

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

**РАЗРАБОТКА ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ  
КОММЕРЧЕСКОГО БАНКА ТЕСНСОМБАНК, ВЬЕТНАМ**

Выпускная квалификационная работа  
обучающегося по направлению подготовки 11.03.02 Инфокоммуникационные  
технологии и системы связи  
очной формы обучения, группы 07001410  
Чан Чунг Хиеу

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

Рецензент  
Начальник службы управления  
сетями, сервисами и  
информационными системами  
Белгородского филиала  
ПАО «Ростелеком»  
Нагорный П. В.

БЕЛГОРОД 2018

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 « Сети связи и системы коммутации »

Утверждаю  
Зав. кафедрой

« \_\_\_\_ » \_\_\_\_\_ 2018 г.

## **ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ**

Чан Чунг Хиеу

---

1. Тема ВКР «Разработка инфокоммуникационной инфраструктуры коммерческого банка Techcombank, Вьетнам »

Утверждена приказом по университету от « \_\_\_\_ » \_\_\_\_\_ 2018 г. № \_\_\_\_\_

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

3. Исходные данные:

объект проектирования – коммерческий банк Techcombank, Вьетнам;

тип сети связи – LAN;

количество абонентов в Центральном офисе – 61.

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

4.1. Описание объекта проектирования;

4.2. Разработка концепции реализации инфокоммуникационной инфраструктуры банка;

4.3. Разработка корпоративной сети связи центрального офиса банка и транспортного сегмента сети;

4.4. Разработка рекомендаций по реализации инфокоммуникационной инфраструктуры банка и обеспечение информационной безопасности;

4.5. Технико-экономическое обоснование проекта.

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

5.1. Проектируемая схема организации связи (А1, лист 1);

5.2. План структурированной кабельной системы центрального офиса здания (А1, лист 1);

5.3. Модель сети банка в среде имитационного моделирования Packet Tracer;

5.4. Технико-экономические показатели проекта.

6. Консультанты по работе с указанием относящихся к ним разделов

Раздел	Консультант	Подпись, дата	
		Задание выдал	Задание принял
4.1. – 4.4	<i>канд. техн. наук, доцент каф. ИТСиТ Девыцына С.Н.</i>		
4.5	<i>канд. техн. наук доцент каф. ИТСиТ Болдышев А.В.</i>		

7. Дата выдачи задания \_\_\_\_\_

**Руководитель**

*канд. техн. наук, доцент,  
доцент кафедры Информационно-телекоммуникационных  
систем и технологий» НИУ «БелГУ», \_\_\_\_\_ С.Н. Девыцына*  
(подпись)

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

## СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1 ОПИСАНИЕ ОБЪЕКТА ПРОЕКТИРОВАНИЯ	5
1.1 Инфраструктура коммерческого банка Techcombank, Вьетнам	5
1.2 Выбор способа обмена данными между подразделениями банка	6
1.3 Постановка задач проектирования	8
2 РАЗРАБОТКА КОНЦЕПЦИИ РЕАЛИЗАЦИИ ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ БАНКА	9
2.1 Анализ и описание современных инфокоммуникационных технологий и способов реализации защищённых корпоративных сетей	9
2.2 Выбор сетевых технологий и схемных решений	11
2.3 Выбор типа трафика в корпоративной сети и расчет нагрузок	14
3 РАЗРАБОТКА КОРПОРАТИВНОЙ СЕТИ СВЯЗИ ЦЕНТРАЛЬНОГО ОФИСА БАНКА И ТРАНСПОРТНОГО СЕГМЕНТА СЕТИ	22
3.1 Проектирование сети связи центрального офиса	22
3.2 Проектирование транспортной инфраструктуры для обмена данными между филиалами банка	30
3.3 Расчет объёма оборудования	34
4 РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО РЕАЛИЗАЦИИ ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ БАНКА И ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	41
4.1 Мероприятия по реализации и технической эксплуатации сети банка	41
4.2 Механизмы обеспечения защиты информации	46
4.3 Охрана труда и техника безопасности при эксплуатации сети	48
5 ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ПРОЕКТА	50
ЗАКЛЮЧЕНИЕ	58
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	59
ПРИЛОЖЕНИЕ А	63
ПРИЛОЖЕНИЕ Б	65
ПРИЛОЖЕНИЕ В	66
ПРИЛОЖЕНИЕ Д	67

					<i>11070006.11.03.02.475.ПЗВКР</i>			
Изм.	Лист	№ докум.	Подпись	Дата				
Разработал	Чан Чунг Хиеу				Разработка инфокоммуникационной инфраструктуры коммерческого банка Techcombank, Вьетнам	Лит.	Лист	Листов
Проверил	Девицына С. Н.						2	68
Рецензент	Нагорный П. В.					<i>НИУ «БелГУ» гр. 07001410</i>		
Н. Контроль	Девицына С. Н.							
Утвердил	Жиляков Е.Г.							

## ВВЕДЕНИЕ

В Социалистической Республике Вьетнам активно внедряются IT-решения во все сферы деятельности. В последние годы интенсивно развивается финансово-экономическая область, требующая использования самых современных информационных технологий. В результате двадцатилетнего применения информационных технологий, финансовый сектор построил более 110 IT-порталов. Применение информационных технологий для обслуживания частных клиентов и предприятий всегда направлено на достижение эффективных результатов в финансовой сфере.

Techcombank – один из ведущих коммерческих банков Вьетнама, с устойчивой финансовой основой и развитой структурой. В своей деятельности банк ориентируется на персонализированные клиент-ориентированные отношения. Поэтому актуальной является задача использования всех преимуществ инфокоммуникационных технологий для управления финансовыми и коммуникационными процессами банка. В выпускной квалификационной работе представлена разработка инфокоммуникационной инфраструктуры организации Techcombank, предназначенной для взаимодействия между сотрудниками банка, обмена, передачи информации и для совместного использования периферийного оборудования и устройств хранения информации.

Целью проекта является разработка инфокоммуникационной инфраструктуры коммерческого банка Techcombank, Вьетнам, которая позволит обеспечить информационный обмен между подразделениями банка, улучшит условия труда сотрудников, повысит конкурентоспособность организации на финансовом рынке.

Для реализации инфокоммуникационной инфраструктуры банка нужно решить следующие задачи:

1. Выбор сетевых технологий;

						Лист
						3
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

2. Разработка схемы организации связи;
3. Выбор и расчет объёма сетевого оборудования;
4. Создание модели сети банка;
5. Исследование параметров сети на основе разработанной модели;
6. Разработка рекомендаций по реализации инфокоммуникационной инфраструктуры банка.

						Лист
						4
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

# 1 ОПИСАНИЕ ОБЪЕКТА ПРОЕКТИРОВАНИЯ

## 1.1 Инфраструктура коммерческого банка Techcombank, Вьетнам

Акционерный коммерческий банк Techcombank является одним из крупнейших акционерных коммерческих банков во Вьетнаме. Techcombank был создан 27 сентября 1993 года, начальный капитал составлял всего 20 миллиардов VND. Techcombank неуклонно развивался с отличными бизнес-результатами и получил широкое признание как финансовое учреждение, и стал самым успешным банком во Вьетнаме. Сегодня, при поддержке стратегических акционеров HSBC, у банка есть прочная финансовая основа, общая сумма активов которой превышает 158.8 миллиарда VND (на конец 2013 года).

Techcombank предоставляет широкий набор финансовых услуг, имеет 315 филиалов и 1229 банкоматов по всей стране, а также обладает новейшими банковскими технологиями.

Кроме того, Techcombank возглавляет талантливая команда опытных многонациональных финансовых специалистов и штат, состоящий из более чем 7000 профессионально подготовленных сотрудников, готовых к внедрению IT-инноваций в финансовой сфере. Цель банка - стать лучшим банком и ведущей коммерческой организацией во Вьетнаме.

Банк предоставляет финансовые продукты и услуги. Разработаны 3 стратегических направления бизнеса: личные финансовые услуги, банковские услуги для малых и средних предприятий, коммерческое банковское обслуживание и транзакционное банковское дело. Банк учитывает разнообразные потребности клиентов разных сегментов. Поэтому более 3,3 миллиона личных клиентов и 45 368 бизнес-клиентов выбрали Techcombank в качестве финансового компаньона. [1]

Территориально банк расположен на нескольких площадках. Головной офис банка расположен в трехэтажном здании, общая площадь составляет 1215

									Лист
									5
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>				

м<sup>2</sup>. На первом этаже имеется 23 компьютера, 14 телефонов, 14 видеокамер, 10 принтеров, одна точка доступа, 5 банкоматов. На втором этаже размещены: 21 компьютер, 1 ноутбук, 10 телефонов, 6 принтеров, 8 видеокамер, один проектор, две точки доступа. На третьем этаже размещено 19 компьютеров, 11 телефонов, 9 принтеров, 9 видеокамер, одна точка доступа (таблица 1.1).

**Таблица 1.1 – Количество и вид оконечного оборудования**

Этаж	1	2	3	Итого:
Компьютер	23	21	17	61
Телефон	14	10	11	35
Видеокамера	14	6	9	29
Принтер	10	8	9	27
Точка доступа	1	2	1	4
Банкомат	5	-	-	5
Ноутбук	-	1	-	1
Проектор	-	1	-	1

Количество устройств, которые должны иметь выход в сеть Интернет – 163. На каждом этаже должен быть установлен коммутационный узел с коммутаторами, маршрутизаторами, патч-панелями, кроссами, серверами.

Поэтому в процессе проектирования будет разработана структурированная кабельная система, позволяющая объединить сетевое оборудование и обеспечить доступ сотрудников банка к интрасети и сети Интернет.

## **1.2 Выбор способа обмена данными между подразделениями банка**

В подразделениях Techcombank будет реализована локальная вычислительная сеть, объединяющая ресурсы компании и позволяющая

						Лист
						6
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	



обмениваться информацией различного вида. Чтобы обмен информацией между подразделениями банка был эффективным, принято решение использовать виртуальную локальную сеть (VLAN).

VLAN (Virtual Local Area Network) – это функция в роутерах и коммутаторах, позволяющая на одном физическом сетевом интерфейсе (Ethernet, Wi-Fi-интерфейсе) создать несколько виртуальных локальных сетей. VLAN используют для создания логической топологии сети, которая никак не зависит от физической топологии.[2]

Пример VLAN показан на рисунке 1.1.

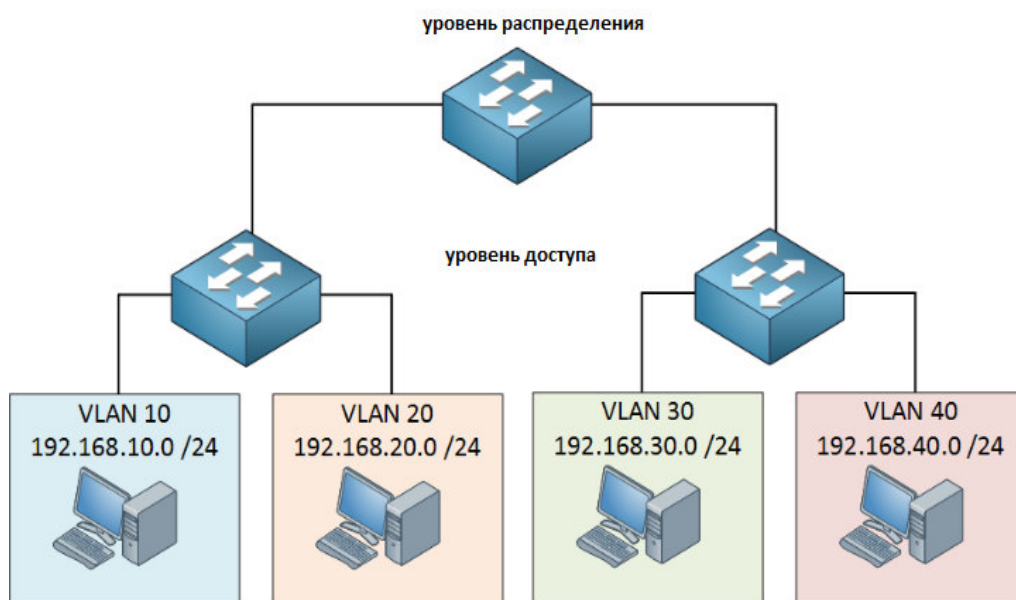


Рисунок 1.1 - Пример VLAN

Виртуальная локальная сеть (VLAN) абстрагирует идею локальной сети; VLAN может содержать подмножество портов на одном коммутаторе или подмножествах портов на нескольких коммутаторах. По умолчанию системы в одной VLAN не видят трафика, связанного с системами на других VLAN в той же сети.

Сети VLAN позволяют сетевым администраторам разбивать свои сети на соответствие функциональным требованиям и требованиям безопасности своих систем без необходимости запуска новых кабелей или существенных

изменений в их текущей сетевой инфраструктуре. VLAN коммерческого банка будет создаваться с учетом рекомендаций IEEE 802.1Q, которые являются стандартом, определяющим понятие и структуру VLAN. Идентификатор или тег VLAN состоит из 12 бит в кадре Ethernet, создавая собственный лимит в 4096 VLAN в локальной сети.

Порты на коммутаторах могут быть назначены одной или нескольким сетям VLAN, что позволяет разделять системы на логические группы. Группы можно выделять по разным признакам: либо по подразделениям банка (кредитный отдел – одна VLAN, служба работы с клиентами – вторая VLAN, и т.п.). Также можно выделять VLAN группам подразделений, например, выявить, с каким подразделением они связаны, и установить правила, как системам в отдельных группах разрешено связываться друг с другом. Такие правила могут изменяться в зависимости от требований к безопасности: от простых и практичных (компьютеры в одной VLAN могут видеть принтер в этой VLAN, но компьютеры за пределами этой VLAN не могут), к сложным (например, компьютеры в торговых отделах не могут взаимодействовать с компьютерами в отделах розничного банковского обслуживания). [3]

### **1.3 Постановка задач проектирования**

Для реализации инфокоммуникационной инфраструктуры Techcombank нужно решить следующие задачи:

1. Выбор сетевых технологий;
2. Разработка схемы организации связи;
3. Выбор и расчет объёма сетевого оборудования;
4. Создание модели сети банка;
5. Исследование параметров сети на основе разработанной модели;
6. Разработка рекомендаций по реализации инфокоммуникационной инфраструктуры банка.

						Лист
					<b>11070006.11.03.02.475.ПЗВК</b>	8
Изм.	Лист	№ докум.	Подпись	Дата		

## **2 РАЗРАБОТКА КОНЦЕПЦИИ РЕАЛИЗАЦИИ ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ БАНКА**

### **2.1 Анализ и описание современных инфокоммуникационных технологий и способов реализации защищённых корпоративных сетей**

Современное общество характеризуется интенсивным участием в процессе информатизации. Информатизация общества - это глобальное социальное явление, которое характеризуется накоплением, обработкой, хранением, передачей и использованием информации. Сегодня информатизация как технико-технологическая база становления информационного общества выступает национальным стратегическим ресурсом, определяющим не только общий уровень социального и культурного развития государства, но и его место в глобальном процессе мирового развития.

