Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к курсовой работе
«Локальная компьютерная сеть, вариант 20»
по дисциплине
«Аппаратное обеспечение компьютерных сетей»

Выполнил:
студент группы 650503
Юревич А. С.

Руководитель:
Глецевич И. И.

Минск 2019

Вариант	20
Сфера деятельности	Центр обработки данных компании, занимающейся программированием.
Помещение и пользователи	В пристройке к многоэтажному зданию, в которую ведет коридор. 2 комнаты (10 и 30 м^2) вдоль коридора, подсобное помещение (7 м^2).
Оборудование	Оснащение рабочих мест для 3 работающих поочередно администраторов, основной и резервный серверы для одновременного обслуживания до 100 пользователей (тонкие клиенты), принтер.
Подключение к Ethernet	Metro Ethernet.
Адресация	IPv4 (выдана подсеть 172.17.0.0), IPv6 (для некоторых приложений программистов).
Безопасность	Подключение к беспроводной сети только администраторов. Удаленное администрирование.
Финансы	Полноценная коммерческая сеть.
Дополнительные требования заказчика	Обеспечить повышенную пожарную безопасность.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ……..4
1 ОБЗОР ИСТОЧНИКОВ……5
2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ……..7
2.1 Виртуальная сеть для администраторов……8
2.2 Виртуальная сеть серверной комнаты……8
3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ……...9
3.1 Обоснование выбора сетевой операционной системы……9
3.2 Обоснование выбора активного сетевого оборудования……9
3.2.1 Маршрутизатор Cisco 2911……..10
3.2.2 Беспроводная точка доступа Cisco Aironet 1602I……...11
3.2.3 Коммутатор Cisco SB SRW2008P……12
3.3 Обоснование выбора серверного оборудования……12
3.3.1 Обоснование выбора терминального сервера……12
3.3.2 Обоснование выбора RADIUS-сервера……...14
3.4 Организация рабочих мест……14
3.4.1 Обоснование выбора рабочей станции администратора……...15
3.4.2 Обоснование выбора принтера……15
3.5 Обоснование выбора пассивного сетевого оборудования……16
3.5.1 Витая пара прямого типа……..16
3.5.2 Обоснование выбора информационных розеток……18
3.5.3 Обоснование выбора кабельного короба……18
3.5.4 Обоснование выбора монтажных стоек……..18
3.6 Описание настройки компонентов локальной сети……19
3.6.1 Разделение сети на виртуальные локальные подсети……19
3.6.2 Настройка удалённого администрирования……...19
3.6.3 Настройка AAA-сервиса и внешнего сервера авторизации……..21
3.6.4 Настройка беспроводной точки доступа……25
3.6.5 Настройка принтера……..27
3.6.6 Настройка персональных компьютеров……..28
3.6.7 Настройка маршрутизатора……29
3.7 Адресация в локальной компьютерной сети……30
4 ПРИНЦИПИАЛЬНОЕ ПРОЕКТИРОВАНИЕ……..32
ЗАКЛЮЧЕНИЕ ……...…..…….…33
СПИСОК ЛИТЕРАТУРЫ……34
ПРИЛОЖЕНИЕ А……..37
ПРИЛОЖЕНИЕ Б……..38
ПРИЛОЖЕНИЕ В……..39
ПРИЛОЖЕНИЕ Г……..40

ВВЕДЕНИЕ

Локальная компьютерная сеть (далее – ЛКС) – сеть из нескольких устройств, объединённых между собой при помощи активного и пассивного сетевого оборудования. Локальные сети могут проектироваться в пределах одного помещения, этажа или целого здания. Основная цель объединения рабочих станций и периферийных устройств в общую сеть – одновременное использование различных сетевых ресурсов, удалённый доступ и другое.

Настройкой активного оборудования, общего доступа и ПО, а также контролем физической целостности ЛКС занимается системный администратор. В обязанности администратора также могут входить устранение неполадок и неисправностей в сети, обеспечение информационной безопасности, подготовка и сохранений резервных копий данных, работа на первой линии поддержки (помощь пользователям в решении их проблем с рабочими станциями, так называемый «эникейщик» от англ. *any key*).

Задача данной курсовой работы – спроектировать локальную компьютерную сеть для центра обработки данных компании, занимающейся программированием. Основная цель создания локальной сети – повышение производительности труда, упрощение взаимодействия сотрудников, обеспечение доступа к общим ресурсам для всех станции, подключенных к ЛКС.

Проектирование ЛКС в рамках данной курсовой работы будет сопряжено со следующими подзадачами:

- изучить физические среды передачи данных;
- ознакомиться с принципами проектирования и построения ЛКС в промышленных масштабах;
- проанализировать способы построение физической структуры ЛКС;
- ознакомиться с правилами адресации в сети;
- изучить способы удалённого администрирования, авторизации пользователей;
- изучить рекомендации по повышению пожарной безопасности ЛКС.

1 ОБЗОР ЛИТЕРАТУРЫ

Основными источниками получения крупного багажа теоретических знаний стали источники [1,2]. Обе книги являются своего рода культовыми пособиями, в которых рассматриваются основы и технологии построения ЛКС, освещаются вопросы основных понятий, моделей и способов построения сетей, организация стека протоколов TCP/IP, создания серверов и служб для IP сетей (например DNS, DHCP, AAA и другие). Оба источника освещают вопросы маршрутизации и коммутации, однако источники [3] и [4] освещают эти вопросы намного шире, так как являются узкоспециализированной литературой по подготовке к сертификационным экзаменам CCNA.

Помимо книг одним из основных источник стал русскоязычный коллективный блок Хабр (в прошлом Хабрахабр), на котором статьи пишут сами пользователи, основываясь на личном опыте. При написании данного проекта много полезной информации было почерпано из источников [5-11]. В этих источниках описана архитектуры Router-on-a-Stick, настройка SSH на устройствах Cisco, настройка беспроводных точек доступа (в частности приведено подробное объяснение работы WPA2 и процесс конфигурации точки доступа с использованием графического интерфейса пользователя), а также описание локальных сетей с тонкими клиентами и терминальным сервером, обслуживающим сеть пользователей.

Помимо источников [8, 9] создание терминальных сетей подробно описывается в источниках [12, 13]. Информация из источника [12] основывается на реальном практическом опыте одного системного администратора в своей компании по выбору терминального сервера и, во много, основываясь на этот источник был выбран терминальный сервер для данного курсового проекта.

Одним из пожеланий заказчика было обеспечить повышенную пожарную безопасность, для чего было необходимо изучить соответствующие источники. Для выбора кабеля подходящих характеристик были изучены источники [14-17] и [22, 23], в которых описываются технические характеристики витой пары, государственный стандарт на кабельные изделия по требованиям пожарной безопасности, а также правила противопожарной безопасности при проектировании структурированной кабельной системы.

В курсовом проекте используется технология 1Gbase-X, способная дать пропускную способность сети до 1 Гб/с. Для достижения данной скорости в ЛКС необходимо использовать определённый вид обжима витой пары. Информация об обжиме прямой витой пары для Gigabit Ethernet была получена в источнике [18].

В англоязычном источнике [19] описываются технические характеристики сервера IBM x3650 M4, использующемся в курсовом проекте в качестве сервера для обслуживания тонких клиентов. Помимо технических характеристик сервера в данном источнике есть информация о его физических габаритах, что позволяет выбрать серверную стойку под этот сервер.

В источнике [20] описываются характеристики серверной стойки, предназначенной для хранения сервера IBM x3650 M4.

В источнике [21] описывается информационная розетка, которая используется в финальном монтаже локальной сети для подключения конечных устройств к локальной сети.

В источнике [23] находится краткая информация об огнестойком канальном коробе, применяющемся в курсовом проекте.

Технические характеристики принтера, подключаемого к локальной сети для нужд администраторов, описаны в источнике [24]. Инструкция по подключению принтера к локальной сети находится в источнике [30].

Характеристики используемого коммутатора Cisco SB SRW2008P описываются в источнике [25].

В источнике [26] описывается беспроводная точка доступа Cisco Aironet 1602I. На этой же странице находится инструкция по первоначальной настройке точки доступа Wi-Fi.

В источниках [27] и [28] описаны технические характеристики двух системных блоков: Jet Office 3i7, используемой в реализуемой ЛКС в качестве RADIUS-сервера, и Irwin Computers Coffee Lake G1-07, который является персональным компьютером для пользования администраторами с целью решения рабочих задач.

В источнике [29] описываются технические характеристики используемого в проекте маршрутизатора Cisco 2911.

В источниках [24 – 29], помимо технических характеристик закупаемого оборудования, приведены цены на оборудование и контактные номера телефонов компаний, реализующих данную продукция для физических и юридических лиц.

2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе пояснительной записки описывается структура организации локальной компьютерной сети для центра обработки данных и проводится обоснование её выбора.

Наиболее распространённой сетевой топологией на данный момент является топология «звезда» (схема топологии изображена на рисунке 2.1). Обычно данная топология используется в небольших локальных сетях в маленьких офисах или в домашних сетях. Центральную роль в этой топологии занимает центральное устройство, к которому подключатся остальные узлы сети. Обмен данными происходит как раз через этот центральный узел.

