Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей
Кафедра электронных вычислительных машин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к курсовому проекту
на тему
ЛОКАЛЬНАЯ КОМПЬЮТЕРНАЯ СЕТЬ

БГУИР КП 1-35 05 01 006 ПЗ

Студент А. А. Пашковский
Руководитель И. И. Глецевич

МИНСК 2016

Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет: ФКСиС. Кафедра: ЭВМ.
Специальность: 40 02 01 «Вычислительные машины, системы и сети»
Специализация: нет

ЗАДАНИЕ
по курсовому проекту студента
Пашковского Антона Анатольевича

1 Тема проекта: «Локальная компьютерная сеть»

2 Срок сдачи студентом законченного проекта: 15 декабря 2016 г.

3 Исходные данные к проекту:

3.1 Используемое оборудование: нет ограничений

3.2 Количество пользовательских станций: больше 1

4 Содержание пояснительной записки (перечень подлежащих разработке вопросов):

Введение. 1. Обзор литературы. 2. Структурное проектирование ЛКС.

3. Функциональное проектирование ЛКС. 4. Проектирование структурной кабельной схемы. Заключение. Литература. Приложения.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На сегодняшний день использование компьютера даёт человеку почти безграничные возможности по обработке информации, возможности, которые казались недостижимыми полвека назад. И параллельно с возрастающими аппаратными возможностями компьютера, развивались и способы их использования, создавалась инфраструктура, которая позволяла людям обрабатывать и распространять информацию в рамках группы компьютеров, разделять дорогостоящие ресурсы (такие как принтеры, дисковая память и т.д.), работать над какими-то проектами совместно, делиться идеями и т.д. И одним из первых примеров таких инфраструктур стали локальные компьютерные сети.

Сейчас локальные компьютерные сети есть повсеместно: корпоративная сеть в офисе любой компании, сети в университетах, сети общежитий и т.д. В операционных системах компьютера по умолчанию встроены все необходимые аппаратные и программные инструменты для того что бы можно было настроить подключение к какой-нибудь локальной сети. Для того что бы настроить себе домашнюю компьютерную сеть нужно лишь понимание того, какую задачу эта сеть будет решать, знания и немного свободного времени.

В рамках данного курсового проекта была поставлена задача создать локальную компьютерную сеть, которая бы работала в рамках квартиры и решала бы какие-либо заранее определённые задачи.

1 ОБЗОР ЛИТЕРАТУРЫ

В этом разделе подробно разобрано что такое локальные компьютерные сети и как их можно классифицировать, беспроводные локальные компьютерные сети и способы их защиты. Также будут рассмотрены основные сервисы, которые настраиваются в локальных компьютерных сетях.

1.1 Классификация локальных компьютерных сетей

Локальная компьютерная сеть (LAN) – компьютерная сеть покрывающая относительно небольшую территорию или группу зданий. Также существуют локальные компьютерные сети, узлы которых разнесены на большое расстояние (космические станции и орбитальные центры). Несмотря на такие расстояния, такие сети всё равно относят к локальным. [1]

Локальные компьютерные сети можно классифицировать по разным параметрам в зависимости от способа их создания и применения. В основном локальные сети можно классифицировать по следующим параметрам:

1) По классу локальные сети делятся на одноранговые (Peer-to-peer) и клиент-серверные (иерархические) сети;
2) По топологии сети делятся на кольцевые, шинные, звездообразные, гибридные;
3) По типу физической среды передачи – на витую пару, коаксиальный или оптоволоконный кабель, инфракрасный канал, радиоканал.
4) По скорости доступа – на низкоскоростные (до 10 Мбит/с), среднескоростные (до 100 Мбит/с), высокоскоростные (свыше 100 Мбит/с);

Одноранговая сеть – это сеть равноправных компьютеров, каждый из которых имеет уникальное имя (имя компьютера) и обычно пароль для входа в него во время загрузки ОС. Имя и пароль входа назначаются владельцем компьютера средствами ОС. Каждый компьютер такой сети может одновременно являться и сервером, и клиентом сети, хотя вполне допустимо назначение одного компьютера только сервером, а другого только клиентом.

