. Семенов А.Ю. Пассивные оптические сети. [Текст] // А.Ю. Семенов - М.: Радио и связь, 2009, 317с.

6. Гольдштейн Б.С. Беспроводные сети доступа [Текст] // Б.С. Гольдштейн, - М.: Радио и связь, 200.-317с.

7. Вишневский В.А. Энциклопедия WiMax. Путь 4G. [Текст] // В.Вишневский, С.Портной, И.Шахнович - М.: Техносфера, 2009 г. — С. 472

8. Парфенов Ю.А., Мирошников Д.Г. Последняя миля на медных кабелях.- М.: ЭКО-Трендз, 2001.-222с.

9. Шмалько А.В. Цифровые сети связи . Основы планирования и построения [Текст] // А.В. Шмалько - М.: ЭКО-ТРЕНДЗ, 2001, -222с.

10. Никульский И.Е. Построение сетей связи на базе технологии DOCSIS [Текст] // И.Е. Никульский, -Вестник связи, 2001, №11.- с.57-61.

11. Колпаков И.А. Универсальная мультисервисная транспортная среда на базе сетей кабельного телевидения (часть 1) [Текст] // Колпаков И.А. Васькин О.П., Смирнов С.С., Теле-Спутник, 2002, январь.- С.54-56.

						Лист
						50
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.321.ПЗВКР</b>	

12. Башилов Г. LTE: эволюция технологий беспроводного доступа [Текст] // Г.А. Башилов, Журнал сетевых решений, 2011, №6.- с.43-61.

13. Решения FTTO на базе оборудования компании Cisco [Электронный ресурс] // Официальный сайт Cisco Systems / Режим доступа: <http://www.cisco.com/ethernet-solutions/ftto.html> (Дата обращения 05.04.18)

14. Одом У. Официальное руководство по подготовке к сертификационным экзаменам CCNA Маршрутизация и коммутация, академическое издание [Текст] // У. Одом - М.: Вильямс, 2015. -761с.

15. Гольдштейн Б.С. Сети связи [Текст] // Гольдштейн Б. С., Соколов Н. А., Яновский Г.Г.- СПб.: «БХВ – Петербург», 2014. – 400 с.

26. Руководящий технический материал «Принципы построения мультисервисных сетей электросвязи» [Текст] // – ФГУП ЦНИИС, 2011. - версия 4.0, с. 291.

17. Международный стандарт ISO/IEC IS 11801-2002 Information Technology. Generic cabling for customer premises [Электронный ресурс] // Сайт sb-ufa ISO/IEC IS 11801-2002 / Режим доступа: [http://sb-ufa.ru/wp-content/uploads/2013/12/ISO\\_IEC\\_11801\\_2002.pdf](http://sb-ufa.ru/wp-content/uploads/2013/12/ISO_IEC_11801_2002.pdf) (Дата обращения 05.04.18)

18. ГОСТ Р 53246-2008 Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования [Электронный ресурс] // Каталог ГОСТ / Режим доступа: <http://www.internet-law.ru/gosts/gost/48148/> (Дата обращения 05.04.18)

19. ГОСТ Р 53245-2008 Информационные технологии. Системы кабельные структурированные. Монтаж основных узлов системы. Методы испытания [Электронный ресурс] // Каталог ГОСТ / Режим доступа: <http://www.internet-law.ru/gosts/gost/48147/> (Дата обращения 05.04.18)

20. ГОСТ 21.406-88 Система проектной документации для строительства. Проводные средства связи. Обозначения условные графические на схемах и планах [Электронный ресурс] // Каталог ГОСТ / Режим доступа: <http://www.internet-law.ru/gosts/gost/19553/> (Дата обращения 05.04.18)

21. IEEE Standarts 802.3: Ethernet [Электронный ресурс] // IEEE Standarts download page / Режим доступа: <http://standards.ieee.org/about/get/802/802.3.html> (Дата обращения 06.04.18)

22. Инкаб Оптические Кабели [Электронный ресурс] // Каталог продукции / Режим доступа: <http://incab.ru/files/spec.pdf> (Дата обращения 10.05.18)

23. СвязьСтройДеталь продукция для построения сетей связи [Электронный ресурс] // Режим доступа: URL: [http://ssd.ru/files/catalog\\_2016.pdf](http://ssd.ru/files/catalog_2016.pdf) (Дата обращения 10.05.18)

24. Монтаж-линия. Кабели связи [Электронный ресурс] // Каталог товаров и услуг / Режим доступа: <http://roitl.com/catalog/2017.pdf> (Дата обращения 19.04.18)

25. Сетевое оборудование ВТК-связь [Электронный ресурс] // Официальный сайт компании ВТК, Каталог оборудования от компании Cisco Systems / Режим доступа: <http://www.vtkt.ru/catalog/localarea/cisco/> (Дата обращения 21.04.18)

26. Сетевое и серверное оборудование [Электронный ресурс] // Официальный сайт компании NAG / Режим доступа: [www.shop.nag.ru/catalog](http://www.shop.nag.ru/catalog) (Дата обращения 21.04.18)

27. IEEE Standarts 802.1Q: VLAN [Электронный ресурс] // IEEE Standarts download page / Режим доступа: <http://standards.ieee.org/about/get/802/802.1q.html> (Дата обращения 16.04.18)

28. СН 512-78 Инструкция по проектированию зданий и помещений для электронно-вычислительных машин, редакция №2 [Электронный ресурс] // Каталог ГОСТ Е.: / Режим доступа: <http://docs.cntd.ru/document/901707386/> (Дата обращения 15.04.18)

29. Руководящий технический материал «Принципы обеспечения безопасности на объектах связи» [Текст]– ФГУП ЦНИИС, 2010.- 145 с.

						Лист
						52
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.321.ПЗВКР</b>	