Такая топология имеет ряд преимуществ (простоту обслуживания и подключения новых устройств, защищённость сети, возможность использования кабелей разных типов), однако и несколько недостатков, которые нивелируются за счёт особенностей конкретной проектируемой локальной компьютерной сети.

К слабым сторонам топологии «звезда» относят наличие единой точки отказа, большое количество кабеля для подключения новых устройств и ограниченное количество устройств, которое можно подключить. Использование дорогого коммутатора компании Cisco с высокой отказоустойчивостью, а также уверенность в том, что в дальнейшем расширение сети не планируется, позволяет с уверенностью выбрать именно эту сетевую топологию для реализации в курсовом проекте.

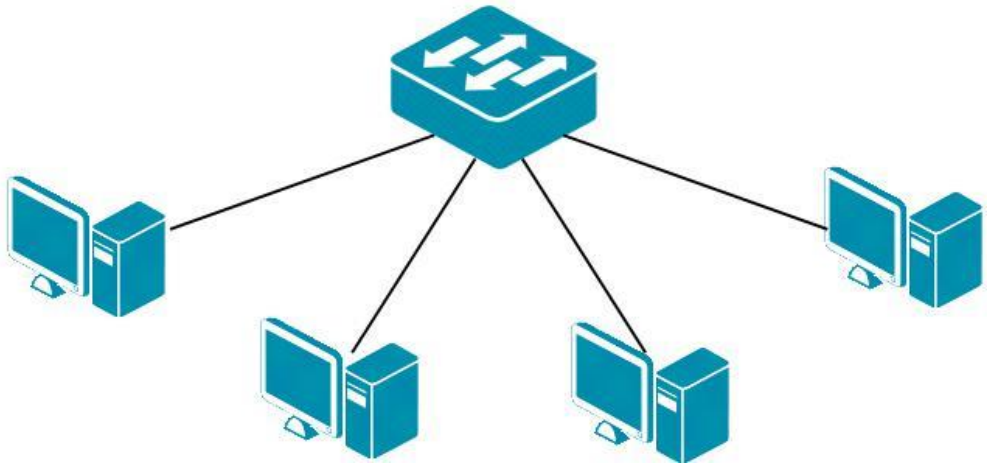

Рисунок 2.1 – Топология «звезда»

Так как в центре обработки данных есть физическое разделение оборудования на два различных помещения – серверную комнату и отдел администрирования – логично применить виртуальные локальные подсети (VLAN). Такое разделение на виртуальные локальные подсети позволяет определять некоторые политики безопасности непосредственно для VLAN, а не для каждой станции и сервера по отдельности, а также упрощает понимание

устройства и структуры ЛКС за счёт абстрагирования от каждой конкретной станции, позволяя рассматривать их целостно, в совокупности.

Для достижения большей степени административного контроля и логического разделения среды передачи данных было принято решение распределить пользовательские станции и сервера следующим образом:

1. VLAN №99 – административный VLAN, выделенный под рабочие станции, принтер и беспроводной маршрутизатор.
2. VLAN №10 – VLAN, выделенный под серверное оборудование.

2.1 Виртуальная сеть для администраторов

В данной структурной единице ЛКС находятся устройства, расположенные в помещении отдела администрирования. К их числу относятся пользовательские станции администраторов, цветной принтер и беспроводной маршрутизатор, обеспечивающий доступ к сети с портативных устройств администраторов (ноутбуки, смартфоны и другие). Все устройства, расположенные в кабинете, подключены к одному коммутатору. Беспроводные устройства, подключенные к точке доступа, хоть и физически находятся в другой подсети, она относится к виртуальной сети для администраторов.

2.2. Виртуальная сеть серверной комнаты

В данной структурной единице ЛКС находятся основной и запасной сервер для обслуживания тонких клиентов, а также AAA-сервер, предназначенный для ограничения доступа к локальной сети. Равно как и устройства в отделе администрирования, все серверы подключены к главному коммутатору.

3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

На этапе функционального проектирования в данном разделе описывается функционирование программной и аппаратной составляющей проектируемой ЛКС. Детально изучить топологию и структуру разрабатываемой локальной компьютерной сети можно в приложении Б.

3.1 Обоснование выбора сетевой операционной системы

В виду разработки полноценной коммерческой сети и получения большого объёма как практической, так и теоретической информации, касающейся оборудования Cisco, была выбрана проприетарная операционная система Cisco IOS. Данная операционная система используется во всех устройствах компании Cisco и является примером для подражания многим более бюджетным компаниям за счёт своей строгой структуры и, одновременно с этим, интуитивной простоты использования и настройки оборудования. Для взаимодействия администратора с оборудованием используется интерфейс командной строки, который предлагает пользователю набор команд в зависимости от уровня абстракции, на котором он находится, и уровня привилегий, который есть у пользователя. Некоторые устройства компании поддерживают графический интерфейс пользователя, однако интерфейс командной строки является классическим для системных администраторов и общепринятой методикой настройки оборудования Cisco.

Cisco IOS является многозадачной ОС и занимается управлением программными и аппаратными ресурсами на маршрутизаторах, коммутаторах и других устройствах, равно как и любая операционная система. Она отвечает за выделение памяти, работу с процессами, работу с внутренней файловой системой. Эти аспекты работы не касаются пользователя.

Особенностью работы с Cisco IOS является то, что для многих маршрутизаторов существует несколько различных образов IOS. Такой образ является файлом формата .img, содержащий всю операционную систему для маршрутизатора. В зависимости от модели маршрутизатора и функций внутри IOS компания Cisco создаёт различные образы IOS. Однако логично предположить, что чем больше функций содержит в себе образ ОС, тем больше внутренней и оперативной памяти требует такая операционная система для её загрузки и хранения.

3.3 Обоснование выбора сетевого оборудования

В сетях происходит пакетная передача данных и важно правильно обработать каждый пакет, узнать источник и пункт назначения пакета, узнать данные, которые он хранит в себе, а также обеспечить целостность пакета и передаваемой им информации и доставить пакет в место назначения. Эту задачу берёт на себя активное сетевое оборудование. Выбор сетевого

оборудования очень важен, так как от него зависит правильность функционирования всей локальной сети, поэтому к нему стоит подойти ответственно.

На данный момент компания Cisco предоставляет самый широкий выбор коммутаторов, маршрутизаторов и другого сетевого оборудования. По данным за 2016 год Cisco контролирует 56% рынка активного сетевого оборудования, что говорит о высоком уровне и качестве. Однако за хорошую технику нужно платить: оборудование компании стоит заметно дороже по сравнению с другими устройствами, но эта переплата стоит того, когда дело касается серьёзных коммерческих сетей, где важна скорость работы и отказоустойчивость. С учётом вышеизложенного и пожеланий заказчика в ходе проектирования ЛКС было принято использовать именно оборудование компании Cisco.

Одним из пожеланий заказчика было подключение сервера для обслуживания до 100 тонких клиентов, следовательно в проекте необходимо было предусмотреть высокую пропускную способность пассивного и активного оборудования.

При одновременном подключении ста тонких клиентов к серверу минимальная скорость соединения, которую нужно обеспечить для потоковой передачи, около 4 Мбит/с на одного пользователя. В таблице 3.1 приведено сравнение интерфейсов локальной сети по их пропускной способности.

Таблица 3.1 – Интерфейсы локальных сетей

Интерфейс	Пропускная способность
Ethernet (10BASE-X)	10 Мбит/с
Fast Ethernet (100BASE-X)	100 Мбит/с
Gigabit Ethernet (1000BASE-X)	1 Гбит/с
10-гигабитный Ethernet (10Gbase-X)	10 Гбит/с
40-гигабитный Ethernet (40Gbase-X)	40 Гбит/с
100-гигабитный Ethernet (100Gbase-X)	100 Гбит/с

Проанализировав таблицу и исходя из необходимой для корректной работы пропускной способности сети было принято решение выбирать сетевое оборудование с интерфейсами Gigabit Ethernet.

1. Маршрутизатор Cisco 2911.
2. Беспроводная точка доступа Cisco Aironet 1602I.
3. Коммутатор Cisco SB SRW2008P.

3.3.1 Маршрутизатор Cisco 2911

Для пересылки пакетов между различными подсетями используется маршрутизатор. В общем случае маршрутизатор получает пакет и, используя адрес получателя и таблицу маршрутизации, определяет куда необходимо

передать пакет данных. В случае, если в таблице маршрутизации отсутствует путь перенаправления пакеты, то он отбрасывается.

Для использования в разрабатываемой компьютерной сети было принято решение использовать маршрутизатор модели Cisco 2911. Данный маршрутизатор перенаправляет пакеты с терминального сервера в сеть Metro Ethernet и наоборот, перенаправляет пакеты из MAN-сети для обработки на терминальный сервер. Данный маршрутизатор отличается относительно небольшой стоимостью и наличием 3 портов Gigabit Ethernet, необходимых для реализации сети. Маршрутизатор поддерживает удалённое администрирование, следовательно им можно будет управлять, подключившись при помощи SSH с административной пользовательской станции.

Рисунок 3.1 – Маршрутизатор Cisco 2911

3.3.2 Беспроводная точка доступа Cisco Aironet 1602I

Беспроводная точка доступа используется для подключения к сети беспроводных устройств по технологии Wi-Fi. Данная точка доступа является одной из самых бюджетных из тех, что предлагает компания Cisco для малого и среднего бизнеса. Она поддерживает используемый в сети протокол аутентификации WPA2, поддерживает питание посредством PoE, а также настраивается при помощи графического интерфейса пользователя. Всё это позволяет принять решение для её использования.