Достоинством одноранговых сетей является их высокая гибкость: в зависимости от конкретной задачи сеть может использоваться очень активно, либо совсем не использоваться. Из-за большой самостоятельности компьютеров в таких сетях редко бывает ситуация перегрузки (к тому же количество компьютеров обычно невелико). Установка одноранговых сетей довольно проста, к тому же не требуются дополнительные дорогостоящие серверы. Кроме того, нет необходимости в системном администрировании, пользователи могут сами управлять своими ресурсами.

К недостаткам одноранговых сетей относятся также слабая система контроля и протоколирования работы сети, трудности с резервным копированием распределенной информации. К тому же выход из строя любого

компьютера-сервера приводит к потере части общей информации, то есть все такие компьютеры должны быть по возможности высоконадежными. Эффективная скорость передачи информации по одноранговой сети часто оказывается недостаточной, поскольку трудно обеспечить быстродействие процессоров, большой объем оперативной памяти и высокие скорости обмена с жестким диском для всех компьютеров сети. К тому же компьютеры сети работают не только на сеть, но и решают другие задачи.

Сейчас считается, что одноранговая сеть наиболее эффективна в небольших сетях (около 10 компьютеров). При значительном количестве компьютеров сетевые операции сильно замедлят работу компьютеров и создадут множество других проблем. Тем не менее, для небольшого офиса одноранговая сеть – оптимальное решение.

Клиент-серверные локальные сети применяются в тех случаях, когда в сеть должно быть объединено много пользователей и возможностей одноранговой сети уже недостаточно. Тогда в сеть включается специализированный компьютер – сервер.

Сервером называется абонент сети, который предоставляет свои ресурсы другим абонентам, но сам не использует ресурсы других абонентов, то есть служит только сети. Выделенный сервер - это сервер, занимающийся только сетевыми задачами. Невыделенный сервер может заниматься помимо обслуживания сети и другими задачами. Существует ещё и специфический тип сервера – сетевой принтер.

Серверы специально оптимизированы для быстрой обработки сетевых запросов на разделяемые ресурсы и для управления защитой файлов и каталогов. При больших размерах сети мощности одного сервера может оказаться недостаточно, и тогда в сеть включают несколько серверов. Серверы могут выполнять и некоторые другие задачи: сетевая печать, выход в глобальную сеть, связь с другой локальной сетью, обслуживание электронной почты и т.д.

Количество пользователей сети на основе сервера может достигать нескольких тысяч. Одноранговой сетью такого размера просто невозможно было бы управлять. Кроме того, в сети на основе серверов можно легко менять количество подключаемых компьютеров, такие сети называются масштабируемыми.

Достоинством сети на основе сервера можно назвать надёжность. Но это верное только если сам сервер надёжен. В противном случае любой отказ сервера приводит к полному выходу из строя сети в отличие от ситуации с одноранговой сетью, где отказ одного из компьютеров не приводит к отказу всей сети. Так же к достоинствам сетей на основе сервера можно отнести централизованную настройку сети.

К недостаткам сети на основе сервера относятся ее громоздкость в случае небольшого количества компьютеров, зависимость всех компьютеров-

клиентов от сервера и высокая стоимость сети вследствие использования дорогого сервера. [2]

Под топологией компьютерной сети обычно понимается расположение компьютеров сети друг относительно друга и способ соединения их линиями связи.

От выбранной топологии зависят требования к оборудованию, тип используемого кабеля, возможные и наиболее удобные методы управления обменом, надежность работы, возможности расширения сети.

Существует три основных топологии сети:

1) шина (bus), при которой все компьютеры параллельно подключаются к одной линии связи и информация от каждого компьютера одновременно передается всем остальным компьютерам. Шина более надёжна, так как отказ одного компьютера не влияет на способность остальных обмениваться информацией, однако эта топология упирается в физические ограничения, связанные с ослаблением сигнала;
2) звезда (star), при которой к одному центральному компьютеру присоединяются остальные периферийные компьютеры, причем каждый из них использует свою отдельную линию связи. Отказ конечных устройств никак не влияет на топологию звезда, однако выход из строя центрального узла полностью разрушает сеть;
3) кольцо (ring), при которой каждый компьютер передает информацию всегда только одному компьютеру, следующему в цепочке, а получает информацию только от предыдущего в цепочке компьютера, и эта цепочка замкнута в «кольцо». Кольцо может содержать большое количество компьютеров и очень устойчиво к большим потокам информации, так как в ней нет конфликтов (как у шины) и нет центрального узла (как у звезды), однако, поскольку информация передаётся через все компьютеры – выход хотя бы одного из них из строя выведет из строя всю сеть;