#### **Интернет**

Интернет представляет собой глобально подключенную сетевую систему, которая использует стек протоколов TCP/IP для передачи данных через различные типы носителей. Интернет - это сеть глобальных обменов, в том числе частных, общественных, деловых, академических и правительственных сетей, связанных с использованием беспроводных и волоконно-оптических технологий.[4]

#### **Протокол IP**

Протокол Интернета (IP) - это метод или протокол, по которым данные передаются с одного компьютера на другой в в глобальной сети Интернет. Каждый компьютер (хост) в Интернете имеет IP-адрес, который однозначно идентифицирует его со всех других компьютеров в Интернете, что позволяет принимать информацию в виде пакетов именно этому получателю.

IP - протокол без установления соединения, то есть между конечными точками, обменивающимися данными, не существует постоянного соединения.

						Лист
					<b>11070006.11.03.02.475.ПЗВК</b>	9
Изм.	Лист	№ докум.	Подпись	Дата		

Каждый пакет, который проходит через Интернет, рассматривается как независимая единица данных без какого-либо отношения к какой-либо другой единице данных. Пакеты попадают в правильном порядке из-за применения TCP - протокола, ориентированного на соединение, который отслеживает последовательность пакетов в сообщении. В модели взаимодействия открытых систем Open Systems Interconnection (OSI) IP находится на уровне 3 - Сетевом уровне.

В сетях используется версия протокола IP 4 (IPv4), однако также начинает поддерживаться IP-версия 6 (IPv6). IPv6 обеспечивает гораздо более длинные адреса и, следовательно, расширить количество пользователей Интернета. IPv6 включает возможности IPv4, и любой сервер, который может поддерживать пакеты IPv6, также может поддерживать пакеты IPv4. [5]

### **Технологии и стандарты Ethernet**

Ethernet широко применяется для создания локальной сети (LAN). Ethernet является протоколом второго уровня (канального) в стеке TCP/IP. Он описывает, как сетевые устройства могут форматировать данные для передачи на другие сетевые устройства в одном и том же сегменте сети, и как вывести эти данные из сетевого подключения. Он охватывает и уровень 1 (физический уровень), и уровень 2 (уровень канала передачи данных) в модели сетевого взаимодействия OSI. Ethernet определяет два блока передачи, пакет и фрейм. Фрейм включает в себя не только «полезную нагрузку» передаваемых данных, но и адресную информацию, идентифицирующую физические адреса «Управление доступом к среде» (MAC) обоих отправителей и получателей, маркировку VLAN и информацию о качестве обслуживания, а также информацию об исправлении ошибок для обнаружения проблемы в передаче. Каждый кадр упакован в пакет, который прикрепляет несколько байтов информации, используемой при установлении соединения и маркировке, где начинается кадр. [6]

						Лист
						10
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

Информация в сетях Ethernet передается кадрами. Кадры передаются без установления соединения и повторной доставки утерянных или искаженных кадров (проблемы решаются на более высоких уровнях модели OSI). [7]

### **Технология АТМ**

Асинхронный режим передачи (Asynchronous Transfer Mode, АТМ) - это технология, основанная на технике виртуальных каналов. Она предназначена для применения в виде единого универсального транспорта сетей с интегрированным обслуживанием. В АТМ применяется метод коммутации пакетов с асинхронным временным мультиплексированием данных.

Асинхронный режим передачи - это сетевая технология, которая передает данные в пакеты или ячейки фиксированного размера. АТМ использует 53-байтовые ячейки (5 байтов для заголовка адреса и 48 байтов для данных). Ячейки обрабатываются АТМ-коммутатором достаточно быстро, при этом поддерживается скорость передачи данных более 600 Мбит/с. [8]

## **2.2 Выбор сетевых технологий и схемных решений**

Как было отмечено ранее, в проекте будет разработана ЛВС, основанная на структурированной кабельной системе. Наиболее эффективным решением в данном случае является применение Fast Ethernet. Использование для реализации горизонтальной подсистемы элементной базы категории 5е обеспечивает передачу по трактам СКС сигналов всех широко распространенных на практике разновидностей Ethernet, вплоть до его высокоскоростного варианта Gigabit Ethernet 802.3ab. Тем самым предлагаемое решение обеспечивает резерв пропускной способности горизонтальных трактов СКС, достаточный для поддержки функционирования всех известных на момент проектирования и перспективных видов приложений.

						Лист
						11
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

Согласно исходным данным, создаваемая информационно-телекоммуникационная система Techcombank предназначена для передачи конфиденциальной информации.

При создании новой сети предприятия учтены важные факторы:

1) Требуемый размер сети (в настоящее время, в ближайшем будущем и по прогнозу на перспективу). Под размером сети понимается как количество объединяемых в сеть компьютеров, так и расстояния между ними.

В центральном офисе Techcombank подключены к сети 60 компьютеров (минимально), планируется довести численность компьютеров в сети до 100 (максимально). В настоящее время ЛВС занимает 3 этажа, в ближайшем будущем, при увеличении штата сотрудников Techcombank, планируется дальнейшее расширение ЛВС по вертикали.

2) Структура, иерархия и основные части сети (по подразделениям Techcombank, а также по комнатам, этажам и зданиям банка).

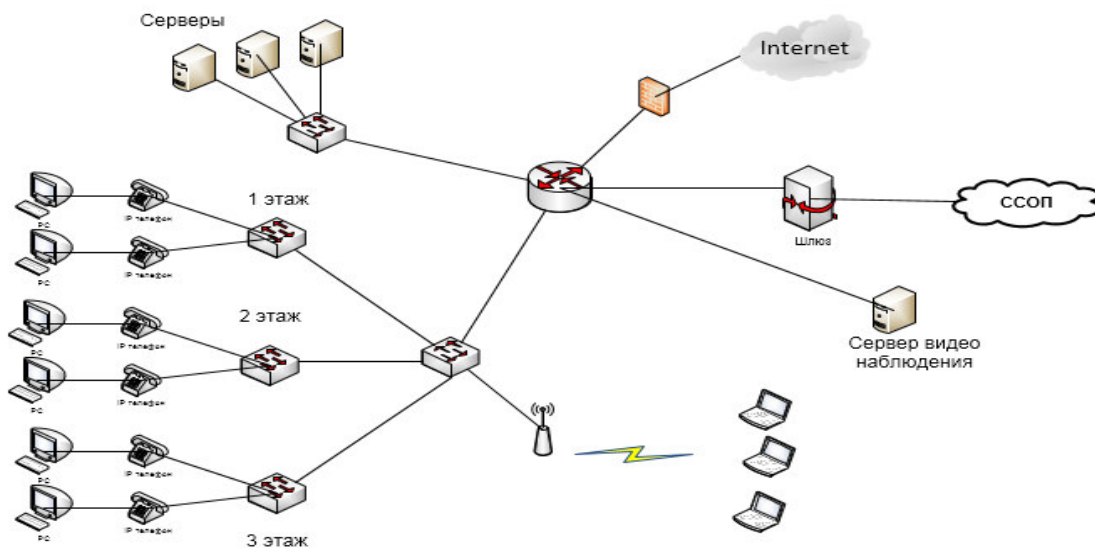


Рисунок 2.1 - Пример общей структура ЛВС организации

Организация занимает три этажа, на первом этаже есть 7 комнат и 1 зал, на втором этаже 7 комнат, на третьем этаже 8 комнат (20 отделов). В этом случае сеть необходимо построить следующим образом.

Компьютеры и IP-телефоны будут объединены между собой коммутаторами. Коммутаторы будут установлены: три на первом этаже, три на втором этаже, два на третьем этаже, они будут размещены в коммутационных узлах каждого этажа.

Общая сеть Techcombank включает три сегмента, объединенные управляемыми коммутаторами. Эти же коммутаторы соединены общим коммутатором, к которому подключен и маршрутизатор (он же файрвол) для подключения к глобальной сети. Серверы располагаются в серверной комнате.

Выбранное решение обеспечивает следующие преимущества:

1) Области коллизий (зоны конфликта) сети будут включать в себя сегменты, расположенные в комнатах каждого отдела, также добавляется сегмент, связывающий коммутатор комнаты с коммутатором этажа.

2) Широковещательные области будут включать все сегменты сети каждого этажа плюс сегмент, связывающий коммутатор с маршрутизатором. Таких широковещательных областей будет три. Области коллизий в данном случае будут включать все сегменты сети каждого отдела плюс сегмент, соединяющий коммутатор отдела и коммутатор этажа. Таких областей коллизий всего три. В единственную широковещательную область войдет вся сеть организации Techcombank.

3) Анализ основных направлений и интенсивности информационных потоков в сети (в настоящее время, в ближайшем будущем и в дальней перспективе) показал, что стремительного увеличения количества сотрудников и сетевых приложений не будет. Характер передаваемой по сети информации - данные, оцифрованная речь, изображения. Виды трафика непосредственно сказываются на требуемой скорости передачи (до нескольких сотен Мбит/с для высокоскоростных приложений).

4) Технические характеристики оборудования (компьютеров, адаптеров, кабелей, репитеров, концентраторов, коммутаторов) и его стоимость

						Лист
						13
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

выбирается, исходя из требований к эффективности обмена данными между подразделениями Techcombank.

5) Предусмотрены возможности прокладки кабельной системы в помещениях и между ними, а также меры обеспечения целостности кабеля.

6) Обеспечивается качественное обслуживание сети и контроль ее безотказности и безопасности.

7) Требования к программным средствам по допустимому размеру сети, скорости, гибкости, разграничению прав доступа, стоимости, по возможностям контроля обмена информацией и т.д. зависят от вида сервисов и особенностей информации, передаваемой между подразделениями Techcombank.

8) Обеспечивается возможность подключения к глобальным или к другим локальным сетям.

Таким образом, принятое проектное решение позволит создать высокоэффективную, гибкую, управляемую сетевую инфраструктуру, адаптированную под особенности информационного обмена в банке Techcombank.

### **2.3 Выбор типа трафика в корпоративной сети и расчет нагрузок**

Данные в разрабатываемой ЛВС будут инкапсулироваться в пакеты, которые обеспечивают сетевую нагрузку. Сетевой трафик является основным компонентом для измерения нагрузки, управления и моделирования.

Управление сетевым трафиком важная задача, решение которой основано на применении процедуры приоритизации, управления или снижения сетевого трафика в зонах с перегрузками.

Правильный анализ сетевого трафика обеспечивает организацию сетевой безопасности, так как необычный объем трафика в сети является возможным признаком атаки. Отчеты о сетевом трафике дают ценную информацию о

						Лист
					<b>11070006.11.03.02.475.ПЗВК</b>	14
Изм.	Лист	№ докум.	Подпись	Дата		



предотвращении таких атак. [9]

Основными видами информации, передаваемой по проектируемой сети Techcombank, является голосовая информация (переговоры сотрудников банка между собой и с клиентами), а также различные данные. Первый вид относится к трафику реального времени, поэтому важно обеспечить быстроедействие сети и минимальные задержки. Это обеспечивается применением современных решений на базе компьютерной телефонии. В проекте принято решение для передачи голоса использовать VoIP.

VoIP (передача голоса по IP) - это передача голосового и мультимедийного контента по сетям с использованием интернет-протокола (IP). Конечные точки VoIP включают в себя выделенные настольные VoIP-телефоны, приложения софтфона, работающие на ПК и мобильных устройствах, и браузеры с поддержкой WebRTC.

VoIP использует кодеки для инкапсуляции аудио в пакеты данных, передачи пакетов по сети IP и инкапсуляции пакетов обратно в аудио на другом конце соединения. Исключая использование сетей с коммутацией каналов для голоса, VoIP снижает затраты на сетевую инфраструктуру, такое решение позволит в Techcombank использовать единую сеть передачи голоса и данных. VoIP также поддерживает обратную связь с отказоустойчивостью сетей на основе IP, обеспечивая быстрый переход на другой ресурс в случае сбоев и избыточных связей между конечными точками и сетями.

Терминалы VoIP обычно используют стандартные кодеки Международного союза электросвязи (МСЭ), такие как G.711, который является стандартом для передачи несжатых пакетов или G.729, который является стандартом для сжатых пакетов. Многие поставщики оборудования также используют собственные кодеки. При сжатии качество голоса может ухудшиться, но сжатие снижает требования к пропускной способности. VoIP обычно поддерживает неответную связь по протоколу ITU T.38 для отправки факсов по сети VoIP или IP в режиме реального времени. [10]

						Лист
						15
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

Исходные данные для расчета нагрузок приведены в таблице 2.1.

**Таблица 2.1 - Значения параметров**

Параметр	Обозначение	Значение
1. Количество сетевых узлов для подключения абонентов	FN	3 (коммутаторы по 24 порта)
2. Число абонентов сети:	NS	61
3. Отношение длины заголовка IP пакета к его общей длине во входящем потоке	OHD	10%
4. Отношение длины заголовка IP пакета к его общей длине в исходящем потоке	OHU	15%
5. Процент абонентов Triply Play: - находящихся в сети в ЧНН; - одновременно принимающих или передающих данные	DAAF  DPAF	80%  40%
6. Услуга передачи данных: 6.1 Пропускная способность сети для передачи данных к абоненту: -средняя пропускная способность; -пиковая пропускная способность; 6.2 Пропускная способность сети для передачи данных от абонента: - средняя пропускная способность; - пиковая пропускная способность;	  ADBS PDBS  AUBS PUBS	  5 Мбит/с 10 Мбит/с  5 Мбит/с 10 Мбит/с

### Расчет трафика передачи данных

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 (2.1):

					<b>11070006.11.03.02.475.ПЗВК</b>	Лист
Изм.	Лист	№ докум.	Подпись	Дата		16

$$AS = TS * DAAF, \text{ абонентов} \quad (2.1)$$

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

Число абонентов на одном сетевом узле определяется по формуле (2.2):

$$TS = NS/FN, \text{ абонентов.} \quad (2.2)$$

где  $NS$  – общее число абонентов,  $FN$  – количество оптических сетевых узлов.

$$AS = (61/3)*0.8 = 16 \text{ абонентов.}$$

В час наибольшей нагрузки в сети находится 16 человек с одного сетевого узла, охватывающего 20 абонентов.

Средняя пропускная способность для приема данных составит (2.3):

$$BDDA = (AS * ADBS) * (1 + OHD), \text{ Мбит/с,} \quad (2.3)$$

где  $AS$  - количество активных абонентов,  $ADBS$  – средняя скорость приема данных,  $OHD$  – отношение длины заголовка IP пакета к его общей длине во входящем потоке.

$$BDDA = (16 * 5) * (1 + 0.1) = 88 \text{ Мбит/с}$$

Средняя пропускная способность для передачи данных (2.4):

$$BUDA = (AS * AUBS) * (1 + OHU), \text{ Мбит/с,} \quad (2.4)$$

где  $AS$  - количество активных абонентов,  $AUBS$  – средняя скорость передачи данных,  $OHU$  – отношение длины заголовка IP пакета к его общей длине в исходящем потоке.