Рисунок 3.2 – Беспроводная точка доступа Cisco Aironet 1602I

3.3.3 Коммутатор Cisco SB SRW2008P

Если маршрутизатор используется для разделения устройств на сегменты (подсети), то коммутатор нужен наоборот, для объединения нескольких устройств в одну подсеть. В данной курсовой работе он служит именно с этой целью: соединить отдел администрирования и серверную комнату в одну подсеть. При этом использование VLAN позволяет логически разделить оба помещения в пределах одной подсети.

Коммутатор Cisco SB SRW2008P является моделью, предназначенной для организации локальной компьютерной сети малых и средних размеров. Относительная дешевизна, наличие 10 портов Gigabit Ethernet, возможность управления и мониторинга коммутатора через веб-интерфейс делают выбор этого коммутатора очевидным и разумным.

Рисунок 3.3 – Коммутатор Cisco SB SRW2008P

3.4 Обоснование выбора серверного оборудования

3.4.1 Обоснование выбора терминального сервера

В настоящее время активно развиваются компьютерные сети, основанные на «тонких» клиентах и терминальном доступе. Это связано с минимальными необходимыми вложениями для создания инфраструктуры. Технически построение сети на основе терминального доступа представлена рисунке 3.4.

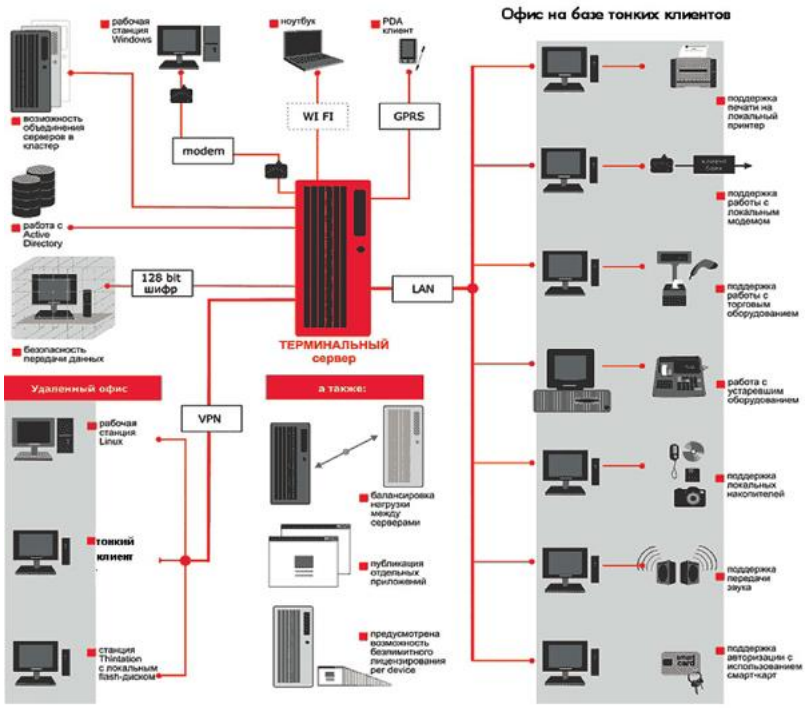

Рисунок 3.4 – Варианты решений на основе терминальной сети.

Работа терминальной сети значительным образом отличается от работы классической компьютерной сети. Терминальный режим подразумевает наличие «тонких» клиентов – это максимально упрощённая версия настольного персонального компьютера. Он значительно меньше по размерам, в нём отсутствуют жёсткий диск, вентиляция, оптический привод. Используются так называемые «холодные» процессоры, которые не требуют активного охлаждения и сильно не нагреваются в процессе работы.

Пользователю на экран приходит лишь изображение экрана, которое обрабатывается на сервере. От пользователя на сервер поступают команды устройств ввода (клавиатура, мышь), терминальный сервер занимается обработкой полученных данных и, в соответствии с ними, изменением изображения на экране пользователя. На самом сервере хранятся приложения, файловые сервисы, базы данных и другие необходимые пользователям сервисы.

В качестве терминального сервера выбор пал на сервер IBM x3650 M4 (рисунок 3.5).

Рисунок 3.5 – IBM x3650 M4

Основные характеристики сервера описаны ниже:
- процессор E5-2620v2 6 ядер 2.1 Гц;
- оперативная память 64 Гб;
- блок питания 2 х 550 Вт;
- 2 диска SSD по 256 Гб;
- 6 дисков по 600 Гб.

Данных характеристик сервера вполне хватит для обслуживания до сотни «тонких» клиентов.

По условию задания необходимо приобрести два таких сервера: один основной и один запасной. Целесообразно разместить их на разных серверных стойках во избежание порчи одновременно двух серверов.

3.4.2 Обоснование выбора RADIUS-сервера

RADIUS-сервер в данной ЛКС используется для хранениях учётных записей администраторов, использующих беспроводной доступ к сети, и обеспечения их доступа к сети.

В рамках проектируемой сети можно обойтись без специализированного сервера, а использовать в его качестве стационарный персональный компьютер, вычислительной мощности которого вполне хватит для обеспечения работы сопутствующего ПО. Выбор пал на бюджетный компьютер Jet Office 3i7, позиционирующий себя как офисный ПК. Процессора Intel Core i3 7100 3900 МГц, 4 Гб оперативной памяти и графического ускорителя Intel HD Graphics 630 будет достаточно для нормальной работы сервера.

3.5 Организация рабочих мест

Под рабочим местом следует понимать выделенную часть площади с расположенным на ней технологическим оборудованием и инвентарём, необходимым для выполнения работы. Рабочее место – это первичная ячейка производственной структуры предприятия.

В рамках проекта организация рабочего места не является трудной задачей. Рабочий места администраторов необходимо обеспечить персональными компьютерами и, по требованию заказчика, принтером.

3.5.1 Обоснование выбора рабочей станции администратора

Основной задачей при организации рабочих мест администраторов была обеспечить комфортные условия работы для сотрудников. В первую очередь рабочие станции должны быть оснащены сетевыми адаптерами с возможностью подключения к LAN и быть достаточно мощными для выполнения всех поставленных задач. Выбор пал на компьютеры Irwin Computers Coffee Lake G1-07. Характеристики данного персонального компьютера можно увидеть в таблице 3.2.

Таблица 3.2 – Технические характеристики Irwin Computers Coffee Lake G1-07

Процессор	Intel Core i5 9400F 2900МГц
Оперативная память	DDR4 16 ГБ
HDD	1000 ГБ
SSD	240 ГБ
Видеокарта	NVIDIA GeForce GTX 1660 6 ГБ

3.5.2 Обоснование выбора принтера

По требованию заказчика в проектируемой локальной сети необходимо наличие принтера для его использования администраторами. Ознакомившись с рынком принтеров был выбран цветной лазерный принтер Ricoh SP C260DNw (рисунок 3.6). Данный принтер имеет возможность быть подключенным к локальной сети либо к беспроводной сети Wi-Fi. Также принтеры компании Ricoh имеют удобный web-интерфейс, попасть в который можно набрав в адресной строке браузера IP-адрес принтера. Он позволяет удалённо посмотреть состояние аппарата, значение счётчиков, а также остаток тонера.

Рисунок 3.6 – Принтер Ricoh SP C260DNw

3.6 Обоснование выбора пассивного сетевого оборудования

К пассивному сетевому оборудованию относят оборудование, которое не питается от электрической сети или других источников питания. К этому виду оборудования относят кабельную систему, информационные розетки, а также кабельные коробы и монтажные шкафы.

3.6.1 Витая пара прямого типа

Кабель «витая пара» имеет несколько категорий, нумеруемых от 1 до 8, которые определяют эффективный пропускаемый частотный диапазон. С категориями кабеля можно ознакомиться в таблице 3.3.

Таблица 3.3 – Категории кабеля «витая пара»

Категория	Полоса частот, МГц	Применение
1	0,1	Телефонные и старые модемные линии
2	1	Старые терминалы
3	16	10BASE-T, 100BASE-T4 Ethernet
4	20	Token ring
5/5e	100	Fast Ethernet, Gigabit Ethernet
6	250	10 Gigabit Ethernet
6A	500	10 Gigabit Ethernet
7	600	10 Gigabit Ethernet
7A	1000	10 Gigabit Ethernet
8/8.1	1600-2000	100 Gigabit Ethernet
8.2	1600-2000	100 Gigabit Ethernet

Одним из пожеланий заказчика является обеспечение пожарной безопасности сети. Исходя из этого пожелания для прокладки кабельной системы необходимо придерживаться ГОСТ 31565-2012 «Кабельные изделия. Требования пожарной безопасности». Согласно нему существует несколько типов исполнения кабельных изделий, перечисленные в таблице 3.4.

Таблица 3.4 – Типы исполнения кабельных изделий.