На практике часто используют комбинации разных топологий, в зависимости от того какая задача решается. [3]

Средой передачи информации называются те линии связи (или каналы связи), по которым производится обмен информацией между компьютерами. В подавляющем большинстве компьютерных сетей (особенно локальных) используются проводные или кабельные каналы связи, хотя существуют и беспроводные сети.

Выбор средства передачи данных зависит от размера сети, требуемой пропускной способности и скорости передачи данных, требуемых служб, работу которых необходимо организовать (передача мультимедиа, речи, простых данных и т.д.) и общей суммы, которую вы готовы потратить на вашу сеть.

Кабели на основе витых пар – самые дешёвые и самые популярные. Неэкранированный кабель слабо защищён от внешних электромагнитных помех и слабой защищённостью от прослушки. Для устранения этих недостатков применяется экранирование. Основные достоинства неэкранированных витых пар - простота монтажа разъемов на концах кабеля, а также простота ремонта любых повреждений по сравнению с другими типами кабеля. Все остальные характеристики у них хуже, чем у других кабелей.

Коаксиальный кабель представляет собой электрический кабель, состоящий из центрального провода и металлической оплетки, разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку. Коаксиальный кабель ранее был достаточно распространен, что связано с его высокой помехозащищенностью (благодаря металлической оплетке), а также более высокими, чем в случае витой пары, допустимыми скоростями передачи данных (до 500 Мбит/с) и большими допустимыми расстояниями передачи (до километра и выше). К нему труднее механически подключиться для несанкционированного прослушивания сети, он также дает заметно меньше электромагнитных. излучений вовне. Однако монтаж и ремонт коаксиального кабеля существенно сложнее, чем витой пары, а стоимость его выше. Сложнее и установка разъемов на концах кабеля. Поэтому его сейчас применяют реже, чем витую пару. [4]

Оптоволоконный (он же волоконно-оптический) кабель — это принципиально иной тип кабеля по сравнению с рассмотренными двумя типами электрического или медного кабеля. Информация по нему передается не электрическим сигналом, а световым. Главный его элемент - это прозрачное стекловолокно, по которому свет проходит на огромные расстояния (до десятков километров) с незначительным ослаблением. Оптоволоконный кабель обладает исключительными характеристиками по помехозащищенности и секретности передаваемой информации. Никакие внешние электромагнитные помехи в принципе не способны исказить световой сигнал, а сам этот сигнал принципиально не порождает внешних электромагнитных излучений. Однако оптоволоконный кабель имеет и некоторые недостатки. Главный из них - высокая сложность монтажа (при установке разъемов необходима микронная точность, от точности скола стекловолокна и степени его полировки сильно зависит затухание в разъеме). Для установки разъемов применяют сварку или склеивание с помощью специального геля, имеющего такой же коэффициент преломления света, что и стекловолокно. В любом случае для этого нужна высокая квалификация персонала и специальные инструменты. Поэтому чаще всего оптоволоконный кабель продается в виде заранее нарезанных кусков разной длины, на обоих концах которых уже установлены разъемы нужного типа. [5]

Наиболее подходящей локальной сетью для квартиры, учитывая небольшое число клиентов и неудобство протяжки кабелей по всей квартире,

была выбрана одноранговая сеть с беспроводным подключением внутри и оптоволоконным подключением снаружи. Поэтому устройство, безопасность и настройку беспроводных локальных сетей будет рассмотрено подробнее.

1.2 Беспроводные локальные компьютерные сети (WLAN)

Стандарт на локальные беспроводные сети (сокращенно WLAN) разработан Институтом инженеров по электротехнике и электронике (IEEE, Institute of Electrical and Electronics Engineers) и официально именуется как 802.11. Однако для конечных пользователей было придумано более простое название – Wi-Fi, которое, кстати, расшифровывается как «wireless fidelity», то есть «беспроводная безукоризненность».