					Лист
					17
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>

$$BUDA = (16 * 5) * (1 + 0.15) = 92 \text{ Мбит/с}$$

Количество абонентов, передающих или принимающих данные в течение некоторого короткого промежутка времени, определяют пиковую пропускную способность сети. Количество этих абонентов в час наибольшей нагрузки определяется коэффициентом Data Peak Activity Factor по формуле (2.5):

$$PS = AS * DPAF, \text{ аб}, \quad (2.5)$$

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

$$PS = 16 * 0.7 = 11 \text{ аб.}$$

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 (2.6):

$$BDDP = (PS * PDBS) * (1 + OHD), \text{ Мбит/с}, \quad (2.6)$$

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

$$BDDP = (11 * 10) * (1 + 0.1) = 121 \text{ Мбит/с}$$

Пиковая пропускная способность для передачи данных в ЧНН (2.7):

$$BUDP = (PS * PUBS) * (1 + OHU), \text{ Мбит/с}, \quad (2.7)$$

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

$$BUDP = (11 * 10) * (1 + 0.15) = 126.5 \text{ Мбит/с}$$

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

						Лист
						18
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

Для проектирования сети необходимо использовать максимальное значение полосы пропускания среди пиковых и средних значений для исключения перегрузки сети (2.8, 2.9):

$$BDD = \text{Max} [BDDA; BDDP], \text{ Мбит/с}, \quad (2.8)$$

$$BDU = \text{Max} [BUDA; BUDP], \text{ Мбит/с}, \quad (2.9)$$

где BDD – пропускная способность для приема данных, BDU – пропускная способность для передачи данных.

$$BDD = \text{Max} [88; 121] = 121 \text{ Мбит/с},$$

$$BDU = \text{Max} [92; 126.5] = 126.5 \text{ Мбит/с}$$

Общая пропускная способность для приема и передачи данных, необходимая для нормального функционирования оптического сетевого узла, составит (2.10):

$$BD = BDD + BDU, \text{ Мбит/с}, \quad (2.10)$$

где BDD – максимальная пропускная способность для приема данных, BDU – максимальная пропускная способность для передачи данных..

$$BD = 121 + 126.5 = 247.5 \text{ Мбит/с}$$

Таким образом, для передачи данных между абонентами сети на одном сетевом узле нужна полоса пропускания 247.5 Мбит/с.

### **Расчет трафика телефонии**

Исходные данные для расчета:

- количество источников – абоненты, использующие терминалы SIP и подключаемые в пакетную сеть на уровне мультисервисного абонентского концентратора,  $N_{\text{SIP}} = 35$  абонентов;
- тип кодека в планируемом к внедрению оборудовании, G.729A;
- длина заголовка IP пакета, 58 байт.

						Лист
					<b>11070006.11.03.02.475.ПЗВК</b>	19
Изм.	Лист	№ докум.	Подпись	Дата		

Полезная нагрузка голосового пакета G.729 CODEC составит по формуле (2.11):

$$Y_{\text{полезн}} = \frac{t_{\text{звуч.голос}} * v_{\text{кодирования}}}{8 \text{ бит/байт}}, \text{ байт} \quad (2.11)$$

где  $t_{\text{звуч.голос}}$  - время звучания голоса,  $v_{\text{кодирования}}$  - скорость кодирования речевого сигнала.

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

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

Общий размер голосового пакета составит согласно по формуле (2.12):

$$V_{\text{пакета}} = L_{\text{Eth}} + L_{\text{IP}} + L_{\text{UDP}} + L_{\text{RTP}} + Y_{\text{полезн}}, \text{ байт}, \quad (2.12)$$

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

$$V_{\text{пакета}} = 14 + 32 + 8 + 16 + 20 = 90 \text{ байт}$$

Использование кодека G.729A позволяет передавать через шлюз по 50 пакетов в секунду, исходя из этого, полоса пропускания для одного вызова (2.13):

$$\text{ППр}_1 = V_{\text{пакета}} * 8 \text{ бит/байт} * 50_{\text{pps}}, \text{ кбит/с} \quad (2.13)$$

где  $V_{\text{пакета}}$  – размер голосового пакета.

$$\text{ППр}_1 = 90 * 8 * 50 = 35 \text{ кбит/с}$$

В проектируемой ЛВС Techcombank устанавливается точка присутствия, в которой имеется 35 голосовых портов. С помощью средств подавления пауз

					<b>11070006.11.03.02.475.ПЗВК</b>	Лист
Изм.	Лист	№ докум.	Подпись	Дата		20

обычный голосовой вызов можно сжать примерно на 50 процентов (по самым консервативным оценкам – 30%). Исходя из этого, необходимая полоса пропускания WAN для точки присутствия составит согласно по формуле (2.14):

$$\text{ППр}_{WAN} = \text{ППр}_1 * N_{SIP} * VAD, \text{ кбит/с} \quad (2.14)$$

где  $\text{ППр}_1$  – полоса пропускания для одного вызова,  $N_{SIP}$  – количество голосовых портов в точке присутствия, [шт], VAD (Voice Activity Detection) – коэффициент механизма идентификации пауз (0,7).

$$\text{ППр}_{WAN} = 35 * 35 * 0.7 = 857.5 \text{ кбит/с}$$

Для предоставления услуги IP-телефония на одном сетевом узле доступа необходима полоса пропускания 857.5, кбит/с

Как показал расчет, в точках агрегации (на этажах здания банка) необходимо использовать FastEthernet, на уровне ядра сети – GigabitEthernet.

					Лист
					21
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>

# 3 РАЗРАБОТКА КОРПОРАТИВНОЙ СЕТИ СВЯЗИ ЦЕНТРАЛЬНОГО ОФИСА БАНКА И ТРАНСПОРТНОГО СЕГМЕНТА СЕТИ

## 3.1 Проектирование сети связи центрального офиса

На основе выбранной технологии разработана сетевая инфраструктура, обеспечивающая возможность обмена данными между подразделениями Techcombank. Для выбора оптимального решения (с точки зрения быстродействия и полосы пропускания), необходимо разработать модель сети, и оценить все «узкие места» перед окончательным выбором сетевой инфраструктуры.

Для начала создадим топологию сети Techcombank в среде имитационного моделирования Cisco Packet Tracer, изображенную на рисунке 3.1.

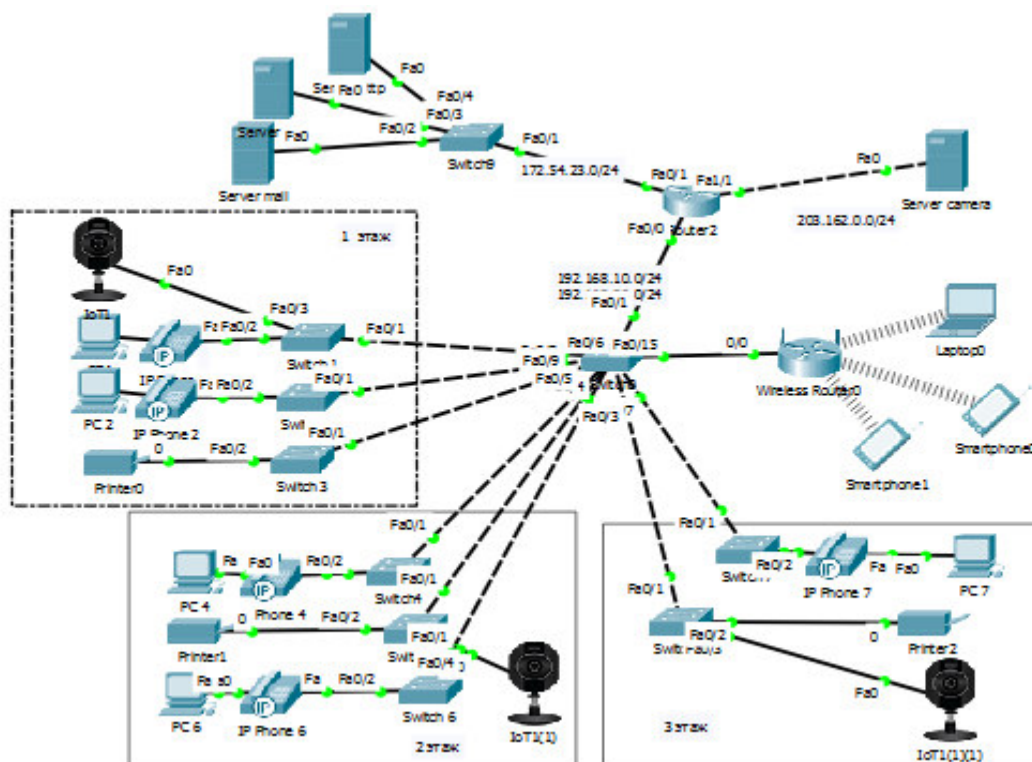


Рисунок 3.1 - Топология сети в среде имитационного моделирования Packet Tracer



Для всех сетевых элементов разработана IP-адресация, представленная в таблице 3.1.

**Таблица 3.1 - Таблица адресации**

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Route	Fa0/0.10	192.168.10.1	255.255.255.0	N/A
	Fa0/0.20	192.168.20.1	255.255.255.0	N/A
	Fa0/1	172.54.23.1	255.255.255.252	N/A
	Fa1/0		255.255.255.0	N/A
	Fa1/1	203.162.0.1	255.255.255.0	N/A
Sw 0	Vlan 99	192.168.99.1	255.255.255.0	N/A
PC 1	N/A	192.168.10.10	255.255.255.0	192.168.10.1
PC 2	N/A	192.168.10.11	255.255.255.0	192.168.10.1
Camera 1	N/A	192.168.10.12	255.255.255.0	192.168.10.1
Printer 1	N/A	192.168.10.13	255.255.255.0	192.168.10.1
PC 4	N/A	192.168.10.14	255.255.255.0	192.168.10.1
PC 6	N/A	192.168.10.15	255.255.255.0	192.168.10.1
Camera 2	N/A	192.168.10.16	255.255.255.0	192.168.10.1
Printer 2	N/A	192.168.10.17	255.255.255.0	192.168.10.1
PC 7	N/A	192.168.10.18	255.255.255.0	192.168.10.1
Camera 3	N/A	192.168.10.19	255.255.255.0	192.168.10.1
Printer 3	N/A	192.168.10.20	255.255.255.0	192.168.10.1
Ip phone 1	N/A	192.168.20.10	255.255.255.0	192.168.20.1
Ip phone 2	N/A	192.168.20.11	255.255.255.0	192.168.20.1
Ip phone 4	N/A	192.168.20.13	255.255.255.0	192.168.20.1
Ip phone 6	N/A	192.168.20.15	255.255.255.0	192.168.20.1
Ip phone 7	N/A	192.168.20.16	255.255.255.0	192.168.20.1
Wireless router	N/A	192.168.10.3	255.255.255.0	192.168.10.1
Laptop	N/A	192.168.0.101	255.255.255.0	192.168.0.1
Sm.phone 1	N/A	192.168.0.102	255.255.255.0	192.168.0.1
Sm.phone 2	N/A	192.168.0.103	255.255.255.0	192.168.0.1
Server Http	N/A	172.54.23.8	255.255.255.0	172.54.23.1
Server Mail	N/A	172.54.23.4	255.255.255.0	172.54.23.1
Server Dns	N/A	172.54.23.6	255.255.255.0	172.54.23.1
Server Camera	N/A	203.162.0.2	255.255.255.0	203.162.0.1

Коммутатор 1 до коммутатора 9, обработка интернет-протокола отключена.

Организация VLAN будет сделана на основе программного обеспечения, вместо физического перемещения устройств. На устройствах Cisco протокол VTP (VLAN Trunking Protocol) предусматривает VLAN-домены для упрощения администрирования. VTP также выполняет «чистку» трафика, направляя VLAN трафик только на те коммутаторы, которые имеют целевые VLAN-порты. Cisco коммутаторы в основном используют протокол ISL (Inter-Switch Link) для обеспечения совместимости информации.

Native VLAN - каждый порт имеет параметр, названный постоянный виртуальной идентификацией (Native VLAN), который определяет VLAN, назначенный получить не теговые кадры.

Приведем необходимые команды для настройки сетевых устройств.

### **Настройка Switch и Router**

- Используя протокол VTP для Switch 0
  - Switch(config)#vtp domain TECHCOMBANK
  - Changing VTP domain name from NULL to TECHCOMBANK
  - Switch(config)#vtp password 123
  - Setting device VLAN database password to 123
  - Switch(config)#vtp mode server
  - Device mode already VTP SERVER.
- Используя протокол VTP для Switch 1 до 8
  - Switch(config)#vtp domain TECHCOMBANK
  - Changing VTP domain name from NULL to TECHCOMBANK
  - Switch(config)#vtp password 123
  - Setting device VLAN database password to 123
  - Switch(config)#vtp mode client
  - Setting device to VTP CLIENT mode.
- Для Switch1 до Switch8 нужно назначить все присутствующие в сети vlans
  - Switch(config)#vlan 10

- Switch(config-vlan)#name data
- Switch(config-vlan)#vlan 20
- Switch(config-vlan)#name voice
- Switch(config-vlan)#vlan 99
- Switch(config-vlan)#name management
- Switch(config-vlan)#exit

• Далее для каждого используемого интерфейса определим свои параметры

- Switch(config)#interface fastEthernet 0/1
- Switch(config-if)#switchport mode access
- Switch(config-if)#switchport access vlan 10
- Switch(config-if)#switchport voice vlan 20
- Switch(config-if)#exit

**Настройка trunk портов следующая**

- Switch(config)#interface fastEthernet 0/1
- Switch(config-if)#switchport mode trunk

Листинг настройки всех коммутаторов представлен в Приложении А.

**Создание логического подинтерфейса для VLAN 10 на Router:**

- Router>enable
- Router#configure terminal
- Router(config-if)#no shutdown
- Router(config)#interface fastEthernet 0/0.10
- Router(config-subif)#encapsulation dot1Q 10
- Router(config-subif)#ip address 192.168.10.1 255.255.255.0
- Router(config-subif)#exit

Листинг настройки всех логических подинтерфейсах на Router0 представлен в Приложении Б.

**Настройка протокола VTP**

VTP, который доступен с продуктами Cisco Packet Tracer, обеспечивает эффективные способы отправки VLAN через каждый коммутатор. Существует также опция обрезки VLAN, которая позволит избежать отправки трафика

						Лист
						25
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

через некоторые коммутаторы. Пользователи могут сделать эти системы обрезкой подходящей или обрезкой неприемлемой.

Одна из концепций в VTP заключается в том, что сети большего масштаба, возможно, должны быть ограничены, с точки зрения которых коммутаторы будут выступать в качестве серверов VLAN. VTP предлагает различные варианты восстановления после сбоя или для эффективного обслуживания избыточного сетевого трафика. [11]

Настройка в среде имитационного моделирования Packet Tracer сделана следующим образом:

- Switch(config)#vtp domain TECHCOMBANK
- Changing VTP domain name from NULL to TECHCOMBANK
- Switch(config)#vtp password 123
- Setting device VLAN database password to 123
- Switch(config)#vtp mode server
- Device mode already VTP SERVER.

### **Настройка HTTP сервера**

HTTP - Протокол передачи гипертекста. HTTP-сервер - это реализация этого протокола в части программного обеспечения.