Тип исполнения кабельного изделия	Расшифровка типа
Без обозначения	Кабельные изделия, не распространяющие горение при групповой прокладке
LS	Кабельные изделия, не распространяющие горение при групповой прокладке, с пониженным дымо- и газовыделением

HF	Кабельные изделия, не распространяющие горение при групповой прокладке и не выделяющие коррозионно-активных газообразных продуктов при горении и тлении
FRLS	Кабельные изделия огнестойкие, не распространяющие горение при групповой прокладке, с пониженным дымо- и газовыделением
FRHF	Кабельные изделия огнестойкие, не распространяющие горение при групповой прокладке и не выделяющие коррозионно-активных газообразных продуктов при горении и тлении
LSLTx	Кабельные изделия, не распространяющие горение при групповой прокладке, с пониженным дымо- и газовыделением и с низкой токсичностью продуктов горения
HFLTx	Кабельные изделия, не распространяющие горение при групповой прокладке, не выделяющие коррозионно-активные газообразные продукты при горении и тлении и с низкой токсичностью продуктов горения
FRLSLTx	Кабельные изделия огнестойкие, не распространяющие горение при групповой прокладке, с пониженным дымо- и газовыделением и с низкой токсичностью продуктов горения
FRHFLTx	Кабельные изделия огнестойкие, не распространяющие горение при групповой прокладке, не выделяющие коррозионно-активных газообразных продуктов при горении и тлении и с низкой токсичностью продуктов горения

Исходя из вышеописанного было принято решение организовать кабельную систему на основе кабеля категории 5е в огнестойкой оболочке из низкотоксичного ПВХ пластика пониженной пожарной опасности с низким дымо- и газовыделением категории FRLSLTx.

Все соединения в данной локальной сети (маршрутизатор – коммутатор, коммутатор – конечное устройство) реализованы витой парой с коннекторами RJ-45 прямого типа. Вариант обжима прямого кабеля для Gigabit Ethernet представлен на рисунке 3.7.

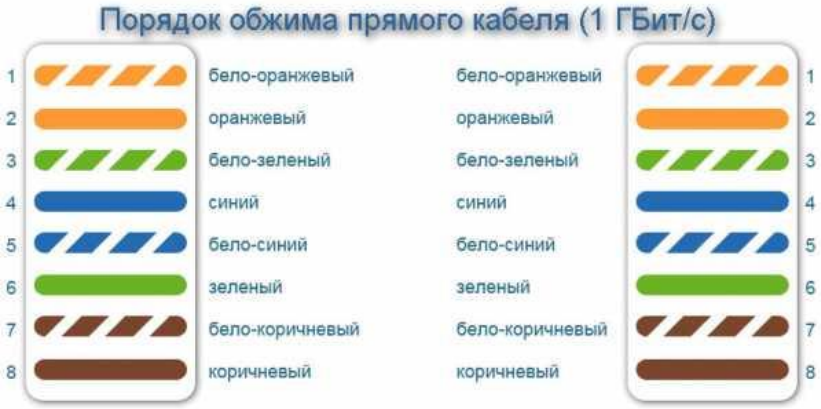

Рисунок 3.7 – Схема обжима прямого кабеля Gigabit Ethernet

3.6.2 Обоснование выбора информационных розеток

Для подключения устройств к сети необходимо обеспечить доступность устройств к кабелю. Удобно и эстетично организовать доступ позволяет монтаж информационных розеток RJ-45. Недорогим вариантом информационных розеток являются отечественные Этюд Кома-001К, обеспечивающие доступ к сети.

3.6.3 Обоснование выбора кабельного короба

Учесть пожелание заказчика, касающееся пожарной безопасности, труднее при выборе кабельного короба. Большинство производителей делают кабельные коробы из легковоспламеняющегося ПВХ без особого внимания к огнестойкости, однако во время поиска подходящего короба на белорусском рынке были найдены огнеупорные каналы ЭкоПласт МЕХ Е15-Е110. Маркировка «Е15-Е110» означает, что изделие выдерживает напор огня от 15 до 110 минут, чего вполне хватит для удовлетворения потребностей заказчика, касающейся пожарной безопасности.

3.6.4 Обоснование выбора монтажных стоек

Для размещения терминальных серверов необходимо приобрести две серверные стойки исходя из размеров терминального сервера (445 мм в ширину, 746 мм в глубину). Под данные габариты подойдёт двухрамная стойка TWT-RACK2-33U (рисунок 3.8). Стойки нужно приобрести в количестве двух штук.

Рисунок 3.8 – Серверная стойка TWT-RACK2-33U

3.7 Описание настройки компонентов локальной сети

3.7.1 Разделение сети на виртуальные локальные подсети

Для достижения большей степени административного контроля и логического разделения среды передачи данных было принято решение разделить устройства, подключенные к сети, на две группы: серверное оборудование и оборудование администраторов.

Рассмотрим процесс создания и настойки административного VLAN на коммутаторе:

1. Создаём административный VLAN.
2. Назначаем порты, к которым подключены конечные устройства, access портами с указанием номера VLAN.

Команды настройки VLAN №99 в Cisco IOS по алгоритму, описанному выше, выглядит так:

```
Switch(config)#vlan 99
Switch(config-vlan)#name Admin
Switch(config-vlan)#exit
Switch(config)#interface range g0/4-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 99
```

Аналогично конфигурируется VLAN №10 для серверной комнаты, разница в номере VLAN и в диапазоне интерфейсов (`interface range g0/1-3`).

В целях безопасности можно прописать port-security на интерфейсах, предназначенных для администраторов. Аналогично настраивается виртуальная подсеть и для серверной комнаты.

Для настройки Inter-VLAN маршрутизации необходимо назначить порт, идущий к маршрутизатору, trunk портом и разрешить прохождение по нему тегированного трафика для 10 и 99 VLAN:

```
Switch(config)#interface g0/0
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10, 99
```

3.7.2 Настройка удалённого администрирования

Согласно заданию, необходимо настроить удалённое администрирование. На данный момент существует большое количество технологий, позволяющих настроить удалённое администрирование, однако основными в Cisco являются Telnet и SSH.

Telnet получил большое распространение в первую очередь в Unix-подобных системах. Сервис позволяет создать удалённого пользователя при

помощи логина и пароля, по которым предоставляется вход в систему. Затем пользователь может удалённо запускать программы или задавать системные команды.

Сетевой протокол SSH (Secure Shell) в отличие от Telnet шифрует все передаваемые данные (в том числе и пароли), что делает его лучшим вариантом, чем Telnet. Шифрование паролей и конфигурационных файлов особенно важно при работе на удалённой пользовательской станции.

Для настройки SSH на маршрутизаторе необходимо подключиться к нему и выполнить следующие пункты:

1. Установит дату и время (необходимо для генерации ключа).
2. Указать домен и имя устройства.
3. Сгенерировать ключ для SSH.
4. Указать шифрование пароля.
5. Создать пользователя с максимальными привилегиями и задать пароль для привилегированного режима.
6. Активировать протокол AAA.
7. Разрешить компьютерам внутренней сети получать доступ к маршрутизатору по SSH.
8. Запретить в режиме конфигурирования терминальных линий всё, кроме SSH.
9. Активировать автоматическое поднятие строки после ответа системы на проделанные изменения, позволить входить сразу в привилегированный режим, настроить автоматическое закрытие SSH сессии через 60 минут.
10. Привязать группу доступа, созданную на шаге 7, к терминальной линии.

Команды настройки SSH приведены ниже:

```
Router#clock set 00:09:04 03 Dec 2019
Router#configure terminal
Router#(config)ip domain name aoks.local
Router#(config)crypto key generate rsa
Router#(config)service password-encryption
Router#(config)username admin privilege 15 secret ********
Router#(config)enable secret ********
Router#(config)aaa new-model
Router#(config)access-list 23 permit 172.17.1.0 0.0.0.255
Router#(config)line vty 0 4
Router#(config-line)transport input ssh
Router#(config-line)logging synchronous
Router#(config-line)privilege level 15
Router#(config-line)exec-timeout 60 0
Router#(config-line)access-class 23 in
```

На этом настройка SSH завершена. Для получения удалённого доступа администратору необходимо лишь установить клиент для протоколов удалённого доступа (например PuTTY). Необходимо выбрать тип соединения

«SSH» и указать IP-адрес маршрутизатора в подсети. Также нужно проверить порт – протокол SSH обычно прослушивает соединения на TCP-порту 22. Пример полностью заполненного окна конфигурации представлен на рисунке 3.8.