Стандарт IEEE 802.11 подразделяется на IEEE 802.11a, b, c, d, e, f, g, h, i, j, k, n. Из всей этой кучи широкого практического применения достигли IEEE 802.11b и IEEE 802.11g, (и совсем-совсем недавно Apple объявила о начале промышленного внедрения 802.11n) – именно такие сети и подразумеваются в первую очередь при упоминании слова Wi-Fi. Сети 802.11b и 802.11g работают в диапазоне 2.4ГГц и различаются скоростью передачи данных и радиусом действия. Для сетей 802.11b максимальная скорость составляет 11Мбит/сек, а радиус действия до 250 метров на открытом пространстве и до 20-30 метров в помещении. Сети 802.11g обеспечивают значительно большую скорость – до 54Мбит/сек, радиус действия у них до 300 метров на открытом пространстве. Все современные точки доступа (точка доступа – это устройство, посредством которого поддерживается связь между клиентами беспроводной сети, работают как с 802.11b, так и с 802.11g. Самые современные имеют поддержку стандарта 802.11n.

Радиус действия домашней Wi-Fi сети зависит от типа используемой беспроводной точки доступа или беспроводного маршрутизатора. К факторам, определяющим диапазон действия беспроводных точек доступа или беспроводных маршрутизаторов, относятся:

1) Тип используемого протокола 802.11;
2) Общая мощность передатчика;
3) Коэффициент усиления используемых антенн;
4) Длина и затухание в кабелях, которыми подключены антенны;
5) Природа препятствий и помех на пути сигнала в данной местности.
6) Препятствия в виде кирпичных стен и металлических конструкций могут уменьшить радиус действия Wi-Fi сети на 25% и более. Поскольку стандарт 802.11a использует частоты выше, чем стандарты 802.11b/g, он является наиболее чувствительным к различного рода препятствиям. На радиус действия Wi-Fi сетей, поддерживающих стандарт 802.11b или 802.11g, влияют также помехи, исходящие от микроволновых печей.

Стандарт 802.11n повышает скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с), при условии использования в режиме

802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с брутто, применяя передачу данных сразу по четырём антеннам. По одной антенне — до 150 Мбит/с.

Устройства 802.11n работают в диапазонах 2,4—2,5 или 5,0 ГГц.

Кроме того, устройства 802.11n могут работать в трёх режимах:

1) наследуемом, в котором обеспечивается поддержка устройств 802.11b/g и 802.11a;
2) смешанном, в котором поддерживаются устройства 802.11b/g, 802.11a и 802.11n;
3) «чистом» режиме — 802.11n (именно в этом режиме и можно воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом 802.11n). [6]

1.3 Безопасность и защита данных в WLAN

Удобность создания беспроводной локальной компьютерной сети состоит в том, что не нужно протягивать кабель к каждой пользовательской машине. Однако это же и порождает проблему безопасности беспроводных сетей – для того что бы подключится к вашей сети не нужно подключать кабель, достаточно просто сесть где-нибудь неподалёку с ноутбуком. Поэтому, если нет желания поделиться своей сетью со всеми соседями – необходимо настраивать ограниченный доступ к вашей сети.

Технологии защиты беспроводных локальных компьютерных сетей прошли за время своего существования своеобразную эволюцию. Далее по пунктам будет разобрано какие технологии защиты и в каком порядке появлялись и что использовалось для обеспечения этой самой защиты:

1) WEP (Wired Equivalent Privacy, или Защита Эквивалентная Проводной). Этот способ защиты применялся на ранних этапах развития беспроводных сетей. Данные шифруются с помощью специальных ключей, – ключ представляет собой пароль длиной 5 или 13 символов ASCII плюс вектор инициализации, сформированный случайным образом (из трех ASCII символов). Этот самый вектор инициализации несложно подобрать прямым перебором – пару часов работы относительно мощного компьютера, и ключ подобран. Сегодня считается, что использование технологии WEP равносильно ее отсутствию. Использовать не рекомендуется.
2) 802.1X - стандарт сетевой аутентификации IEEE, нашел широкую поддержку у производителей сетевого оборудования и ПО. Основные составляющие — протоколы EAP и RADIUS. Протокол 802.1X работает на канальном уровне и определяет механизм контроля доступа к сети на основе принадлежности к порту (в контексте стандарта порт — точка подключения к сети). Согласно этому протоколу доступ к сети получают