Протокол определяет, как должна запрашиваться информация и как формируются ответы, поэтому присутствуют два важных участника: HTTP-клиент (браузер) и HTTP-сервер.

HTTP-сервер «обслуживает» контент, расположенный на сервере, включая HTML, изображения, флеш-память и любые связанные с ними файлы. Сервер не ограничивается статическим контентом сервера, он также обслуживает динамический контент, сгенерированный из базы данных или аналогичный.[12]

Для настройки HTTP сервера необходимо:

- Включить на сервере поддержку HTTP сервиса в программе Packet Tracer;

- Заполнить “Default Page Content(index.html)” в программе Packet Tracer, которая будет являться стартовой странице HTTP сервера;
- Указать IP адрес и маску подсети сервера;
- Указать шлюз, через который сервер соединен с остальной сетью.

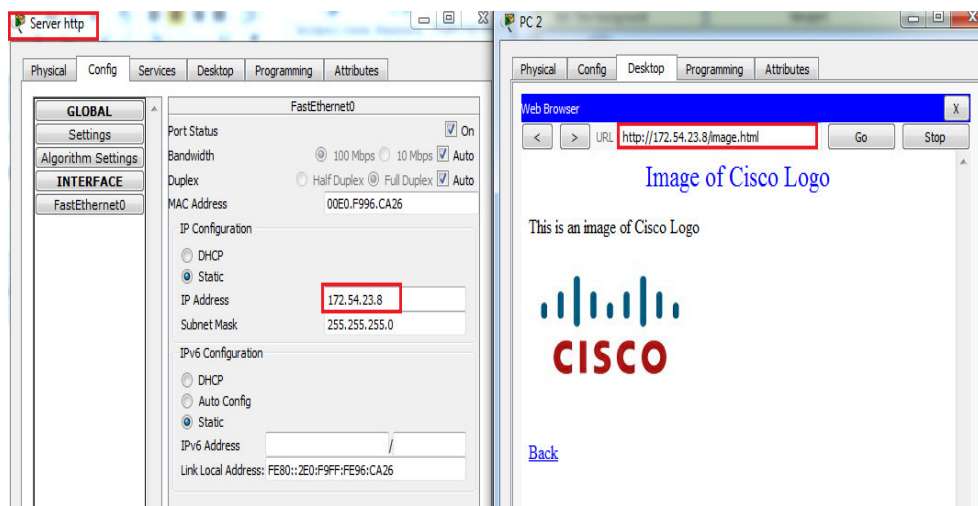


Рисунок 3.2 – Пример настройки HTTP сервера

### Настройка MAIL сервера

Почтовый сервер - это компьютерный эквивалент почтового менеджера. При отправлении письма происходит сложная серия переходов между почтовыми серверами. Почтовые серверы можно разделить на две основные категории: серверы исходящей почты и входящие почтовые серверы. Серверы исходящей почты известны как SMTP или Simple Mail Transfer Protocol, серверы. Входящие почтовые серверы представлены в двух основных вариантах. POP3 или Post Office Protocol, версия 3, серверы наиболее известны для хранения отправленных и полученных сообщений на локальных жестких дисках ПК. IMAP или Internet Message Access Protocol, серверы всегда хранят копии сообщений на серверах. [13]

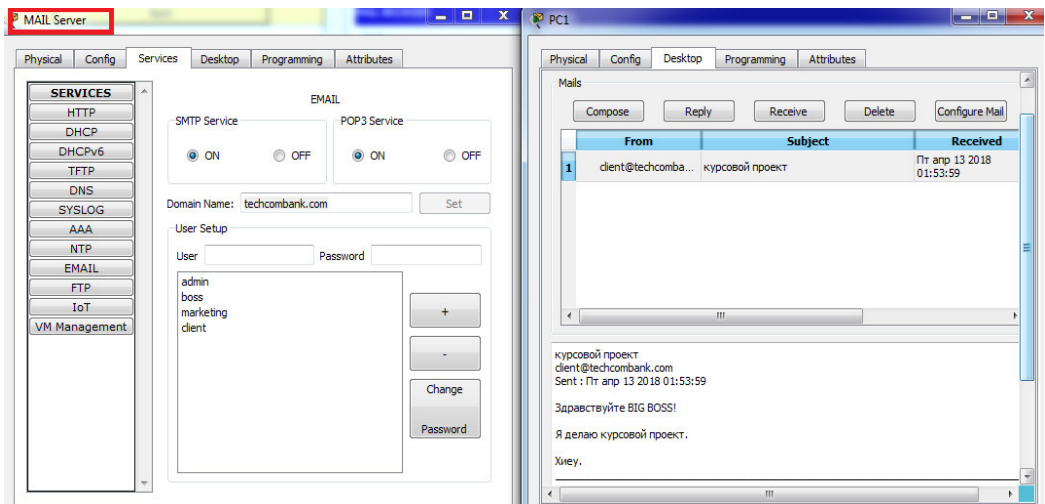


Рисунок 3.3 – Пример MAIL сервера

### Настройка DNS сервера

DNS-сервер является основной частью инфраструктуры DNS (доменной системы). Здесь хранятся все IP-адреса и их имена хостов, и они используются для разрешения любых вызовов пользователей для доступа к определенному веб-сайту, устройству или любой другой сетевой системе, использующей IP-адрес. DNS-сервер используется всякий раз, когда пользователь вводит адрес или URL-адрес хоста в свою адресную строку. [14]

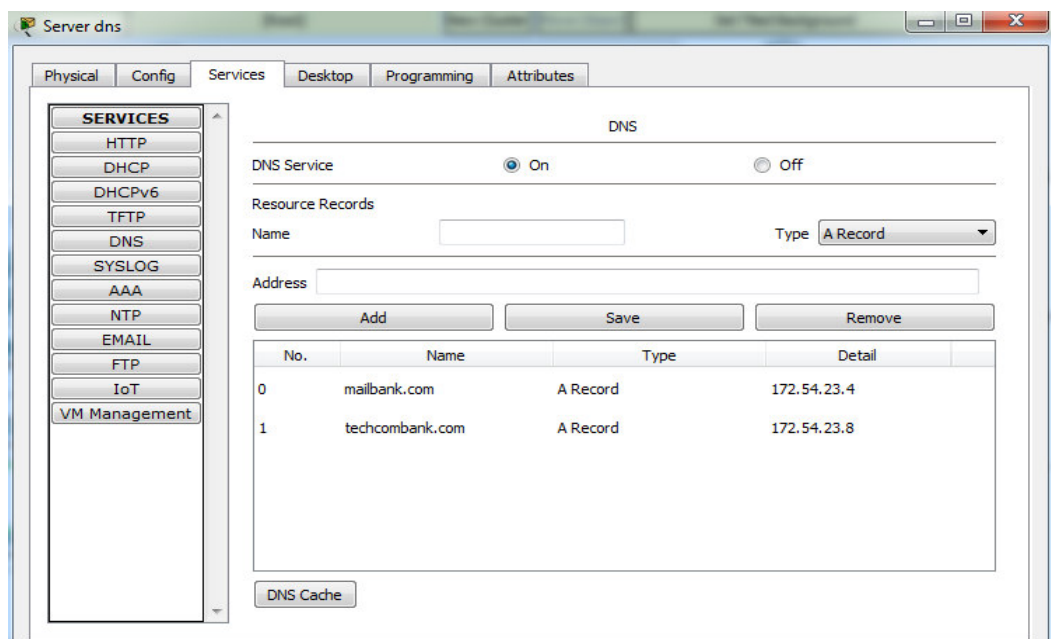


Рисунок 3.4 – Пример DNS сервера

## Настройка DHCP сервиса

DHCP-сервер - это сетевой сервер, который автоматически предоставляет и назначает клиентским устройствам IP-адреса, шлюзы по умолчанию и другие сетевые параметры. Он использует для ответа на широковещательные запросы клиентов протокол конфигурации динамического хоста или DHCP. DHCP-серверы назначают каждому клиенту уникальный динамический IP-адрес, который изменяется, когда срок аренды клиента для этого IP-адреса истек.

Лучшим подходом, чем попытка использовать DHCP на маршрутизаторе / коммутаторе, является использование централизованного DHCP-сервера. Это особенно справедливо для сетевых сред, которые требуют одновременной поддержки как DHCP для IPv4, так и DHCP для IPv6. Практически все поставщики серверов DHCP поддерживают оба протокола, поэтому можно использовать один и тот же интерфейс управления для IPv4 и IPv6. [15]

### Настройка DHCP

Настройка в среде имитационного моделирования Packet Tracer выглядит следующим образом:

- Router(config)# ip dhcp pool 10
- Router(dhcp-config)#default-router 192.168.10.1
- Router(dhcp-config)#network 192.168.10.0 255.255.255.0
- Router(dhcp-config)#exit

Листинг полной настройки DHCP представлен в Приложении В.

### Настройка точки доступа WiFi

Wi-Fi-соединение устанавливается с помощью беспроводного адаптера для создания областей вблизи беспроводного маршрутизатора, которые подключены к сети и позволяют пользователям получать доступ к интернет-услугам. После настройки WiFi обеспечивает беспроводное подключение к устройствам, используемым сотрудниками банка. Компьютер на рабочем месте сотрудника должен содержать беспроводной адаптер, который преобразует данные в радиосигнал. Этот же сигнал будет передаваться через антенну в

						Лист
					<b>11070006.11.03.02.475.ПЗВК</b>	29
Изм.	Лист	№ докум.	Подпись	Дата		

декодер. После декодирования данные будут отправляться в Интернет через проводное Ethernet-соединение.

Беспроводная сеть будет передавать на частотном уровне 2,4 ГГц или 5 ГГц для адаптации к количеству данных, которые отправляются сотрудниками банка. [16]

### **Настройка zone-based policy firewall**

Начиная с версии IOS 12.4, в маршрутизаторах появилась функция Zone-Based Policy Firewall, позволяющая производить настройку правил межсетевого экрана. Эта функция позволяет назначить интерфейсам маршрутизатора зоны безопасности и установить правила взаимодействия между ними. [17]

Конфигурирование Zone-Based Policy Firewall заключается в выполнение следующих шагов:

- 1) назначить зоны межсетевого экрана;
- 2) определить возможность прохождения сетевого трафика между зонами;
- 3) включить существующие сетевые интерфейсы в созданные зоны;
- 4) определить классы, к которым будут применяться политики для пересечения пары зон;
- 5) определить политики для пар зон, регламентирующие производимые действия над проходящим сетевым трафиком;
- 6) применить политики для выбранных пар зон.

## **3.2 Проектирование транспортной инфраструктуры для обмена данными между филиалами банка**

Для обеспечения защищенного обмена данными между филиалами Techcombank принято решение использовать виртуальную частную сеть. Виртуальная частная сеть (VPN) - это зашифрованное соединение через

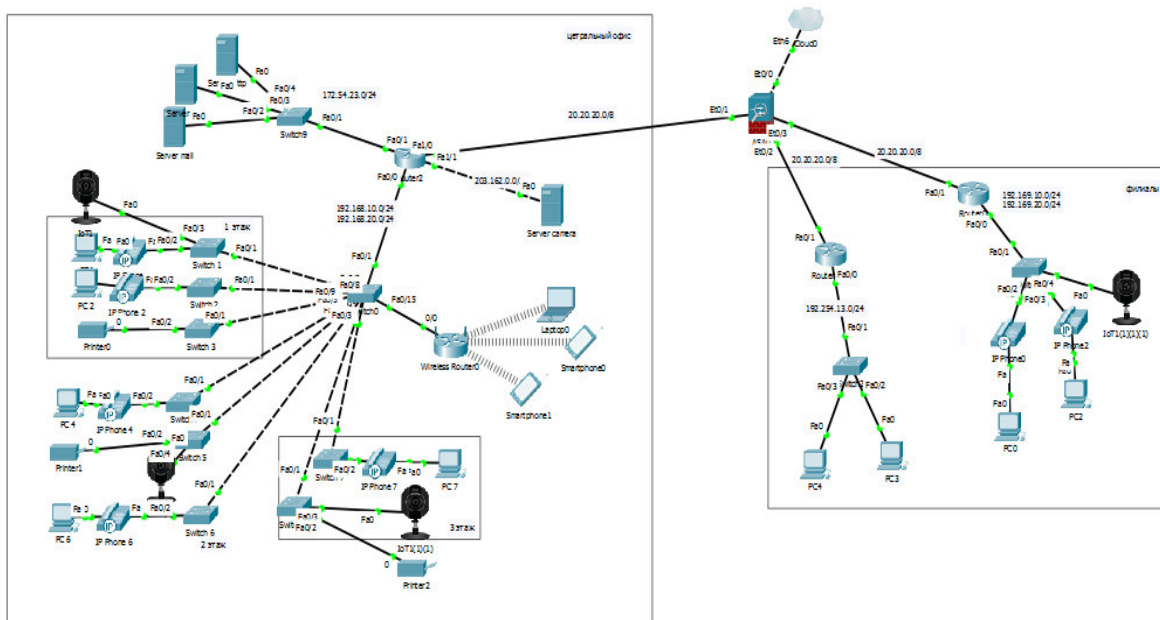
						Лист
						30
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	



Интернет от устройства к сети. Зашифрованное соединение помогает обеспечить безопасную передачу конфиденциальных данных. Это предотвращает перехватывание и несанкционированный доступ к трафику, и позволяет пользователю проводить удаленную работу. Технология VPN широко используется в корпоративных средах. VPN расширяет корпоративную сеть через зашифрованные соединения, выполненные через Интернет. Поскольку трафик зашифрован между устройством и сетью, трафик остается закрытым по мере его перемещения. Сотрудник может работать за пределами офиса и все же надежно подключаться к корпоративной сети. Даже смартфоны и планшеты могут подключаться через VPN.

Удаленный доступ обеспечивает безопасный способ удаленного подключения пользователей и устройств к корпоративной сети Techcombank. Он включает технологию VPN, которая использует надежные способы аутентификации пользователя или устройства.

На рисунке 3.5 показан пример использования VPN между подразделениями Techcombank.



**Рисунок 3.5 - Пример использования VPN**

Проектируемая сеть VPN обеспечит:

1. Безопасность - сеть должна быть устойчива к воздействиям извне.

2. Отказоустойчивость - сеть можно быстро восстановить в случае повреждения, либо имеются пути резервирования.

3. Масштабируемость - к сети можно подключать новых участников/сети без перерыва в работе сети.

4. Управляемость - сеть позволяет оперативно изменять настройки в любое время.

Если указанные выше принципы соблюдены, то сеть VPN позволяет получить следующие преимущества:

1. Информация, передаваемая по сети защищена от считывания и внешнего воздействия.

2. Участники соединения могут находиться в любой точке мира, главное чтобы у них был доступ к Интернет.

3. Упрощенная сетевая топология.

4. Повышенная продуктивность.

5. Существенное снижение расходов на инфраструктуру сети.

6. Низкое время развертывания сети даже для самых удаленных объектов.