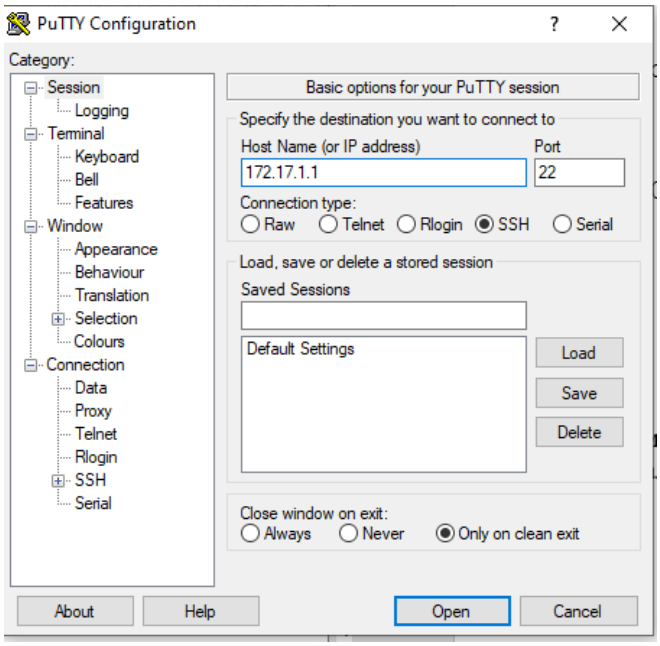

Рисунок 3.8 – Настройка сессии удалённого соединения

3.7.3 Настройка AAA-сервиса и внешнего сервера авторизации

AAA (сокращение от английского Authentication, Authorization and Accounting) – как следует из расшифровки аббревиатуры, система аутентификации, авторизации и учёта событий, встроенная в Cisco IOS. Эта система предоставляет пользователям безопасный удалённый доступ к сетевому оборудованию, например к беспроводным маршрутизаторам. Система занимается сбором и отправкой информации на сервер, аутентификацией пользователей и их авторизацией.

Аутентификация – процесс идентификации пользователя по паре «логин - пароль». Аутентификация определяет, каким образом клиент будет представляться беспроводной точке доступа. Для использования в курсовой работе был выбран протокол EAP, определяющий подлинность подключаемого устройства внешним сервером.

Авторизация – предоставление возможностей пользователю для удалённого доступа.

Аккаунтинг – служба, занимающаяся сборов и отправкой информации на сервер. Используется для составления отчётности, для биллинга (обработка платежей, работа с тарификацией и выставлением счетов пользователям) и для аудита. Может включать в себя различные данные, например время начала и окончания сессии, количество отправленных или полученных пакетов или байт и другое.

Очевидно, что Немаловажную роль в защищённом доступе играет шифрование данных. В настоящее время широко известны технологии WEP, WPA и WPA2. WEP-шифрование использовать категорически не рекомендуется в связи с тем, что оно было скомпрометировано. Разница между WPA и WPA2 лишь в алгоритме шифрования (TKIP или AES). Так как AES является более совершенным алгоритмом шифрования, чем TKIP, было решено выбрать его.

WPA2 Personal и WPA2 Enterprise различаются тем, откуда берутся ключи шифрования. В первом случае используется статический ключ, который задаётся в настройках точки доступа. Такой ключ является общедоступным для всех пользователей точки и может быть легко скомпрометирован, что повлечёт за собой смену паролей у всех пользователей. Динамический ключ используется для корпоративного применения во избежание таких ситуаций. Ключ может обновляться по ходу работы, при этом не разрывая текущее соединение. За генерацию ключа отвечает дополнительный компонент системы – сервер авторизации. Это может быть RADIUS-сервер, TACACS, TACACS+ и другие. Работа RADIUS-сервера показана на рисунке 3.9.

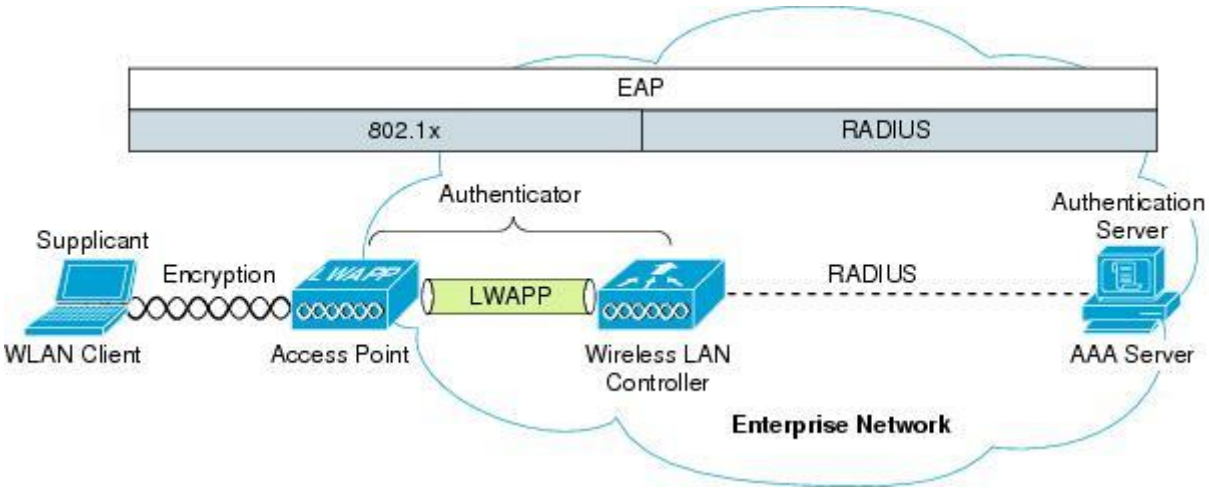

Рисунок 3.9 – Общая схема работы AAA-сервера

Использование шифрования WPA2 Enterprise подразумевает наличие в сети RADIUS-сервера. Учитывая разработку ЛКС для полноценной коммерческой сети целесообразно использовать проприетарный продукт Cisco Secure Access Control Server (ACS) в стеке с ПК Jet Office 3i7. Cisco Secure ACS – программный продукт, конфигурирующийся через веб-интерфейс, позволяющий создавать и управлять мощными, надёжными и отказоустойчивыми системами.

Для настройки AAA на сервере необходимо установить на него Cisco Secure ACS. Установка программы не должна вызвать трудностей. Для перехода к настройкам серверам необходимо в адресную строку браузера ввести IP-адрес сервера, откроется web-интерфейс, после прохождения

авторизации в котором будут доступны настройки AAA. Изображение интерфейса представлено на рисунке 3.10.

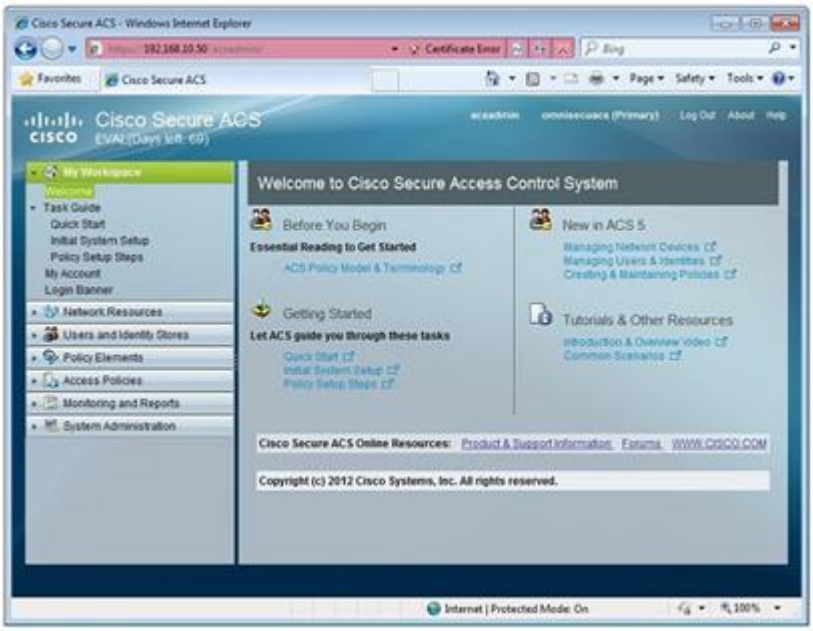

Рисунок 3.10 – Web-интерфейс Cisco Secure ACS

Для настройки сервера RADIUS необходимо перейти во вкладку «Network Resources», выбрать там подкатегорию «AAA», далее «AAA Servers and Groups», затем выбрать «Servers». Откроется список созданных серверов. Для создания нового сервера необходимо нажать кнопку «Add» и настроить новый сервер: выбрать тип сервера «RADIUS», назначить IP сервера 172.17.1.12, проверить порт авторизации и порт аккаунтинга (обычно это 1645 и 1646, стандартные порты для Cisco) и задайте ключ конфигурации (его необходимо запомнить для дальнейшей настройки). По нажатию «ОК» начинается процесс создания сервера, окно становится неактивно. В случае успешного создания сервера окно конфигурирования закроется, новый RADIUS-сервер появится в списке серверов.

Для управления пользователями необходимо нажать на вкладку «Users and Identity Stores», затем «Internal Identity Stores» и «Users». Для создания и добавления пользователя необходимо кликнуть на кнопку «Create» (рисунок 3.11).

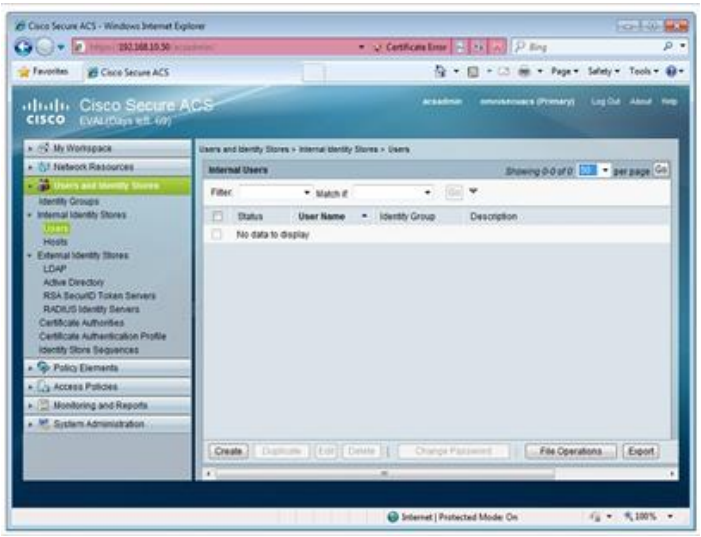

Рисунок 3.11 – Список пользователей в Cisco Secure ACS

Далее необходимо заполнить имя пользователя, выставить статус «Enabled» и ввести пароль пользователя (рисунок 3.12). При необходимости можно заполнить описание пользователя и определить для него группу, но для маленькой сети это имеет не много смысла.