только клиенты, прошедшие аутентификацию, если аутентификация не была пройдена, доступ с соответствующего порта будет запрещен. Используются динамические ключи шифрования, то есть те, которые периодически меняются во времени. Пользователи работают сеансами, по окончании сеансов им присылается новый ключ.

3) WPA (Wi-Fi Protected Access) – введен в работу с конца 2003 года. Является по сути суммой нескольких технологий. Из 802.1X позаимствована идея динамической смены ключа, плюс многочисленные улучшения включая проверку целостности сообщений. Очень хорошая технология, рекомендуется для домашних сетей и малого офиса.
4) WPA2 (он же 802.11i). Появился в 2004 году, максимально защищенный стандарт, изначально разработанный для беспроводных сетей (в отличие от VPN). Сочетает средства WPA1 и AES (Advanced Encryption Standard). Технологию можно разделить на WPA2 Personal и WPA2 Enterprise, которые отличаются охватом пользователей и наличием сервера аутентификации.
5) VPN (Virtual Private Network) – эта технология предложена компанией Intel и предназначена для безопасного соединения клиентских ПК с серверами по общедоступным интернет каналам. VPN очень хороша в плане шифрования и надежности аутентификации. Хотя эта технология и не разрабатывалась для применения в беспроводных сетях, она может с успехом применяться и здесь. Состоит из внутренней (может быть несколько) и внешней сети. По внешней сети проходит инкапсулированное соединение. С инкапсулированными пакетами можно делать всё что угодно (шифровать, сжимать и т.д.), главное, чтобы обратное действие проводилось на другой стороне подключения. Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP и UDP). [7]

1.4 Сервисы, используемые в локальных компьютерных сетях

HTTP - это протокол передачи гипертекста между распределёнными системами. Общение между хостом и клиентом происходит в два этапа: запрос и ответ. Клиент формирует HTTP запрос, в ответ на который сервер даёт ответ. Доступный ресурс на сервере идентифицируется с помощью специального адреса - URL (Universal Resource Locator). Зная нужный URL можно получить с сервера файл с гипертекстом, который храниться по этому адресу. Таким образом, с помощью HTTP на можно организовать хранение на сервере связанных данных в виде веб-сайта.

TFTP (простой протокол передачи файлов) - используется главным образом для первоначальной загрузки бездисковых рабочих станций.

FTP (протокол передачи файлов) — протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к FTP серверам, просматривать содержимое каталогов и загружать файлы с сервера или на сервер.

DNS (система доменных имён) — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста. Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу. Основой протокола является иерархическая структура, которая позволяет знать одному DNS – серверу только о какой-то части доменного имени, а остальную часть делегировать DNS серверу верхнего уровня.

AAA (англ. Authentication, Authorization, Accounting) — используется для описания процесса предоставления доступа и контроля над ним.

SYSLOG (англ. system log — системный журнал) — стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания логов), использующийся в компьютерных сетях, работающих по протоколу IP.

NTP (протокол сетевого времени) – используется в сетях для синхронизации времени. Даёт точность до 10мс при синхронизации через сеть интернет и 0.2мс и выше, если сервер точного времени находится в локальной компьютерной сети. В OS Windows представлен службой (W32Time), в Linux (Ntpd). [8]

Заключение

В этом разделе были описаны виды локальных сетей, способы их защиты и основные сервисы которые настраиваются в локальных сетях. Было решено сделать беспроводную локальную компьютерную сеть с WPA2 аутентификацией с FTP сервером для совместного хранения файлов.

2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В рамках структурного проектирования будет сделан выбор топологии сети и описан способ подключения локальной сети к сети Internet. Саму локальную сеть описывать нет необходимости, потому что всё её внутреннее устройство будет раскрыто на этапе функционального проектирования. На структурной схеме локальная сеть будет обозначаться одним блоком.