Существует несколько механизмов организации VPN соединений: межсетевой экран (Firewall), шифрование, использование протокола IPSec, применение на сети специального сервера AAA. [18]

**Межсетевой экран** или **Firewall** представляет собой барьер, который ограничивает сеть пользователя от остальной публичной сети. Он преграждает доступ извне для пользователей, не имеющих на это право, а разрешает только по заранее установленному списку. Таким образом, Firewall позволяет разграничивать доступ и тем самым создавать виртуальную сеть с другими пользователями и сетями, у которых на вход в общедоступную сеть также стоит подобная защита. Межсетевой экран может быть организован программно – в виде ПО установленного на пограничном маршрутизаторе либо ПК пользователя, либо аппаратно в виде отдельного элемента сети. Обычно

						Лист
						32
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

Firewall используется совместно с другими средствами защиты, например, шифрованием. [19]

В VPN компьютеры на каждом конце туннеля шифруют данные, входящие в туннель, и расшифровывают их на другом конце. Однако для VPN требуется больше, чем просто пара ключей для применения шифрования. VPN-соединение между сайтами может использовать протокол защиты протокола IP (IPSec) или инкапсуляцию общей маршрутизации (GRE). GRE обеспечивает основу для того, как упаковать данные для передачи по интернет-протоколу (IP). Эта структура включает информацию о том, какой тип пакета инкапсулируется, и о связи между отправителем и получателем. [20]

IPSec - широко используемый протокол для обеспечения безопасности трафика в сетях IP, включая Интернет. IPSec может шифровать данные между различными устройствами, включая маршрутизатор, межсетевой экран, рабочий стол. IPSec состоит из двух под-протоколов, которые предоставляют инструкции, необходимые VPN для защиты своих пакетов:

- Инкапсулированная полезная нагрузка безопасности (ESP) шифрует полезную нагрузку пакета (данные, которые он транспортирует) с симметричным ключом.
- Заголовок проверки подлинности (AH) использует операцию хэширования в заголовке пакета, чтобы помочь скрыть определенную информацию о пакете (например, идентификатор отправителя) до тех пор, пока он не достигнет своего адресата.

Сетевые устройства могут использовать IPSec в одном из двух режимов шифрования. В транспортном режиме устройства шифруют данные, перемещающиеся между ними. В туннельном режиме устройства создают виртуальный туннель между двумя сетями. VPN используют IPSec в туннельном режиме с совместной работой IPSec ESP и IPSec AH. [21]

Еще один способ создания VPN - это установка специального сервера, который получил название аутентификация, авторизация и учет (AAA). Он

						Лист
					<b>11070006.11.03.02.475.ПЗВК</b>	33
Изм.	Лист	№ докум.	Подпись	Дата		

используется для интеллектуального контроля доступа к компьютерным ресурсам, обеспечения соблюдения политики безопасности, использования аудита и предоставления информации, необходимой для выставления счетов за услуги. Эти комбинированные процессы считаются важными для эффективного управления сетью и обеспечения безопасности.

Таким образом, независимо от способа организации, VPN - это эффективный способ создания защищенной инфокоммуникационной сети, не требующий инвестирования значительных финансовых средств и предоставляющий все преимущества выделенной независимой сети.

Листинг полной настройки VPN представлен в Приложении Д.

### 3.3 Расчет объёма оборудования

В качестве производителя кабелей и оборудования СКС выбрана Вьетнамская компания изготовитель «Huynh Chan Duy» [26]. Структурированная кабельная система банка спроектирована в соответствии со стандартами СКС, которые регламентируют структуру СКС, а именно: совместимость компонентов и систему маркировки. [27, 28]

Схематичный план СКС здания показан на рисунке 3.6. Планируется организация горизонтальной подсистемы, охватывающей офисы каждого этажа, и вертикальной подсистемы, объединяющей горизонтальные сегменты и позволяющей выполнить ввод магистрального кабеля от провайдера в здание банка.

						Лист
						34
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	



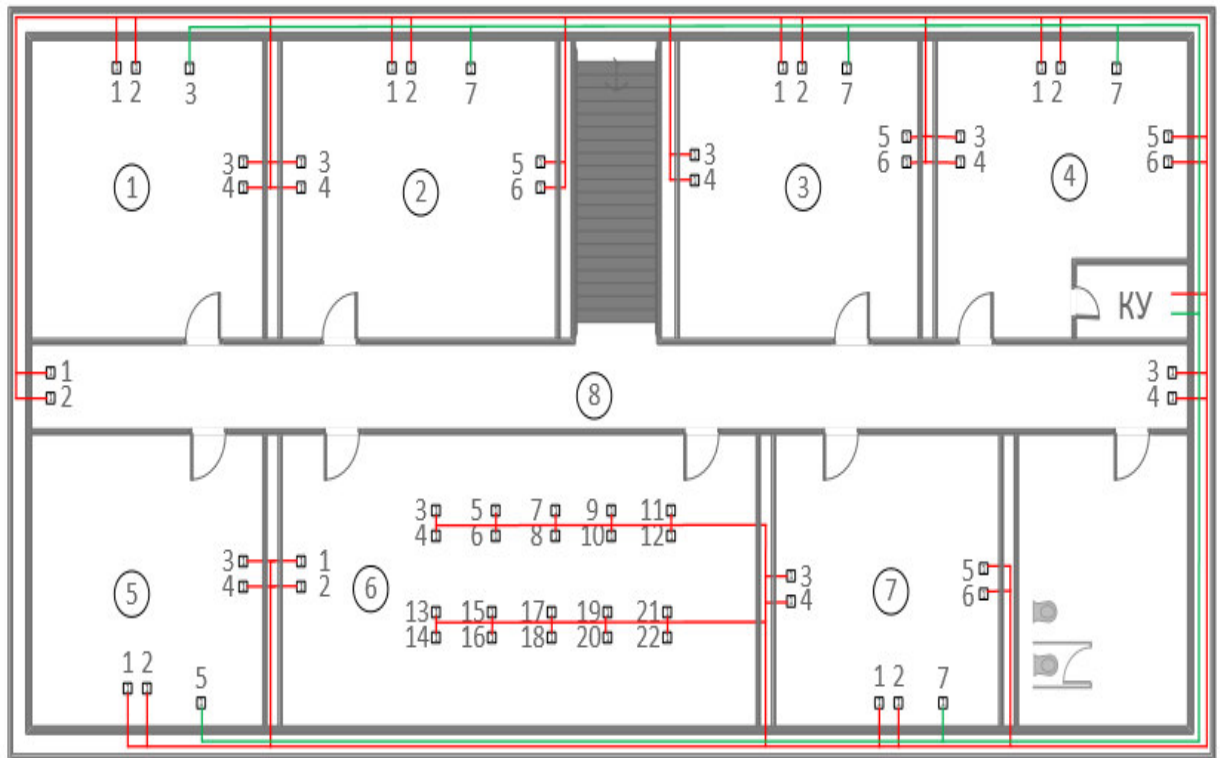


Рисунок 3.8 – План СКС здания на втором этаже

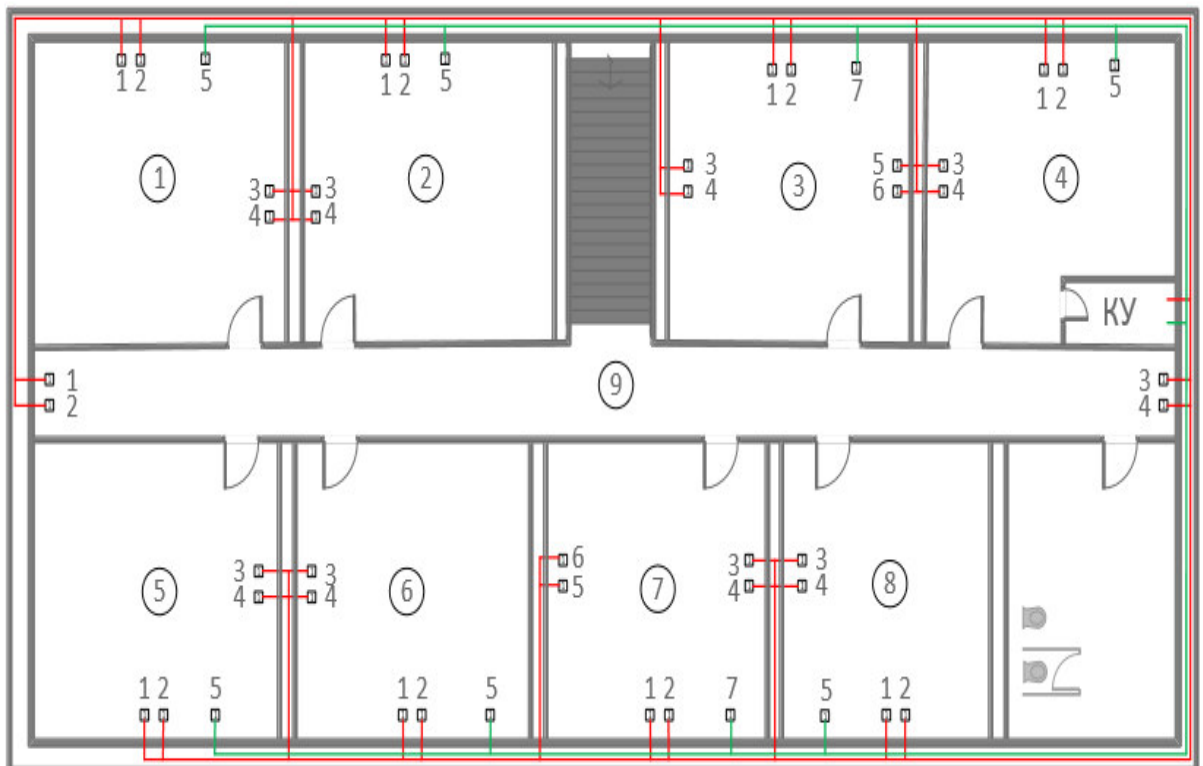


Рисунок 3.9 – План СКС здания на третьем этаже

Спецификация оборудования СКС представлена в таблице.

Таблица 3.2 - Спецификации оборудования СКС

Наименование и техническая характеристика	Ед. изм.	Кол-во
1	2	3
<b>Подсистема рабочего места</b>		
Розеточный модуль категории 5е серии МАХ, 1-портовый, Т568В, наклонный	шт.	170
Адаптер 45х45 мм для установки розеточных модулей серии МАХ в рамки Mosaic	шт.	85
Оконечные шнуры с модульными разъемами RJ45, категория 5е, длина 2 м	шт.	66
Оконечные шнуры с модульными разъемами RJ45, категория 5е, длина 3 м	шт.	30
<b>Горизонтальная подсистема</b>		
Кабель: витая пара - 4 пары, категория 5е	м	5 162
<b>Подсистема внутренних магистралей</b>		
Кабель кат. 3 - 100 пар	м	40
Кабель оптический: 12 х 62,5/125 волокна в PVC оболочке	м	45
Кабель: витая пара - 4 пары, категория 5е	м	200
<b>Подсистема внешних магистралей</b>		
Кабель оптический: 8 х 9/125 волокна с броней из стальной гофрированной ленты	м	7 00
<b>Горизонтальная подсистема</b>		
Коммутационная панель с розетками модульных разъемов RJ45, категории 5е	шт.	10
<b>Магистраль категории 3</b>		
Кроссовая панель типа 110, 19", категории 5, 200-парная с организатором	шт.	3
Кроссовая башня типа 110 категории 5, 400-парная	шт.	4

Продолжение таблицы 3.2

1	2	3
<b>Волоконно-оптическая магистраль</b>		
Коммутационная оптическая полка 19" - 1U-DSC-MM-12	шт.	6
Коммутационная оптическая полка 19" - 1U-FC-SM-8	шт.	1
Шнур монтажный многомодовый 1 м (62,5/125) с вилкой разъема SC	шт.	545
Шнур монтажный одномодовый 1 м с вилкой разъема	шт.	4
Гильза защитная КДЗС	шт.	50
Корпус сплайс-пластины для коммутационных оптических полок 19"	шт.	7
Держатели защитных гильз КДЗС	шт.	14
Крышка корпуса сплайс-пластины	шт.	7
<b>Шнуры из витых пар</b>		
Коммутационный шнур категории 5е с модульными разъемами RJ45, длина 1,0 м	шт.	55
Коммутационный шнур категории 5е с модульными разъемами RJ45, длина 1,5 м	шт.	135
Коммутационный шнур категории 5е с модульными разъемами RJ45, длина 2,0 м	шт.	27
Коммутационный шнур категории 5 с разъемами 110-RJ45, 1 пара - 1,0 м	шт.	80
Коммутационный шнур категории 5 с разъемами 110-RJ45, 1 пара - 1,5 м	шт.	70
Коммутационный шнур с разъемами 110-110, 1 пара - 1,0 м	шт.	170
25-парный коммутационный шнур с разъемов Telco, односторонний «папа» - 5,0 м	шт.	12
<b>Оптические шнуры</b>		
Оптический шнур с разъемами SC, 62,5/125, дуплексный - 3,0 м	шт.	18
Оптический шнур с разъемами FC-SC, 9/125, дуплексный - 3,0 м	шт.	3



### Окончание таблицы 3.2

1	2	3
<b>Шкафы для технических помещений</b>		
Шкаф напольный 42 U, 2033x800x875 мм	шт.	3
Комплект для соединения шкафов	шт.	1
Модуль вентиляторный 600 Series (монтаж сверху) - 2 вентилятора	шт.	3
Ножки для монтажного шкафа 19" (набор из 4 шт.)	шт.	3
Полка перфорированная для оборудования 19" длиной 454 мм	шт.	3
Силовые розетки для шкафов, вертикальные, 8 розеток	шт.	5
Винт с шайбой и гайкой для 19" оборудования, упаковка 50 шт.	шт.	5

### Администрирование и техническая эксплуатация сети

Проектные решения предусматривают применение многоточечного администрирования. Тип администрирования зависит от топологии ее сети, в данном случае - это иерархическая звезда.

Главный плюс многоточечного администрирования заключается в надежности компонентов. Техническая неисправность одной единицы оборудования или магистрали участка не затрагивает функционирование сети в целом.

Основные положения и нормы администрирования СКС представлены в международном стандарте (ISO/IEC 14763-1). Стандарт трактует требования и условия при которых упрощаются мероприятия по эксплуатации кабельной системы.

Для эффективной организации проводки и ее дальнейшей эксплуатации все пассивное и активное оборудование, монтируемое в специальные конструктивы технических помещений, разделяется на самостоятельные функциональные сегменты с определенным набором функций.

Задачу маркировки самостоятельных функциональных сегментов в рамках современных норм и стандартов возможно осуществить разными

						Лист
						39
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

методами. Один из которых заключается в использование символьной маркировки. Рекомендации трактуют использование регламента (ISO/IEC 14763-1) стандартов.

Предложенные проектные решения по организации СКС центрального офиса банка могут быть применены для остальных офисов и подразделений, так как схема разработана с учетом всех нормативных документов и стандартов. Составление спецификации оборудования было основано на экспликации реальных объектов, что позволят более точно оценить требования к капитальным вложениям в реализацию сети связи. [27, 28]

						Лист
						40
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

## **4 РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО РЕАЛИЗАЦИИ ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ БАНКА И ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

### **4.1 Мероприятия по реализации и технической эксплуатации сети банка**

Структурированная кабельная система устанавливается на первом этаже в 3-этажном здании офисного назначения, отдельные этажи которого имеют разную планировку, изображенную на рисунках 4.1-4.3. Высота этажа в свету между перекрытиями составляет 3 метра, общая толщина междуэтажных перекрытий равна 50 см.