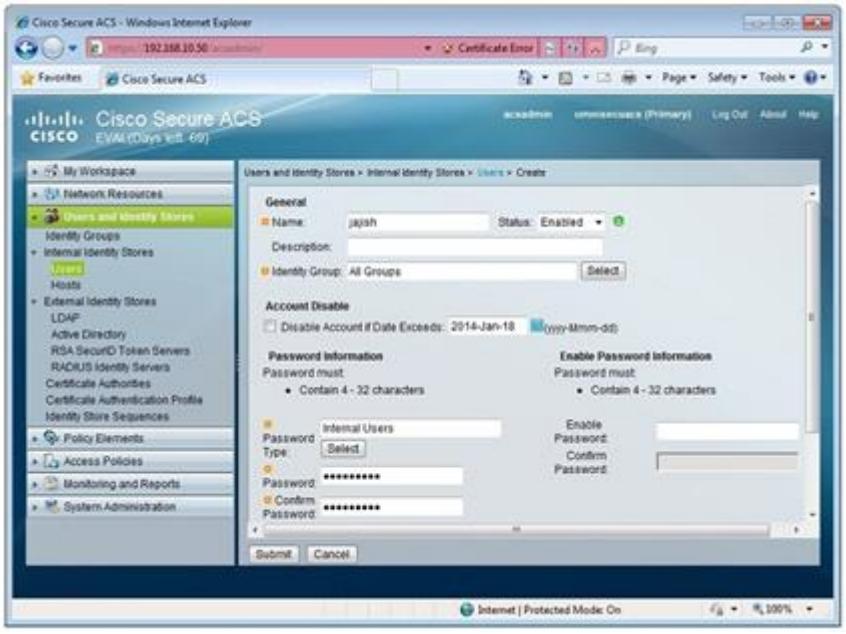

Рисунок 3.12 – Создание нового пользователя в Cisco Secure ACS

По нажатию на кнопку «Submit» создание пользователя будет завершено, окно будет закрыто, отобразится список всех пользователей (рисунок 3.13). На этом процесс создания пользователя завершается.

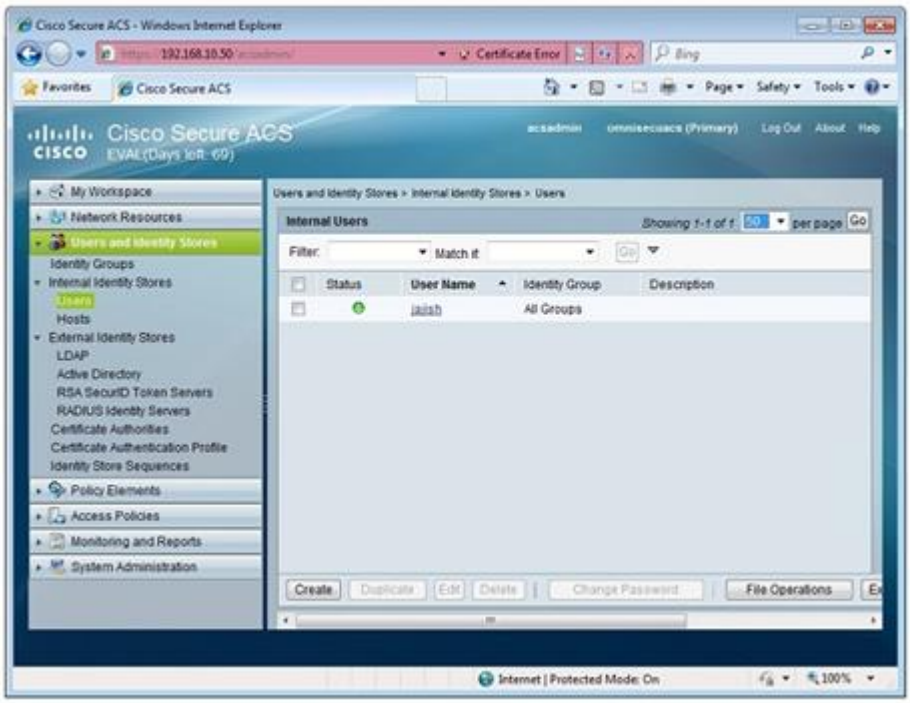

Рисунок 3.13 – Обновлённый список пользователей после создания одного из них в Cisco Secure ACS

3.7.4 Настройка беспроводной точки доступа

Для использования беспроводной точки доступа её необходимо заранее настроить. Для перехода к графическому интерфейсу настройки необходимо в адресной строке браузера ввести IP-адрес точки доступа (172.17.1.6).

На вкладке «General» необходимо ввести SSID точки доступа (имя, по которому происходит подключение к сети), шлюз по умолчанию (172.17.1.1), IP-адрес точки доступа в рамках подсети в текстовом поле «Internet IP Address» (172.17.1.6) и адрес внутри WAN в текстовом поле «Router IP Address» (172.17.3.1).

Перейдём к настройке шифрования, для этого нужно перейти на вкладку WLAN и выбрать «Create New». В открывшемся окне нужно выбрать вкладку «Security», в ней «Layer 2». В окне настройки безопасности выбрать тип шифрования «WPA+WPA2», отметить чекбокс «WPA2 Policy-AES» и «802.1X Enable» (рисунок 3.14).

Рисунок 3.14 – Окно настройки WLAN

Далее необходимо настроить доступ к AAA-серверу на беспроводной точке доступа. Для этого, не покидая вкладки «Security», следует нажать на вкладку «AAA Servers», выбрать вид аутентификации «RADIUS Authentication», кликнуть «New», после чего перейти к настройке сервера (рисунок 3.15).

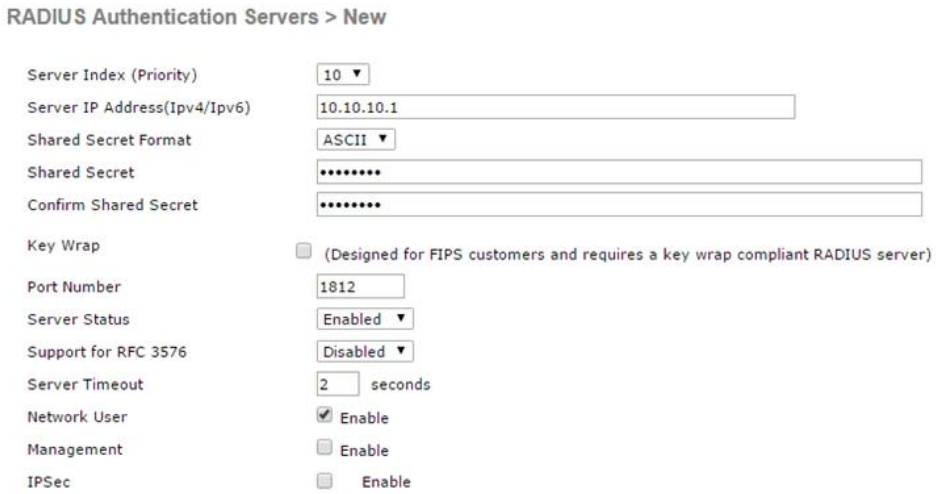

Рисунок 3.15 – Окно настройки RADIUS-сервера

Здесь необходимо указать IP-адрес RADIUS-сервера (172.17.2.14), ввести ключ RADUIS-сервера, вводимый ранее, изменить порт по умолчанию на порт 1645, проверить статус сервера и после этого нажать «ОК».

Для автоматического назначения IP-адресов подключаемым устройствам нужно настроить работу DHCP.

DHCP – это протокол, позволяющий раздавать IP-адреса подключаемым устройствам. Он позволяет упростить процесс выдачи адресов, перекладывая эту работу на сторону сервера. Точка доступа Cisco Aironet 1602I поддерживает протокол DHCP, для его настройки также необходимо воспользоваться графическим интерфейсом пользователя.

Во вкладке «General» необходимо пролистать вниз до «DHCP Server Settings». В окне настройки нажать кнопку «Enable» напротив «DHCP Server», выбрать начальный IP-адрес для раздачи (например, 172.17.3.5), и выбрать максимальное количество пользователей (с учётом размеров сети десяти пользователей будет достаточно).

На этом настройка беспроводной точки доступа закончена.

3.7.5 Настройка принтера

Для подключения принтера к локальной сети необходимо подключиться к нему с административной станции при помощи USB-кабеля и запустить установку драйверов с установочного диска, идущего в комплекте. В окне с предложением выбрать тип подключения выберите «Сетевое подключение» (рисунок 3.16).