2.1 Выбор способа подключения к сети Internet

Одной из самых главных возможностей для узлов локальной сети квартиры является возможность выхода в Internet. Способов подключения к сети интернет несколько, и выбор зависит от необходимой скорости и финансовых возможностей.

Способы подключения к сети интернет:

1. Коммутируемый доступ к интернету с использованием модема. Подключиться к сети интернет по телефонной линии можно по старой технологии Dial-Up или более продвинутой технологии ADSL. Скорость у Dial-Up будет до 56 Кбит/с, у ADSL до 24 Мбит/с.
2. Фиксированный широкополосный доступ к сети интернет по выделенной линии. В квартиру проводится Ethernet или GPON кабель, к которому подключается, к примеру, беспроводной маршрутизатор. А все остальные устройства в квартире подключаются к маршрутизатору по Wi-Fi. Скорость в таком случае будет до 100 Мбит/с или до 1 Гбит/с (теоретически, GPON).
3. Передача данных по коаксиальному (телевизионному) кабелю. Передача данных по данному стандарту у провайдера осуществляется к клиенту (downstream) на скорости 42/38 Мбит/с, а от пользователя (upstream) 10/9 Мбит/с. Вести коаксиальный кабель ради интернета смысла нет, но если он уже есть и оператор кабельного телевидения предоставляет такую услугу – то может быть вполне разумно этой услугой воспользоваться.
4. Спутниковый интернет. Используется обычно там, где никакого другого интернета нет и не предвидится. Провести можно куда угодно, но его сложно настраивать, дорогое и сложное в установке оборудование, большое время отклика.

Исходя из имеющихся вариантов наиболее подходящим для квартиры является подключение по выделенной оптоволоконной линии беспроводного маршрутизатора.

2.2 Выбор способа организации беспроводной сети

Одним из основных вопросов при организации WLAN-сетей является размер покрытия. При идеальных условиях распространения радиоволн зона покрытия одной точки доступа будет иметь следующие значения:

1. Сеть стандарта IEEE 802.11a - 50 м
2. Сети 802.11b, g, n - порядка 100 м.

В зависимости от того какую задачу нам нужно решить при построении беспроводной сети выделяют три вида организации беспроводных сетей:

1. Эпизодическая сеть (Ad-Hoc или IBSS – Independent Basic Service Set).
2. Основная зона обслуживания Basic Service Set (BSS) или Infrastructure Mode.
3. Расширенная зона обслуживания ESS – Extended Service Set.

Режим Ad-Hoc (Independent Basic Service Set (IBSS) или Peer-to-Peer) – простейшая структура локальной сети, когда абонентские станции (ноутбуки или компьютеры) взаимодействуют непосредственно друг с другом. Такая структура удобна для срочного развертывания сетей. Для ее создания необходим минимум оборудования – каждая абонентская станция должна иметь в своем составе адаптер WLAN.

В режиме BSS узлы сети взаимодействуют друг с другом не напрямую, а через точку доступа (Access Point, AP). В режиме BSS все узлы взаимодействуют между собой через одну AP, которая может играть роль моста для подключения к внешней кабельной сети.

Режим ESS позволяет объединить несколько точек доступа, т.е. объединяет несколько сетей BSS. В данном случае точки доступа могут взаимодействовать и друг с другом. Расширенный режим удобно применять тогда, когда необходимо объединить в одну сеть несколько пользователей или подключить несколько проводных или беспроводных сетей.

Поскольку в рамках квартиры не нужно покрывать беспроводной сетью большую территорию, но есть единая точка доступа, наша беспроводная локальная компьютерная сеть будет работать в режиме BSS.

Заключение

Локальная сеть будет состоять из 5 ЭВМ, находящихся на одном этаже и в одном сегменте. Все ЭВМ будут подключены по беспроводному маршрутизатору. На одной из ЭВМ будет настроен FTP сервер для хранения файлов общего пользования.

Структурная схема представлена в приложении «А».