Из структуры организации, которая будет эксплуатировать кабельную систему сразу после завершения строительства (коммерческий банк), и технических требований [27, 28] следует, что функционирование ЛВС связано с обработкой и передачей достаточно больших объемов информации.

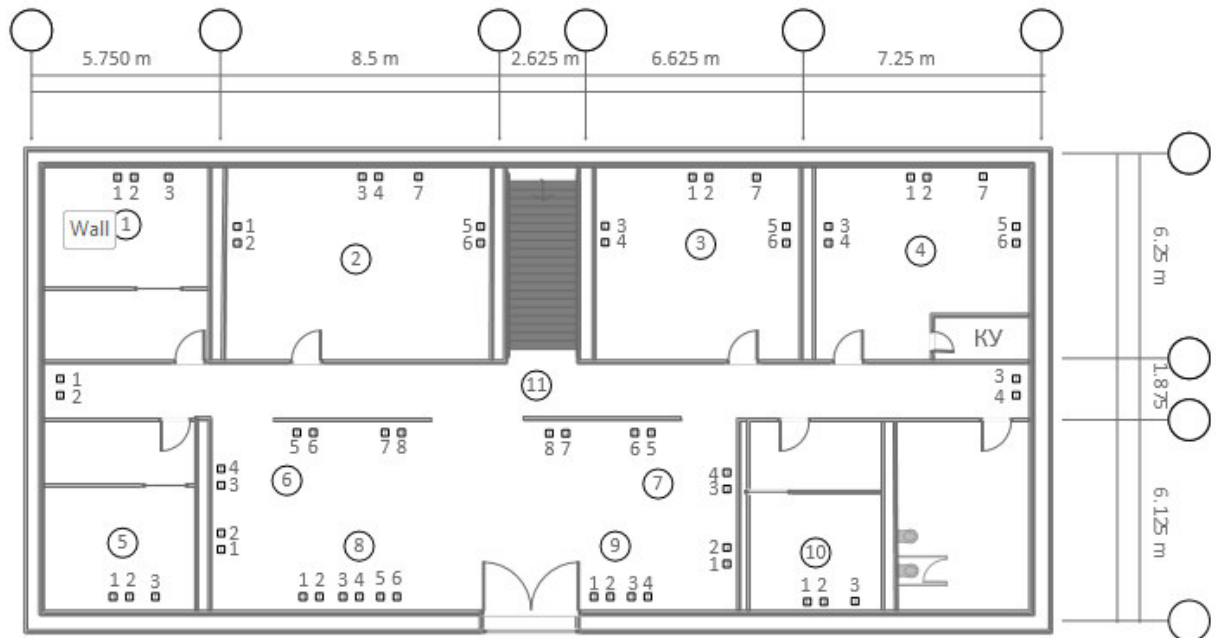
Так как банк размещается в помещении коммерческого типа, в нем предусмотрена возможность установки инженерных коммуникаций. В помещениях офисов для размещения оборудования СКС предусмотрена установка фальшстен с шириной свободного пространства 30см, а в коридорах предусмотрена установка фальшпотолка с высотой свободного пространства 20 см. За фальшстеной имеется достаточно свободного места для размещения лотков, используемых для прокладки кабелей различного назначения. Каких-либо дополнительных каналов в полу и потолках, которые могут быть использованы для прокладки кабелей, проектом здания не предусмотрено.

#### **Архитектурная фаза проектирования**

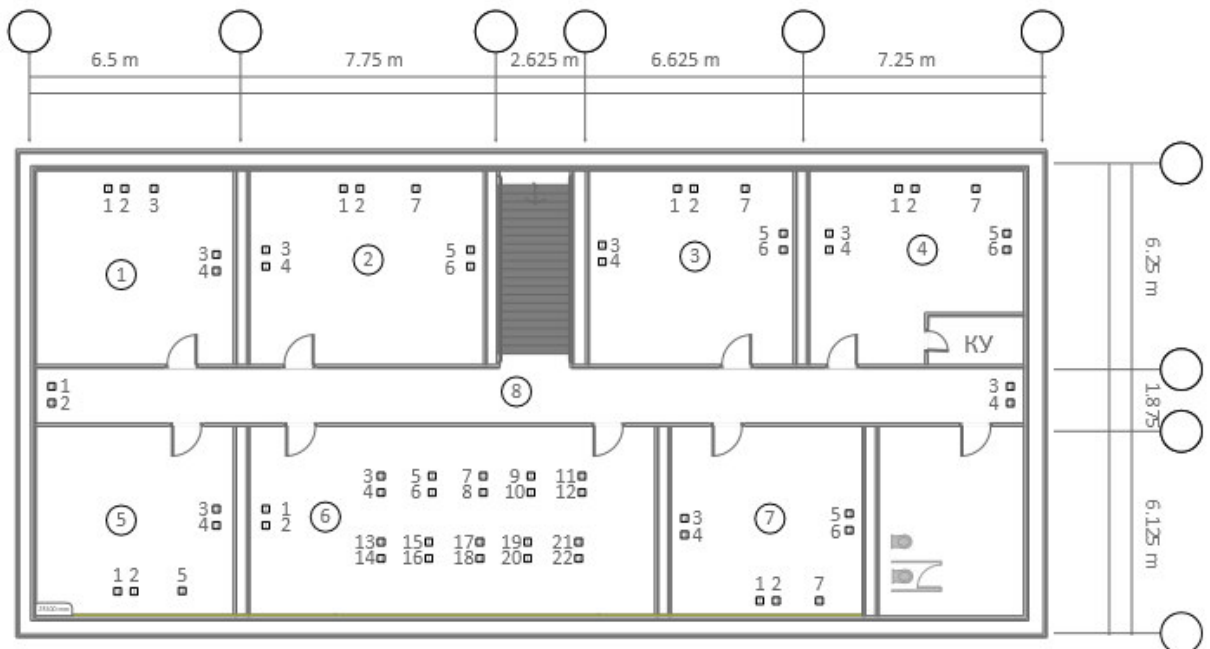
На первом этаже здания согласно плану рис. 4.1 имеется по 7 рабочих помещений, предназначенных для размещения пользователей. На втором этаже здания согласно плану рис. 4.2 имеется также 7 рабочих помещений,

						Лист
					<b>11070006.11.03.02.475.ПЗВК</b>	41
Изм.	Лист	№ докум.	Подпись	Дата		

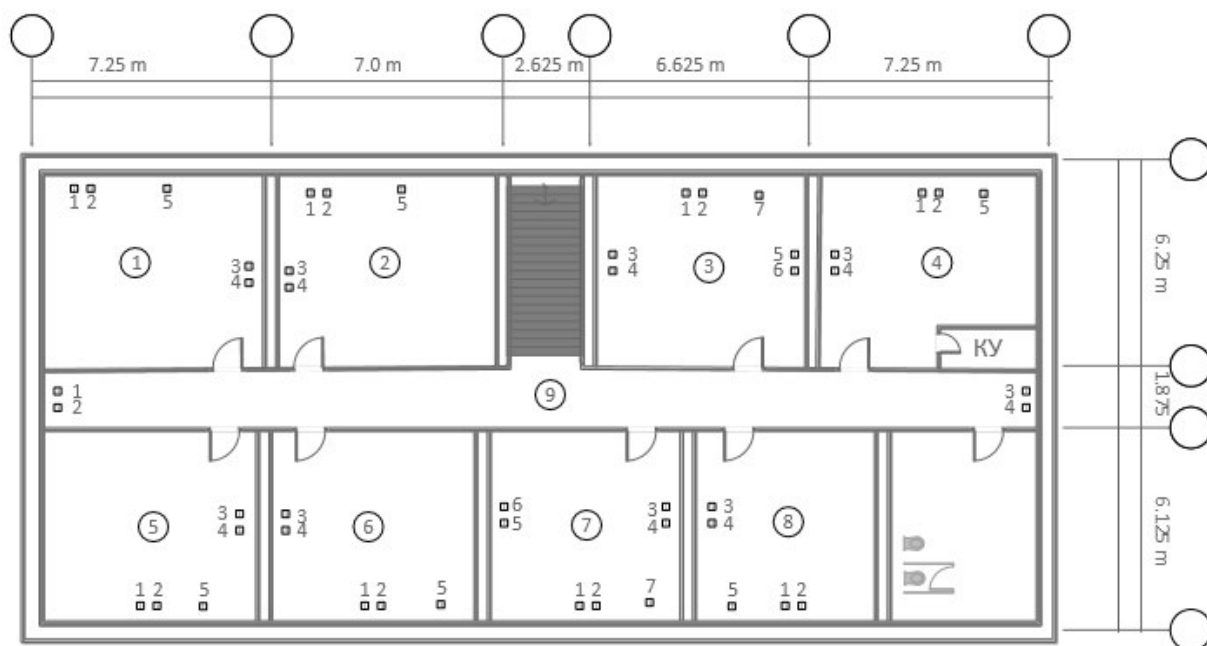
предназначенных для размещения пользователей. На третьем этаже здания согласно плану рис. 4.3 имеется по 8 рабочих помещений, предназначенных для размещения пользователей.



**Рисунок 4.1 - План 1-го этажа здания с указанием мест расположения рабочих мест и кабельных каналов в коридорах и помещениях для размещения пользователей**



**Рисунок 4.2 - План 2-го этажа здания с указанием мест расположения рабочих мест и кабельных каналов в коридорах и помещениях для размещения пользователей**



**Рисунок 4.3 - План 3-го этажа здания с указанием мест расположения рабочих мест и кабельных каналов в коридорах и помещениях для размещения пользователей**

Данные по площади этих помещений и количеству информационных розеток (ИР) сведены в таблицы 4.1, 4.2, 4.3.

**Таблица 4.1 - Помещения для установки индивидуальных розеток ИР проектируемой СКС для первого этажа**

Номер помещения	Площадь, м <sup>2</sup>	Количество устанавливаемых ИР
1	35.9	3
2	53.1	7
3	41.4	7
4	45.3	7
5	35.2	3
6	35.7	8
7	35.5	8
8	15.1	6
9	9.6	4
10	25.1	3
11	57.7	4
Итого	389.6	60

Рабочие площади на первом этаже, предназначенные для размещения рабочих мест пользователей, в соответствии с данными табл. 4.1 составляют 389.6 м<sup>2</sup>.

**Таблица 4.2 - Помещения для установки индивидуальных розеток ИР проектируемой СКС для второго этажа**

Номер помещения	Площадь, м <sup>2</sup>	Количество устанавливаемых ИР
1	40.6	3
2	48.4	7
3	41.4	7
4	45.3	7
5	39.8	5
6	80.0	22
7	36.1	7
8	57.7	4
Итого	389.3	62

Рабочие площади на втором этаже, предназначенные для размещения рабочих мест пользователей, в соответствии с данными табл. 4.2 составляют 389.3 м<sup>2</sup>.

**Таблица 4.3 Помещения для установки индивидуальных розеток ИР проектируемой СКС для третьего этажа**

Номер помещения	Площадь, м <sup>2</sup>	Количество устанавливаемых ИР
1	45.3	5
2	43.8	5
3	40.6	7
4	45.3	5
5	44.4	5
6	38.0	5
7	37.7	7
8	35.7	5
9	57.7	4
Итого	388.5	48

Рабочие площади на третьем этаже, предназначенные для размещения рабочих мест пользователей, в соответствии с данными табл. 4.3 составляют 389.5 м<sup>2</sup>.

## Кабельные каналы

Для прокладки горизонтальных и магистральных кабелей подсистемы внутренних магистралей проектируемой СКС требуется использовать следующие разновидности каналов:

- Закрытые металлические лотки за фальшстеной, предназначенные для прокладки кабелей горизонтальной подсистемы в коридорах;
- Декоративные кабельные короба (в местах с отсутствием каналов в стенах и в полу рабочих помещений пользователей), изготовленные из негорючего пластика и используемые для прокладки кабелей горизонтальной подсистемы и силовых кабелей питания.

Для уменьшения расхода декоративного короба и соответственно минимизации стоимости проекта и некоторого снижения продолжительности его реализации применяется горизонтальная прокладка короба в помещениях для размещения пользователей на высоте расположения розеток и одним вертикальным спуском за фальшстеной для прокладки кабелей.

**Таблица 4.4 - К определению максимальной и минимальной длины горизонтального кабеля**

Участок кабельной трассы	Максимальная длина, м	Минимальная длина, м
Подъем в монтажном шкафу и запасы на разделку	3	3
Участок «шкаф – стена технического помещения»	1	1
Подъем до кабельного лотка в техническом помещении	3	3
Расстояние до ввода в комнату	35,17	3,25
Ввод в комнату	0,8	0,8
Величина спуска в комнате	2,2	2,2
Длина горизонтального участка трассы в комнате	6,19	1,8
<b>Итого</b>	<b>51,36</b>	<b>15,05</b>
Среднее значение	33,2	

## **Размещение оборудования**

В проектируемой системе с учетом общего количества обслуживаемых рабочих мест примем следующую схему размещения оборудования:

- В помещении кроссовой устанавливаются монтажные конструктивы типа шкафов со стеклянной передней дверью;
- В помещении аппаратной применяется смешанный вариант монтажа с размещением части оборудования на стене.

Помещение аппаратной для экономии площади совмещается с кроссовой 1-го этажа. Поэтому с учетом размещения дополнительного сетевого оборудования коллективного пользования в этом техническом помещении устанавливается два монтажных конструктива.

## **4.2 Механизмы обеспечения защиты информации**

### **Способы защиты информации**

Данные в компьютерных системах подвержены риску утраты из-за неисправности или уничтожения оборудования, а также риску хищения. Способы защиты информации включают использование аппаратных средств и устройств, а также внедрение специализированных технических средств и программного обеспечения.

### **Методы защиты**

На практике используют несколько групп методов защиты, в том числе:

- Препятствие на пути предполагаемого похитителя; препятствие создают физическими и программными средствами;
- Управление, или оказание воздействия на элементы защищаемой системы;
- Маскировка, или преобразование данных, обычно – криптографическими способами;

									Лист
									46
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>				



- Регламентация, или разработка нормативно-правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению;

- Принуждение, или создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными;

- Побуждение, или создание условий, которые мотивируют пользователей к должному поведению.

Каждый из методов защиты информации реализуется при помощи различных категорий средств. Основные средства – организационные и технические.

### **Технические средства защиты информации**

Группа технических средств защиты информации совмещает аппаратные и программные средства:

- Резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе – на регулярной основе;

- Дублирование и резервирование всех подсистем сетей, которые имеют значение для сохранности данных;

- Создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов;

- Обеспечение возможности использовать резервные системы электропитания;

- Обеспечение безопасности от пожара или повреждения оборудования водой;

- Установка программного обеспечения, которое обеспечивает защиту баз данных и другой информации от несанкционированного доступа.

В комплекс технических мер входят и меры по обеспечению физической недоступности объектов компьютерных сетей, например, такие практические способы, как оборудование помещения камерами и сигнализацией.