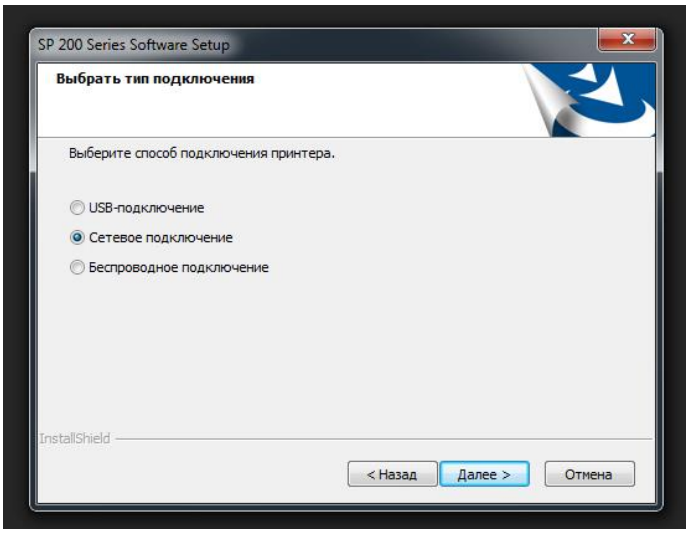

Рисунок 3.16 – Выбор типа подключения принтера

Далее следует перейти к ручной настройке сети принтера. В открывшемся окне необходимо задать наличие/отсутствие DHCP, IP-адрес, маску подсети и шлюз. После настройки принтера можно воспользоваться его web-интерфейсом, введя в адресной строке браузера IP-адрес принтера (рисунок 3.17). В web-интерфейсе информация о количестве тонера, очереди документов и другом.

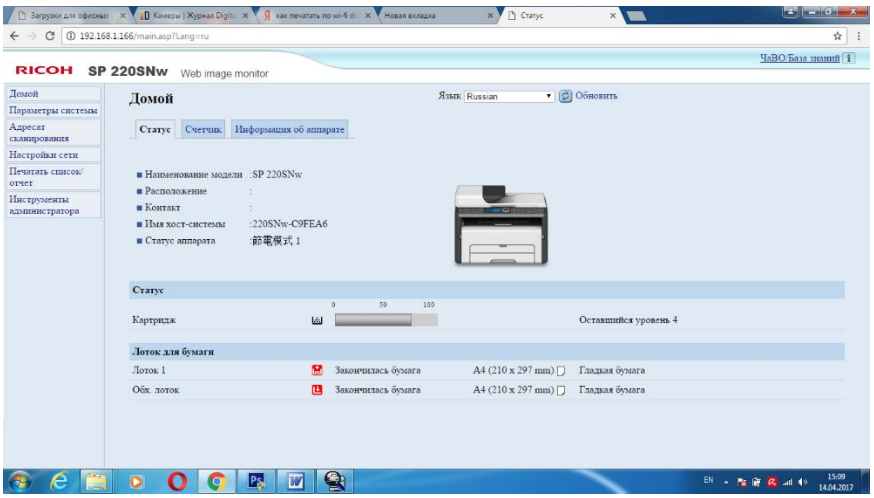

Рисунок 3.17 – Web-интерфейс принтера Ricoh SP C260DNw

3.7.6 Настройка персональных компьютеров

Персональные компьютеры администраторов подключаются посредством Ethernet. Для настройки администраторских ПК необходимо зайти в панель управления, выбрать раздел «Сеть и Интернет», в разделе «Сетевые подключения» нажать кнопку «Изменение настроек адаптера». В открывшемся окне перейти к настройкам Ethernet, нажать на «IP версии 4», на кнопку свойства и задать в открывшемся окне свойств IP-адрес компьютера, маску подсети и основной шлюз. Пример настройки представлен на рисунке 3.18. После успешной настройки изображение красного крестика пропадёт.

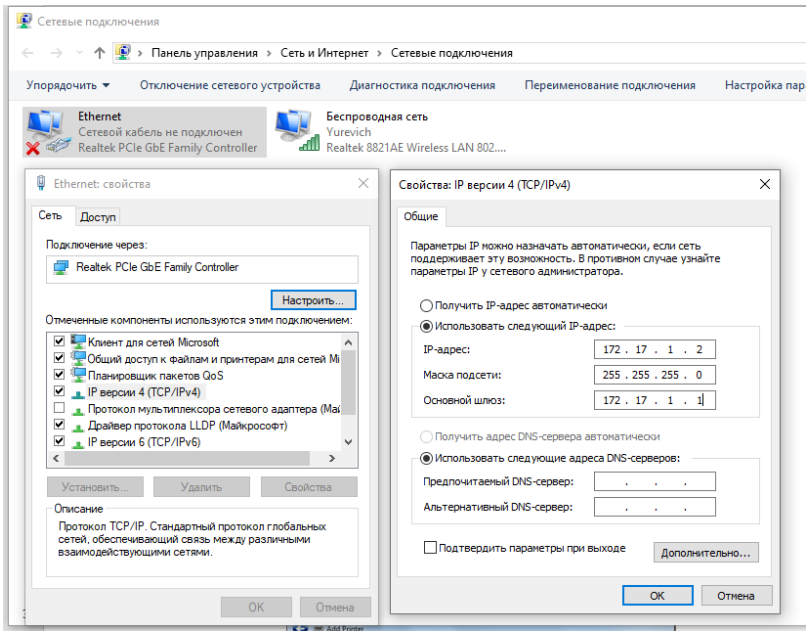

Рисунок 3.18 – Настройка IPv4 на ПК

Аналогичным образом настраивается и IPv6 адрес, пример настройки на рисунке 3.19.

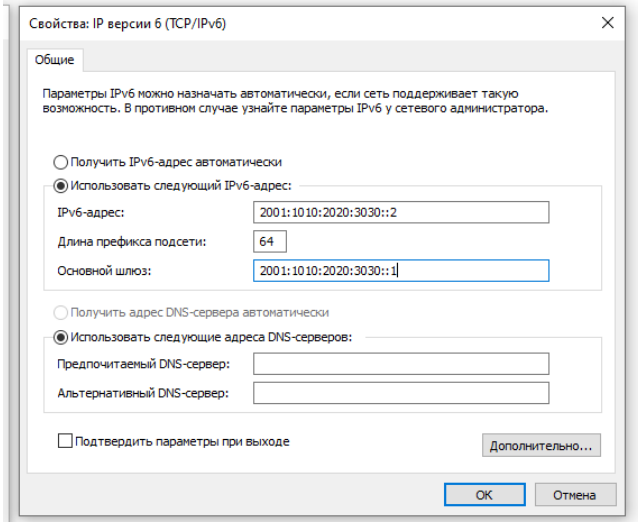

Рисунок 3.19 – Настройка IPv6 на ПК

Процедуру настройки адресов необходимо повторить на всех административных персональных компьютерах.

3.7.7 Настройка маршрутизатора

Для маршрутизации пакетов между отделом администрирования и серверной комнатой необходимо настроить Inter-VLAN Routing. Исходя из особенностей топологии и имеющегося в пользовании оборудовании целесообразно применить метод маршрутизации между VLAN «Router-on-a-Stick».

Суть данного метода сводится к использованию одного физического интерфейса для создания подмножества логических виртуальных интерфейсов, что позволяет обеспечить маршрутизацию. Подобным образом работают коммутаторы, разделяя локальную сеть на множество виртуальных подсетей.

Для реализации Inter-VLAN Routing на интерфейсе роутера необходимо создать подинтерфейсы по количеству VLAN, определить стандарт инкапсуляции и соответствующий подинтерфейсу IP-адрес.

Полный набор команд для настройки Inter-VLAN Routing выглядит следующим образом:

```
Router#configure terminal
Router(config)#interface g0/1.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 172.17.2.1 255.255.255.0
Router(config-subif)#interface g0/1.99
Router(config-subif)#encapsulation dot1q 99
Router(config-subif)#ip address 172.17.1.1 255.255.255.0
Router(config-subif)#interface g0/1
Router(config-if)#ip address 172.17.1.10 255.255.255.0
Router(config-if)#no shutdown
```

Для маршрутизации пакетов в подсеть 172.17.3.0/24 необходимо настроить на роутере путь в подсеть. Для маршрутизации пакетов в MAN необходимо настроить в неё путь по умолчанию:

```
Router(config)#ip route 172.17.3.0 255.255.255.0 172.17.1.6
Router(config)#ip route 0.0.0.0 0.0.0.0 g0/0
```

Для использования IPv6 необходимо задать IPv6 адрес на интерфейсе, разрешить маршрутизацию и задать путь по умолчанию в MAN:

```
Router(config)#interface g0/1
Router(config-if)#ipv6 address 2001:1010:2020:3030::1/64
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 route ::/0 g0/0
```

3.8 Адресация в локальной компьютерной сети

По условию задания в разрабатываемой ЛКС необходимо осуществить адресацию с применение протоколов IPv4 и IPv6. Протокол адресации IPv4 использует четырёхбайтные адреса, ограничивающие адресное пространство. Традиционно адрес IPv4 записывается четырьмя десятичными числами от 0 до 255, разделёнными точками, через дробь указывается длина маски подсети. Однако данный вид адресации столкнулся с проблемой исчерпания адресов. В ноябре 2019 года были распределены последние IPv4 адреса в Европе, странах бывшего СССР и на Ближнем Востоке. Решить эту проблему призвана новая версия протокола – IPv6. Протокол IPv6 отличается от своего предшественника использованием увеличенной в 4 раза длиной адреса. В связи с исчерпанием IPv4 адресов продвижение новой версии протокола началось активнее.