3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

3.1 Адресация

В качестве адреса подсети для локальной компьютерной сети был выбран адрес 192.168.100.0/24. Статический адрес FTP сервера – 192.168.100.106/24.

3.2 Подключение и настройка беспроводного маршрутизатора

В качестве беспроводного маршрутизатора был выбран маршрутизатор Промсвязь MT-PON-AT-4 (см. рисунок 3.2.1). На маршрутизаторе есть интерфейс GPON стандарта ITU-T G.984 со скоростью передачи 2.488 Гбит/с по линии вниз и 1.244 Гбит/с по линии вверх. Устройство поддерживает полный спектр услуг Triple Play, включая голос, видео (IPTV/CATV) и высокоскоростной доступ к Интернет.
Трафик по линии вверх передаётся в сеть по оптоволоконному кабелю. Одно оптоволокно служит для переноса как восходящего, так и нисходящего трафика. Реальная же скорость, зависящая от тарифа – 29 Мбит/с на получение и 21 Мбит/с на передачу.

Настройка беспроводного маршрутизатора будет проходить в 4 этапа:

1. Сброс настроек на заводские.
2. Настройка подключения к Internet путём ввода имени пользователя и пароля из договора с Белтелеком.
3. Настройка Wi-Fi.
4. Настройка работы DNS сервера.

Сброс настроек на заводские должен выполнятся во избежание всяческих недоразумений. Настраивать на маршрутизаторе нужно далеко не всё, поэтому сброс настроек — это единственный способ убедиться, что всё что нам не нужно настроено по умолчанию.

После сброса настроек лучше сразу сменить логин и пароль для входа на роутер. Этого можно и не делать, но тогда существует угроза стать частью какого-нибудь ботнета. Окно для смены пароля можно увидеть, зайдя на вкладку Networks (см. рисунок 3.2.2).

После введения данных из договора и получения доступа к сети Internet, необходимо настроить раздачу сети Wi-Fi с маршрутизатора. Для этого нужно указать SSID (идентификатор сети) и настроить защиту подключения WPA2 Personal. Настроить WPA2 Personal можно зайдя на вкладку Network-> WLAN-> Security (см. рисунок 3.2.3).

Для настройки DNS серверов нужно зайти на вкладку Application-> DNS Service-> DNS и ввести первичный и вторичный DNS сервера Google. (8.8.8.8) и (8.8.4.4) соответственно.

Рисунок 3.2.1 Маршрутизатор Промсвязь MT-PON-AT-4

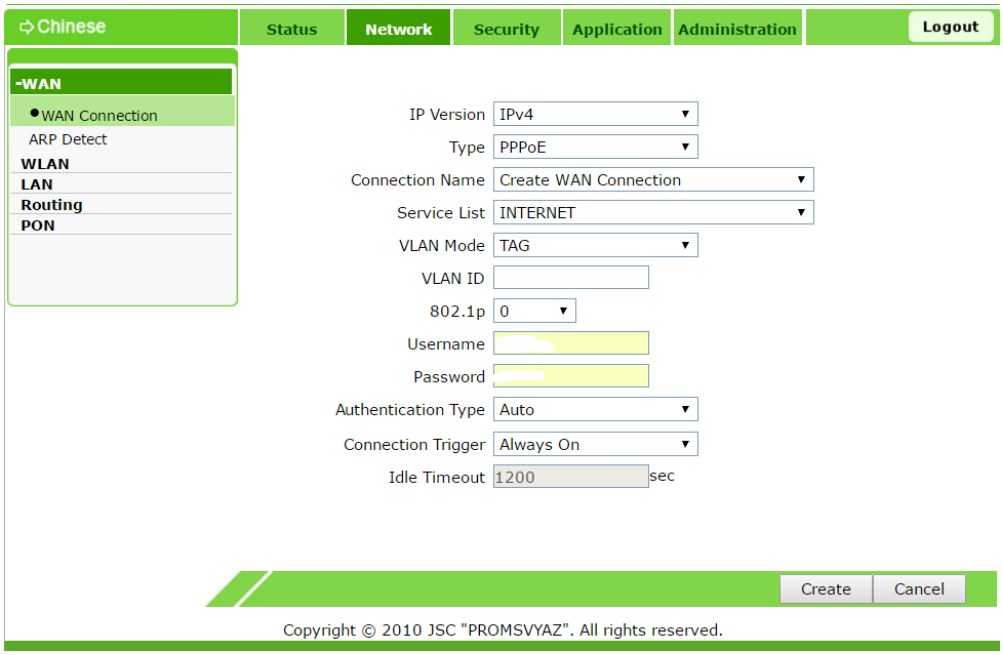

Рисунок 3.2.2 Окно смены пароля на маршрутизаторе MT-PON-AT-4.