### **Аутентификация и идентификация**

						Лист
						47
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

Чтобы исключить неправомерный доступ к информации применяют такие способы, как идентификация и аутентификация.

Идентификация - это механизм присвоения собственного уникального имени или образа пользователю, который взаимодействует с информацией.

Аутентификация - это система способов проверки совпадения пользователя с тем образом, которому разрешен допуск.

Эти средства направлены на то, чтобы предоставить или, наоборот, запретить допуск к данным. Подлинность, как правило, определяется тремя способами: программой, аппаратом, человеком. При этом объектом аутентификации может быть не только человек, но и техническое средство (компьютер, монитор, носители) или данные. Простейший способ защиты - пароль. [22]

#### **4.3 Охрана труда и техника безопасности при эксплуатации сети**

Совокупность факторов производственной среды, оказывающей влияние на здоровье и работоспособность человека в процессе труда называется условиями труда. В проектируемой ЛВС банка предусмотрено размещение оборудования в помещении кроссовой (серверной), с установкой рабочего места инженера связи и системного администратора, обеспечивающих администрирование сети банка, в отдельном офисном помещении. Основная работа выполняется на рабочем месте, с использованием ЭВМ (компьютера). Поэтому требования к охране труда соответствуют нормативным документам для операторов ЭВМ.

Таким образом, при использовании вышеуказанной аппаратуры и соблюдении требований условий работы за дисплеем, мероприятия по охране труда будут выполнены в соответствии с основными требованиями санитарных норм и правил.

						Лист
						48
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

## Электропожаробезопасность

Для обеспечения электробезопасности в помещении должны проверены следующие показатели:

- соответствие напряжения в сети тому на которое рассчитан ПК;
- наличие защитного заземления;
- меры защиты от перепадов в сети.

Приборы, находящиеся в помещении работают от номинального напряжения 220 В. В проектируемой сети все оборудование используется с применением заземления с изолированной нейтралью. Заземление выведено на заземляющий контур с сопротивлением 4 Ом. Заземление дисплеев осуществляется через системный блок ЭВМ. Соединение ПК с сетью выполнено с помощью трехжильного медного силового кабеля с вилкой, имеющей клеммы заземления. Все провода в рабочем помещении имеют характеристики, соответствующие токам и напряжениям в сети. [23]

Обязательно наличие порошкового огнетушителя в помещении кроссовой (серверной).

						Лист
						49
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

## 5 ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ПРОЕКТА

Проектом предусмотрена реализация корпоративной сети банка, поэтому в технико-экономическом обосновании будут рассчитаны капитальные вложения и эксплуатационные расходы. Доход от реализации проекта является косвенным, то есть компания будет экономить средства на ведение телефонных переговоров и отчисления провайдером услуг.

### Расчет капитальных вложений

Общие капитальные вложения на приобретение оборудования могут быть вычислены по формуле (5.1):

$$K_{об} = \sum_{i=1}^N K_i, \text{руб} \quad (5.1)$$

где  $K_{об}$  - суммарный объем затрат на приобретение оборудования;  $K_i$  - общая стоимость одной позиции (типа оборудования);  $N$  - количество позиций.

**Таблица 5.1 - Смета затрат на приобретение оборудования**

Наименование и техническая характеристика 1	Ед. изм. 2	Кол-во 3	Стоимость ед. Руб. 4	Стоимость обор. Руб. 5
<b>Подсистема рабочего места</b>				
Розеточный модуль категории 5е серии МАХ, 1-портовый, Т568В, наклонный	шт.	170	60	10200
Адаптер 45x45 мм для установки розеточных модулей серии МАХ в рамки Mosaic	шт.	85	35	2975
Оконечные шнуры с модульными разъемами RJ45, категория 5е, длина 2 м	шт.	66	110	7260
Оконечные шнуры с модульными разъемами RJ45, категория 5е, длина 3 м	шт.	30	150	4500
<b>Горизонтальная подсистема</b>				
Кабель: витая пара - 4 пары, категория 5е	м	5 162	21	108402
<b>Подсистема внутренних магистралей</b>				
Кабель кат. 3 - 100 пар	м	40	360	14400
Кабель оптический: 8 x 62,5/125 волокна в PVC оболочке	м	45	87	3915
Кабель: витая пара - 4 пары, категория 5е	м	200	21	4200

**Продолжение таблицы 5.1**

1	2	3	4	5
<b>Подсистема внешних магистралей</b>				
Кабель оптический: 8 х 9/125 волокна с броней из стальной гофрированной ленты	м	7 00	49	34300
Коммутационная панель с розетками модульных разъемов RJ45, категории 5е	шт.	10	2500	25000
<b>Магистраль категории 3</b>				
Кроссовая панель типа 110, 19", категории 5, 200-парная с организатором	шт.	3	1500	4500
Кроссовая башня типа 110 категории 5, 400-парная	шт.	4	1700	6800
<b>Волоконно-оптическая магистраль</b>				
Коммутационная оптическая полка 19" - 1U-DSC-MM-12	шт.	6	4200	25200
Коммутационная оптическая полка 19" - 1U-FC-SM-8	шт.	1	3700	3700
Шнур монтажный многомодовый 1 м (62,5/125) с вилкой разъема SC	шт.	545	70	38150
Шнур монтажный одномодовый 1 м с вилкой разъема FC	шт.	4	65	260
Гильза защитная КДЗС	шт.	50	6	300
Корпус сплайс-пластины для коммутационных оптических полок 19"	шт.	7	1050	7350
Держатели защитных гильз КДЗС	шт.	14	4	56
Крышка корпуса сплайс-пластины	шт.	7	6200	43400
<b>Шнуры из витых пар</b>				
Коммутационный шнур категории 5е с модульными разъемами RJ45, длина 1,0 м	шт.	55	300	16500
Коммутационный шнур категории 5е с модульными разъемами RJ45, длина 1,5 м	шт.	135	315	42525
Коммутационный шнур категории 5е с модульными разъемами RJ45, длина 2,0 м	шт.	27	350	9450
Коммутационный шнур категории 5 с разъемами 110-RJ45, 1 пара - 1,0 м	шт.	80	270	21600
Коммутационный шнур категории 5 с разъемами 110-RJ45, 1 пара - 1,5 м	шт.	70	290	20300
Коммутационный шнур с разъемами 110-110, 1 пара - 1,0 м	шт.	170	170	28900
25-парный коммутационный шнур с разъемов Telco, односторонний «папа» - 5,0 м	шт.	12	250	3000

### Окончание таблицы 5.1

1	2	3	4	5
<b>Оптические шнуры</b>				
Оптический шнур с разъемами SC, 62,5/125, дуплексный - 3,0 м	шт.	18	410	7380
Оптический шнур с разъемами FC-SC, 9/125, дуплексный - 3,0 м	шт.	3	290	870
<b>Монтажное оборудование</b>				
<b>Шкафы для технических помещений</b>				
Шкаф напольный 42 U, 2033x800x875 мм	шт.	3	30000	90000
Комплект для соединения шкафов	шт.	1	330	330
Модуль вентиляторный 600 Series (монтаж сверху) - 2 вентилятора	шт.	3	3600	10800
Ножки для монтажного шкафа 19" (набор из 4 шт.)	шт.	3	650	1950
Полка перфорированная для оборудования 19" длиной 454 мм	шт.	3	1370	4110
Силовые розетки для шкафов, вертикальные, 8 розеток	шт.	5	1600	8000
Винт с шайбой и гайкой для 19" оборудования, упаковка 50 шт.	шт.	5	70	350
Коммутатор Cisco Catalyst WS-C2960-24-S 2-го уровня 24 x FE RJ-45, 1 CON порт RJ-45.	шт.	10	28500	285000
Маршрутизатор Cisco CISCO2811-V/K9	шт.	1	122000	122000
Сервер Cisco UCSC-C220-M4S	шт.	4	212000	848000
Межсетевой экран Cisco ASA5505-BUN-K9	шт.	1	27000	27000
Компьютер HP 290 G1 MT Bundle 2TP49ES	шт.	61	23000	1403000
IP телефон ATCOM AT-530P	шт.	35	2100	73500
Камера видеонаблюдения FALCON EYE FE-IDV720AHD/35M, 2.8 - 12 мм	шт.	29	1700	49300
МФУ Epson Expression Home XP-330 с картриджами Lucky Print	шт.	27	5400	145800
Точка доступа D-LINK DAP-1360U/A1A	шт.	4	1400	5600
Ноутбук Dell Inspiron 3565 Black	шт.	1	21000	21000
Проектор BENQ MS527	шт.	1	22000	22000
<b>Итого:</b>				<b>3613133</b>

При приобретении оборудования обычно предусматриваются следующие расходы:  $K_{пр}$  – Затраты на приобретение оборудования;  $K_{тр}$  – транспортные расходы в т.ч. таможенные расходы (4% от  $K_{пр}$ );  $K_{смп}$  – строительно-монтажные расходы (20% от  $K_{пр}$ );  $K_{т/у}$  – расходы на тару и упаковку (0,5% от  $K_{пр}$ );  $K_{зсп}$  – заготовительно-складские расходы (1,2% от  $K_{пр}$ );  $K_{ппр}$  – прочие непредвиденные расходы (3% от  $K_{пр}$ ).

Таким образом, общие капитальные вложения рассчитываются как (5.2):

						Лист
						52
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

$$KB = K_{об} + (K_{тр} + K_{смп} + K_{т/у} + K_{зср} + K_{пнр})K_{об} \quad (5.2)$$

$$KB = 3613133 + (0.04 + 0.2 + 0.005 + 0.012 + 0.03) * 3613133$$

$$KB = 4650102, \text{ руб.}$$

### **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 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 5.2 – Состав персонала по обслуживанию оборудования**

Наименование должности	Оклад	Количество, чел.	Сумма з/п, руб.
Инженер связи	50 000	1	50 000
Системный администратор	40 000	1	40 000
Монтажник	40 000	1	40 000
<b>Итого(ЗП):</b>		<b>3</b>	<b>130 000</b>

Годовой фонд оплаты труда для персонала рассчитывается как (5.3):

$$\text{ФОТ} = \text{ЗП} * T * K_{pr} * 12, \text{ руб} \quad (5.3)$$

где:  $T=1$  – коэффициент, учитывающий доплату за работу с вредными условиями труда; 12 – количество месяцев;  $K_{pr} = 1.25$  – коэффициент премии.

$$\text{ФОТ} = 130000 * 12 * 1 * 1.25 = 1950000 \text{ руб.}$$

Страховые взносы составляют 30 % от фонда оплаты труда (2018 год):

$$\text{СВ} = \text{ФОТ} * 0.3, \text{ руб} \quad (5.4)$$

$$\text{СВ} = 1950000 * 0.3 = 585000 \text{ руб.}$$

Сумма страховых взносов составляет 585 тысячи рублей.

Под амортизацией понимается процесс постепенного возмещения стоимости основных фондов, в целях накопления средств для реконструкции и приобретения основных средств. Самым распространенным способом оценки амортизации является учет амортизации, составленный исходя из общего срока службы основных фондов, в этом случае:

$$\text{АО} = T/F, \text{ руб} \quad (5.5)$$

где  $T$  – стоимость оборудования,  $F$  – срок службы этого оборудования, (Примерно  $F = 10$  лет).



$$AO = 3613133/10 = 361313, \text{ руб.}$$

Затраты на амортизационные отчисления 361 тыс. 313 рублей.

Величина материальных затрат включает в себя оплату электроэнергии для производственных нужд, затраты на материалы и запасные части и др. Эти составляющие материальных затрат определяются следующим образом:

**а)** затраты на оплату электроэнергии определяются в зависимости от мощности стационарного оборудования (5.6):

$$Z_{\text{ЭН}} = T * 24 * 365 * P \quad (5.6)$$

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

При  $T=2.254$  руб./кВт (для Вьетнама),  $P=150$  кВт, затраты на оплату электроэнергии определяются в зависимости от мощности стационарного оборудования:

$$Z_{\text{ЭН}} = 2.254 * 24 * 365 * 150 = 2961756, \text{ руб}$$

**б)** затраты на материалы и запасные части составляют 3,5% от основных производственных фондов (5.7):

$$Z_{\text{МЗ}} = KB * 0.035 \quad (5.7)$$

где  $KB$  – капитальные вложения.

$$Z_{\text{МЗ}} = 4650102 * 0.035 = 162754, \text{ руб}$$

Общие материальные затраты определяется по формуле (5.8):

$$Z_{\text{Общ}} = Z_{\text{ЭН}} + Z_{\text{МЗ}} \quad (5.8)$$

где  $Z_{\text{ЭН}}$  – затраты на оплату электроэнергии;  $Z_{\text{М}}$  – материальные затраты.

$$Z_{\text{Общ}} = 2961756 + 162754 = 3124510, \text{ руб}$$

						Лист
					<b>11070006.11.03.02.475.ПЗВК</b>	55
Изм.	Лист	№ докум.	Подпись	Дата		

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

$$Z_{пр} = \text{ФОТ} * 0.15 \quad (5.9)$$

$$Z_{эк} = \text{ФОТ} * 0.25 \quad (5.10)$$

где ФОТ – годовой фонд оплаты труда.

$$Z_{пр} = 2400000 * 0.15 = 292500, \text{ руб}$$

$$Z_{эк} = 2400000 * 0.25 = 487500, \text{ руб}$$

Таким образом, сумма прочих расходов определяется по формуле (5.11):

$$Z_{прочие} = Z_{пр} + Z_{эк} \quad (5.11)$$

$$Z_{прочие} = 292500 + 487500 = 780000 \text{ руб}$$

Результаты расчета годовых эксплуатационных расчетов сводятся в общую таблицу 5.3

**Таблица 5.3- Годовые эксплуатационные расходы**

Наименование затрат	Сумма затрат, руб.	Удельный вес статей, %
1. ФОТ	1950000	28.67
2. Страховые взносы	585000	8.62
3. Амортизационные отчисления	361313	5.32
4. Материальные затраты	3124510	45.92
5. Прочие расходы	780000	11.47
ИТОГО	6800823	100

Определены основные оценочные показатели проекта, характеризующие эффективность его реализации. Рассчитанные технико-экономические показатели на конец расчетного периода сведены в таблицу 5.4.

**Таблица 5.4 – Основные технико-экономические показатели проекта**

<b>Показатели</b>	<b>Численные значения</b>
Количество абонентов, чел	61
Капитальные затраты, руб	4650102
Численность персонала, чел	3
Ежегодные эксплуатационные расходы, руб, в том числе:	6800823
Фонд оплаты труда	1950000
Страховые взносы	585000
Амортизационные отчисления	361313
Материальные затраты	3124510
Прочие расходы	780000

Таким образом, осуществлены расчеты капитальных вложений в предлагаемый проект и калькуляция эксплуатационных расходов, позволяющие оценить необходимые инвестиции в строительство и эксплуатацию сети связи банка.

## ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы были получены следующие результаты:

- 1) Разработан проект инфокоммуникационной сети коммерческого банка.
- 2) Разработаны и проанализированы варианты реализации сетевой инфраструктуры в центральном офисе банка, и VPN между подразделениями.