Сеть разделена на 2 виртуальные подсети:

1. VLAN №99 – административная подсеть.
2. VLAN №10 – серверная подсеть.

IPv6 адреса нужны лишь для некоторых приложений администраторов на их рабочих станциях, поэтому можно назначить эти адреса только на персональных компьютеров администраторов.

В таблице 3.5 отображено соответствие конечного устройства доступному IP-адресу и маскам подсети.

Таблица 3.5 – Соответствие конечного устройства IP-адресу и маске подсети

Устройство	VLAN	IP-адрес	Маска подсети
1	2	3	4
Рабочая станция #1	VLAN №99	172.17.1.2 2001:1010:2020:3030::2	255.255.255.0 /64

Продолжение таблицы 3.5

1	2	3	4
Рабочая станция #2	VLAN №99	172.17.1.3 2001:1010:2020:3030::3	255.255.255.0 /64
Рабочая станция #3		172.17.1.4 2001:1010:2020:3030::4	255.255.255.0 /64
Принтер		172.17.1.5	255.255.255.0
Беспроводная точка доступа		172.17.1.6	255.255.255.0
Wi-Fi DHCP Pool		172.17.3.5 172.17.3.6 … 172.17.3.15	255.255.255.0
Основной терминальный сервер	VLAN №10	172.17.2.12	255.255.255.0
Запасной терминальный сервер		172.17.2.13	255.255.255.0
AAA-сервер		172.17.2.14	255.255.255.0

4 ПРИНЦИПИАЛЬНОЕ ПРОЕКТИРОВАНИЕ

В проектируемой ЛКС кабельная подсистема реализована с помощью прокладки в кабельном коробе витой пары категории 5е вдоль стены по плинтусу. На коридор и в серверную комнату кабель распространяется через поперечные отверстия в стене. В коридоре кабельный короб прокладывается под фальшполом. В кабельном коробе кабель идёт до соответствующей ему информационной розетки, через которую происходит подключение конечных устройств к сети. Сетевые розетки расположены на стене близко к полу и в непосредственной близости к соответствующим устройствам.

Рабочие места администраторов расположены в углу отдела администрирования и оснащены столами (2 прямых и один угловой), креслами, персональными компьютерами. В помещении также находятся зона отдыха с холодильником и диваном.

Между стеной коридора и столом одного из администраторов расположен шкафчик, внутри которого находятся маршрутизатор и коммутатор. Во избежание использования вертикальных кабельных подсистем беспроводную точку доступа было решено расположить на центральном рабочем месте. Принтер расположен рядом с одним из рабочих мест и подключен в локальную сеть.

В серверной комнате находятся две серверные стойки на расстоянии одного метра друг от друга с расположенными на них основным и запасным серверами для обслуживания тонких клиентов. Рядом с запасным сервером находится RADIUS-сервер.

Для обеспечения пожарной безопасности в отделе администрирования и в серверной комнате расположены углекислотные огнетушители. Углекислотные огнетушители в процессе тушения не наносят ущерб электро- и оргтехнике.

Со схемой помещения можно ознакомиться в приложении В.

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсового проекта была разработана локальная компьютерная сеть для центра обработки данных компании, занимающейся программирование. По итогу работы была спроектирована завершённая структурированная кабельная система, выбрано необходимое оборудование, произведены все настройки, необходимые для работы конечных устройств локальной сети. Созданная локальная сеть получилась достаточно простой для её реализации и надёжной.

Полученная сеть полностью удовлетворяет пожеланиям, предъявленным заказчиком:

1. Основное помещение оснащено тремя рабочими местами для администраторов и принтером.
2. Серверная комната оснащена основным и резервным серверами для одновременного обслуживания до 100 тонких клиентов.
3. Реализована возможность подключения к беспроводной сети и ограничение доступа для лиц, не являющимися сотрудниками центра обработки данных.
4. Обеспечено удалённое администрирование маршрутизатором.
5. Обеспечена повышенная пожарная безопасность сети.

Активное и пассивное сетевое оборудование, а также пользовательские станции, принтер, серверы и другое техническое обеспечение, выбранное для реализации, соответствует стандартам качества, надёжности и зарекомендовало себя как одно из лучших решений для малых и средних локальных компьютерных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Сергеев, А. Основы локальных компьютерных сетей / А. Сергеев – М.: Лань, 2016. – 185 с.
2. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзэролл – СПБ.: Питер, 2012 – 962 с.
3. Одом, У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация / У. Одом, пер. с английского ООО «И. Д. Вильямс», М.: 2015. – 736 с., с илюс.
4. Одом, У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND1 100-101. Академическое издание / У. Одом, пер. с английского ООО «И. Д. Вильямс», М.: 2016. – 903 с., с илюс.
5. Архитектура Router-on-a-Stick в сети передачи данных [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/138573/
6. Wi-Fi с логином и паролем для каждого пользователя или делаем WPA2-EAP/TLS подручными средствами [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/170949/
7. WPA2-Enterprise, или правильный подход к безопасности Wi-Fi сети [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/150179/
8. Тонкий клиент – что это и с чем его едят [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/76159/
9. Тонкие клиенты как они есть [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/90670/
10. Настройка SSH в Cisco [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/68262/
11. Настройка беспроводных сетей на контроллере Cisco [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/148903/
12. Проект. Терминальный сервер на 100 человек [Электронный ресурс]. – Электронные данные. – Режим доступа: http://itsave.ru/тонкие-клиенты-для-малого-бизнеса/
13. Создание терминальных сетей на базе тонких клиентов [Электронный ресурс]. – Электронные данные. – Режим доступа: https://alex-service.ru/product/clients/
14. Категория пожарной опасности (кабельная маркировка) [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.profsector.com/parameter/1228/kategoriya-pozharnoy-opasnosti-kabelnaya-markirovka
15. Правила противопожарной безопасности при проектировании СКС [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.xnets.ru/plugins/content/content.php?content.96.8

16. ГОСТ 31565-2012 Кабельные изделия. Требования пожарной безопасности [Электронный ресурс]. – Электронные данные. – Режим доступа: http://docs.cntd.ru/document/1200101754
17. Технические характеристики витой пары [Электронный ресурс]. – Электронные данные. – Режим доступа: https://hobbyits.com/texnicheskie-xarakteristiki-vitoj-pary/
18. Обжим кабеля RJ45 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://day24h.ru/raznoe/obzhim-kabelya-rj45-kompyuter-router-raspinovka-setevogo-kabelya-router-kompyuter.html#_RJ45_RJ45
19. System x3650 M4 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://lenovopress.com/tips0850-system-x3650-m4-e5-2600-v2
20. Стойка двухрамная TWT-RACK2-33U-6x10 M4 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.ttn.by/computers_and_networks/server_equipment/server_cabinets_and_racks/stoyka_dvuhramnaya_twt_twt_rack2_33u_6x10_code430891
21. Розетка компьютерная RJ45 кат. 5e [Электронный ресурс]. – Электронные данные. – Режим доступа: http://wolframbel.by/r-koma-001k/
22. Кабель «витая пара» (LAN) для структурированных систем связи [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.tinko.ru/catalog/product/267136/
23. Огнестойкие кабельные системы [Электронный ресурс]. – Электронные данные. – Режим доступа: http://lebelectro.by/ognestojkie-kabelnye-linii/ognestojkie-kabelnye-kanaly
24. Принтер Ricoh SP C260DNw [Электронный ресурс]. – Электронные данные. – Режим доступа: https://catalog.onliner.by/printers/ricoh/spc260dnw
25. Коммутатор Cisco SB SRW2008P-K9-EU [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.tehnorus01.ru/index.php?route=product/product&product_id=127
26. AIR-CAP1602I-R-K9 Cisco WIFI [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.vtkt.ru/catalog/wlanarea/wifiapoints/cisco_aironet_air_cap1602i_wifi_tochka_dostupa_s_3_vstroennymi_antennami/
27. Jet Office 3i7 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://catalog.onliner.by/desktoppc/jets/jet13i7100d8h0mn
28. Irwin Computers Coffee Lake G1-07 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://catalog.onliner.by/desktoppc/irwin/coffeelakeg107
29. Cisco 2911 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://shop.nag.ru/catalog/02092.Cisco/07121.1900-2900-3900/11471.CISCO2911K9

30. Инструкция по подключению многофункциональных устройств серии [Электронный ресурс]. – Электронные данные. – Режим доступа: Ricoh SP 220 https://www.ixbt.com/infopages/ricoh-sp-220-325.shtml#ethernet

ПРИЛОЖЕНИЕ А
(обязательное)

Схема структурная

ПРИЛОЖЕНИЕ Б
(обязательное)

Схема СКС функциональная

ПРИЛОЖЕНИЕ В
(обязательное)

Пристройка. План этажа

ПРИЛОЖЕНИЕ Г
(обязательное)

Перечень оборудования, изделий и материалов