В ходе проектирования принято решение реализовать инфокоммуникационную инфраструктуру банка на базе технологии Ethernet, с разработкой проекта структурированной кабельной системы. В качестве производителя оборудования СКС выбрана вьетнамская компания Huynh Chan Duu, т.к. она имеет лицензии и сертификаты на применение сетевого оборудование в сетях связи Вьетнама.

Для анализа эффективности сетевой инфраструктуры принято решение провести имитационное моделирование. В результате разработана модель сети банка в среде имитационного моделирования Cisco Packet Tracer, проведена настройка сетевого оборудования, включая серверы. Также создана модель сети VPN, объединяющей филиалы подразделений банка.

Рассчитаны технико-экономические показатели проекта. Капитальные вложения составили 4650102 руб, эксплуатационные расходы – 6800823 руб.

Таким образом, задачи, поставленные в техническом задании, полностью решены. В результате работы создана инфокоммуникационная инфраструктура коммерческого банка и разработаны рекомендации по её реализации. Разработанная сеть позволит улучшить информационный обмен между подразделениями банка, улучшит условия труда сотрудников, повысит конкурентоспособность организации на финансовом рынке. Применение современных инфокоммуникационных технологий гарантирует актуальность проектных решений и их практическую ценность.

						Лист
					<b>11070006.11.03.02.475.ПЗВК</b>	58
Изм.	Лист	№ докум.	Подпись	Дата		

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Описание коммерческого банка Techcombank, Вьетнам [Электронный ресурс]/ [www.techcombank.com.vn](http://www.techcombank.com.vn) – официальный сайт Techcombank, Вьетнам// URL: <https://www.techcombank.com.vn/gioi-thieu/ve-chung-toi/lich-su-techcombank> (дата обращения 06.02.2018г.)

2. Виртуальная локальная сеть - VLAN [Электронный ресурс]/ [www.searchnetworking.techtarget.com](http://www.searchnetworking.techtarget.com) –сайт компании Search Networking // URL: <https://searchnetworking.techtarget.com/definition/virtual-LAN> (дата обращения 12.02.2018г.)

3. IEEE Standarts 802.1Q: VLAN [Электронный ресурс] // <http://standards.ieee.org/> - материалы IEEE Standarts download page E// URL: <http://standards.ieee.org/about/get/802/802.1q.html> (дата обращения 17.02.2018г.)

4. Интернет протокол [Электронный ресурс]/ [www.searchnetworking.techtarget.com](http://www.searchnetworking.techtarget.com) – сайт компании Search Networking// URL: <https://searchnetworking.techtarget.com/definition/Internet-Protocol> (дата обращения 15.02.2018г.)

5. Таненбаум, Э., Уэзеролл, Д. Компьютерные сети: пятое издание [Текст]/ Э.Таненбаум, Д.Уэзеролл. - СПб.: Питер, 2012. - 960с.

6. Уэнделл, Одом. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND 2 200 - 101: маршрутизация и коммутация, акад. Изд.: Пер. с англ. - М.: Издательский дом "Вильямс", 2015. - 736с.

7. Уэнделл, Одом. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND 2 100 - 101, акад. Изд. : Пер. с англ.- М.: Издательский дом "Вильямс", 2015. - 912с.

8. Олифер, В., Олифер, Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. Пятое издание. - СПб.: Питер, 2016. - 992с.

									Лист
									59
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>				

9. Принципы организации учёта IP-трафика [Электронный ресурс]/ [www.special.habrahabr.ru](http://www.special.habrahabr.ru) – сайт сетевых разработчиков// URL: <https://special.habrahabr.ru/kyocera/p/136844/> (дата обращения 06.04.2018г.)
10. Голосовой трафик: VOIP, терминация и связь [Электронный ресурс]/ [www.youmagic.pro](http://www.youmagic.pro) – официальный сайт компании Youmagic // URL: <https://youmagic.pro/blog/poleznoe/golosovoj-trafik/> (дата обращения 13.04.2018г.)
11. Амато, Вито. Основы организации сетей Cisco, том 1 [Текст]/ В. Амато. - М.: Издательский дом "Вильямс", 2004. - 512с.
12. Амато, Вито. Основы организации сетей Cisco, том 2 [Текст]/ В. Амато. М.: Издательский дом "Вильямс", 2004. - 464с.
13. Андрончик, А. Н. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учеб. пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков ; под общ. ред. Н. И. Синадского. – Екатеринбург : Изд-во Урал. ун-та, 2014. - 180 с.
14. DNS сервер BIND [Электронный ресурс]/ [www.habr.com](http://www.habr.com) - сайт сетевых разработчиков// URL: <https://habr.com/post/137587/> (дата обращения 19.04.2018г.)
15. Правила назначения IP адресов [Электронный ресурс] / [www.kvb.ucoz.ru](http://www.kvb.ucoz.ru) – каталог статей // URL: [http:// kvb.ucoz.ru/books/IP-02.pdf](http://kvb.ucoz.ru/books/IP-02.pdf) (дата обращения 21.04.18)
16. WIFI технология [Электронный ресурс] / [www.ccm.net](http://www.ccm.net) - Официальный сайт компании ССМ // URL: <https://ccm.net/faq/298-what-is-wifi-and-how-does-it-work> (дата обращения 21.04.18)
17. Уэнстром, Майкл. Организация защиты сетей Cisco / пер. с англ.– М. : Издательский дом «Вильямс», 2005. – 768 с.
18. Gary Hallen, G. Kellogg Security Monitoring with Cisco Security MARS. – USA : Cisco Press, 2007. – 335 p.
19. Стивенс, У. Р. Протоколы TCP/IP. Практическое руководство /пер. с англ. – СПб. : БХВ-Петербург, 2003. – 672 с.

						Лист
						60
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

20. Кульгин, М. Практика построения компьютерных сетей. Для профессионалов [Текст]/ М. Кульгин. – СПб. : Питер, 2001. – 320 с.

21. Сетевое и серверное оборудование [Электронный ресурс] / [www.lanbi.ru](http://www.lanbi.ru) - Официальный сайт компании поставщика сетевого оборудования // URL: <http://lanbi.ru/catalog/category183> (дата обращения 23.04.2018г.)

22. Безопасен ли Ethernet? [Электронный ресурс] // <http://www.thicongpro.com> – официальный сайт компании Thicongpro// URL: <http://www.thicongpro.com/2015/01/ethernet-la-gi-mang-ethernet-co-an-toan.html> (дата обращения 27.04.2018)

23. Обзор сетевых систем [Электронный ресурс] // Режим доступа: <https://voer.edu.vn/m/tong-quan-ve-he-thong-mang/13224.pdf> (дата обращения 02.05.2018г.)

24. Решения FTTH на базе оборудования компании Cisco [Электронный ресурс] / [www.cisco.com](http://www.cisco.com) - Официальный сайт Cisco Systems // URL: <http://www.cisco.com/ethernet-solutions/ftth.html> (дата обращения 04.04.2018г.)

25. ГОСТ Р 21.1703-2000 Государственный стандарт Российской Федерации «Система проектной документации для строительства. Правила выполнения рабочей документации проводных средств связи» System of design documents for construction. Rules of executing of working documents for wire communication systems [Электронный ресурс] // Режим доступа: <http://msk.mos.ru/Handlers/Files.ashx/Download?ID=17045> (дата обращения 02.03.2018г.).

26. Каталог продукции Hosiwell Cable Provider Huynh Chan Duy [Электронный ресурс]/ <http://huynhchanduy.com/> - официальный сайт компании Huynh Chan Duy// URL: <http://huynhchanduy.com/product-category/cap-dieu-khien-control-cables> (дата обращения 05.04.2018г.).

27. ISO/IEC 11801-2008, Ed 2.1 + Amd. 1+ Amd. 2 - 2010 г. Структурированная кабельная система для помещений заказчиков.

						Лист
						61
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

28. ANSI/TIA/EIA 568-C.0C.1 - 2009 г. Стандарт на телекоммуникационные кабельные системы коммерческих зданий. Общие положения.

						Лист
						62
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	



**Настройка VLAN для коммутатора 0:**

- Switch(config)#vtp domain TECHCOMBANK
- Changing VTP domain name from NULL to TECHCOMBANK
- Switch(config)#vtp password 123
- Setting device VLAN database password to 123
- Switch(config)#vtp mode server
- Device mode already VTP SERVER.
- Switch(config)#vlan 10
- Switch(config-vlan)#name data
- Switch(config-vlan)#vlan 20
- Switch(config-vlan)#name voice
- Switch(config-vlan)#vlan 30
- Switch(config-vlan)#name marketing
- Switch(config-vlan)#vlan 40
- Switch(config-vlan)#name client
- Switch(config-vlan)#exit
- Switch(config)#interface range fastEthernet 0/1-10
- Switch(config-if-range)#switchport mode trunk
- Switch(config-if-range)#exit

**Настройка VLAN для коммутатора 1 до 3**

- Switch(config)#vtp domain TECHCOMBANK
- Changing VTP domain name from NULL to TECHCOMBANK
- Switch(config)#vtp password 123
- Setting device VLAN database password to 123
- Switch(config)#vtp mode client
- Setting device to VTP CLIENT mode.
- Switch(config)#interface fastEthernet 0/1
- Switch(config-if)#switchport mode trunk
- Switch(config-if)#no shutdown
- Switch(config-if)#exit

- Switch(config)#interface fastEthernet 0/3
- Switch(config-if-range)#switchport mode access
- Switch(config-if-range)#switchport access vlan 10
- Switch(config-if-range)#no shutdown
- Switch(config-if-range)#exit
- Switch(config)#interface fastEthernet 0/5
- Switch(config-if-range)#switchport mode access
- Switch(config-if-range)#switchport access vlan 30
- Switch(config-if-range)#no shutdown
- Switch(config-if-range)#exit

						Лист
						64
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

## ПРИЛОЖЕНИЕ Б

```
- Router(config)#interface fastEthernet 1/0.10
- Router(config-subif)#encapsulation dot1Q 10
- Router(config-subif)#ip address 192.168.10.1 255.255.255.0
- Router(config-subif)#exit
- Router(config)#interface fastEthernet 1/0.20
- Router(config-subif)#encapsulation dot1Q 20
- Router(config-subif)#ip address 192.168.20.1 255.255.255.0
- Router(config-subif)#exit
- Router(config)#interface fastEthernet 1/0.30
- Router(config-subif)#encapsulation dot1Q 30
- Router(config-subif)#ip address 192.168.30.1 255.255.255.0
- Router(config-subif)#exit
- Router(config)#interface fastEthernet 1/0.40
- Router(config-subif)#encapsulation dot1Q 40
- Router(config-subif)#ip address 192.168.40.1 255.255.255.0
- Router(config-subif)#exit
- Router(config)#interface fastEthernet 0/1
- Router(config-if)#ip address 172.54.23.1 255.255.255.252
- Router(config-if)#no shutdown
- Router(config-if)#exit
- Router(config)#interface fastEthernet 1/1
- Router(config-if)#ip address 203.162.0.1 255.255.255.252
- Router(config-if)#no shutdown
- Router(config-if)#exit
```

					Лист
					65
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>

## ПРИЛОЖЕНИЕ В

```
- Router(config)#ip dhcp excluded-address 192.168.10.1
192.168.10.5
- Router(config)#ip dhcp excluded-address 192.168.20.1
192.168.20.5
- Router(config)#ip dhcp excluded-address 192.168.30.1
192.168.30.5
- Router(config)#ip dhcp excluded-address 192.168.40.1
192.168.40.5
- Router(config)#ip dhcp pool data
- Router(dhcp-config)#network 192.168.10.0 255.255.255.0
- Router(dhcp-config)#default-router 192.168.10.1
- Router(dhcp-config)#exit
- Router(config)#ip dhcp pool voice
- Router(dhcp-config)#network 192.168.20.0 255.255.255.0
- Router(dhcp-config)#default-router 192.168.20.1
- Router(dhcp-config)#option 150 ip 192.168.20.1
- Router(dhcp-config)#exit
- Router(config)#ip dhcp pool marketing
- Router(dhcp-config)#network 192.168.30.0 255.255.255.0
- Router(dhcp-config)#default-router 192.168.30.1
- Router(dhcp-config)#exit
- Router(config)#ip dhcp pool client
- Router(dhcp-config)#network 192.168.40.0 255.255.255.0
- Router(dhcp-config)#default-router 192.168.40.1
- Router(dhcp-config)#exit
```

						Лист
						66
Изм.	Лист	№ докум.	Подпись	Дата	<b>11070006.11.03.02.475.ПЗВК</b>	

**Конфигурация ISAKMP на маршрутизаторе центрального офиса**

- Techcombank1 (config)#crypto isakmp policy 10
- Techcombank1 (config-isakmp)#hash md5
- Techcombank1 (config-isakmp)#encryption des
- Techcombank1 (config-isakmp)#group 2
- Techcombank1 (config-isakmp)#authentication pre-share
- Techcombank1 (config-isakmp)#exit
- Techcombank1 (config)#crypto isakmp key TECHCOMBANK address 20.20.20.3

**Конфигурация ISAKMP на маршрутизаторе филиала**

- Techcombank15 (config)#crypto isakmp policy 10
- Techcombank15 (config-isakmp)#hash md5
- Techcombank15 (config-isakmp)#encryption des
- Techcombank15 (config-isakmp)#group 2
- Techcombank15 (config-isakmp)#authentication pre-share
- Techcombank15 (config-isakmp)#exit
- Techcombank15 (config)#crypto isakmp key TECHCOMBANK address 20.20.20.1

**Настройка IPsec transform set**

- Techcombank1 (config)#crypto ipsec transform-set MYSET esp-des
- Techcombank1 (config)#crypto ipsec security-association lifetime seconds 1800
  
- Techcombank15 (config)#crypto ipsec transform-set MYSET esp-des
- Techcombank15 (config)#crypto ipsec security-association lifetime seconds 1800

**Создание Access Control List (ACL)**

						Лист
					<b>11070006.11.03.02.475.ПЗВК</b>	67
Изм.	Лист	№ докум.	Подпись	Дата		

- Techcombank1 (config)#access-list 100 permit ip 192.168.10.0 0.0.0.255 192.169.10.0 0.0.0.255
- Techcombank15 (config)#access-list 100 permit ip 192.169.10.0 0.0.0.255 192.168.10.0 0.0.0.255

### Конфигурация Crypto Map

- Techcombank1 (config)#crypto map TECHCOMBANK-MAP 10 ipsec-isakmp
- Techcombank1 (config-crypto-map)#set peer 20.20.20.3
- Techcombank1 (config-crypto-map)#match address 100
- Techcombank15 (config)#crypto map TECHCOMBANK-MAP 10 ipsec-isakmp
- Techcombank15 (config-crypto-map)#set peer 20.20.20.1
- Techcombank15 (config-crypto-map)#match address 100

### Включение Crypto Map на интерфейсе

- Techcombank1 (config)#interface s0/0
- Techcombank1 (config-if)#crypto map TECHCOMBANK-MAP
- Включение Crypto Map на интерфейсе
- Techcombank15 (config)#interface s0/0
- Techcombank15 (config-if)#crypto map TECHCOMBANK-MAP