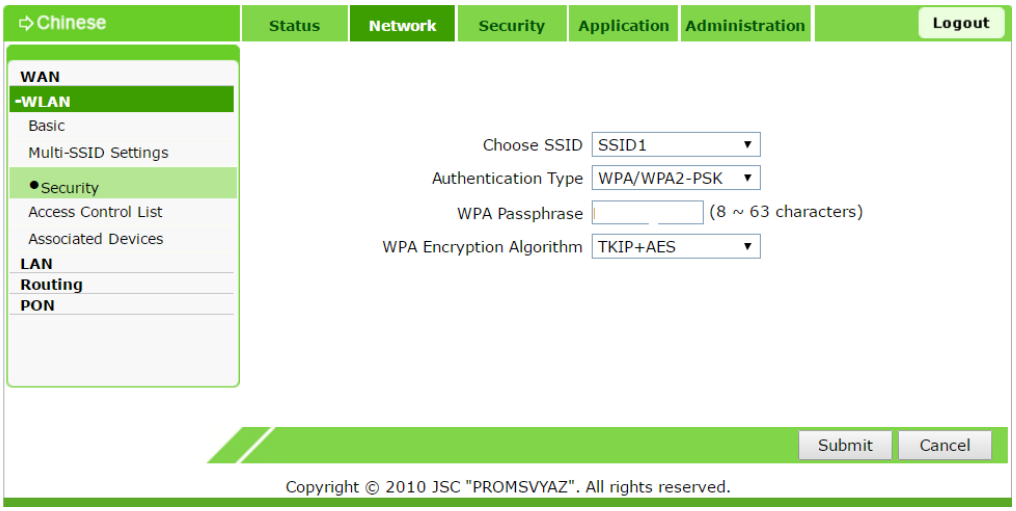

Рисунок 3.2.3 Настройка защиты подключения WPA2-Personal.

3.3 Настройка FTP сервера

После того как настроен беспроводной маршрутизатор и все компьютеры в сети получили свои адреса, одним из планов была настройка FTP сервера для локальной сети. FTP сервер необходим в локальной сети как сервис обеспечивающий совместное хранение файлов. Для этого используем одну пользовательскую станцию в качестве FTP сервера.

Перед тем как настраивать FTP-сервер необходимо убедиться, что на серверной машине открыт порт 21 и что серверная машина доступна из локальной сети. Для того что бы открыть порт нужно прописать правило для Firewall:

iptables -I INPUT -p tcp -m tcp --dport 21 -j ACCEPT

Далее были использованы следующие команды для настройки FTP сервера:

1) Устанавливается утилита для ftp сервера:

sudo apt-get install vsftpd

vsftpd — Very Secure FTP Daemon

2) Для настройки FTP сервера нужно отредактировать конфигурационный файл, который изначально находиться в /etc/vsftpd.conf. Редактировать файл можно в любом текстовом редакторе, однако этот редактор нужно запустить от имени суперпользователя. Пример:

sudo vim /etc/vsftpd.conf

Для того, чтобы настроить беспарольный доступ к FTP серверу редактируется следующий флаг:

anonymous_enable=YES

Разрешается вносить изменения в файловую систему (например, загрузка новый файлов на FTP сервер)

write_enable=YES

В конфигурационном файле есть множество параметров, изменяя которые можно настроить сервер под любые нужды.

3) Для того, чтобы демон смог применить изменения, нужно сделать рестарт сервиса FTP сервера:

sudo service vsftpd restart

Для того, чтобы увидеть статус работы демона, нужно набрать следующую команду (см. рисунок 3.3.1):

sudo service vsftpd status

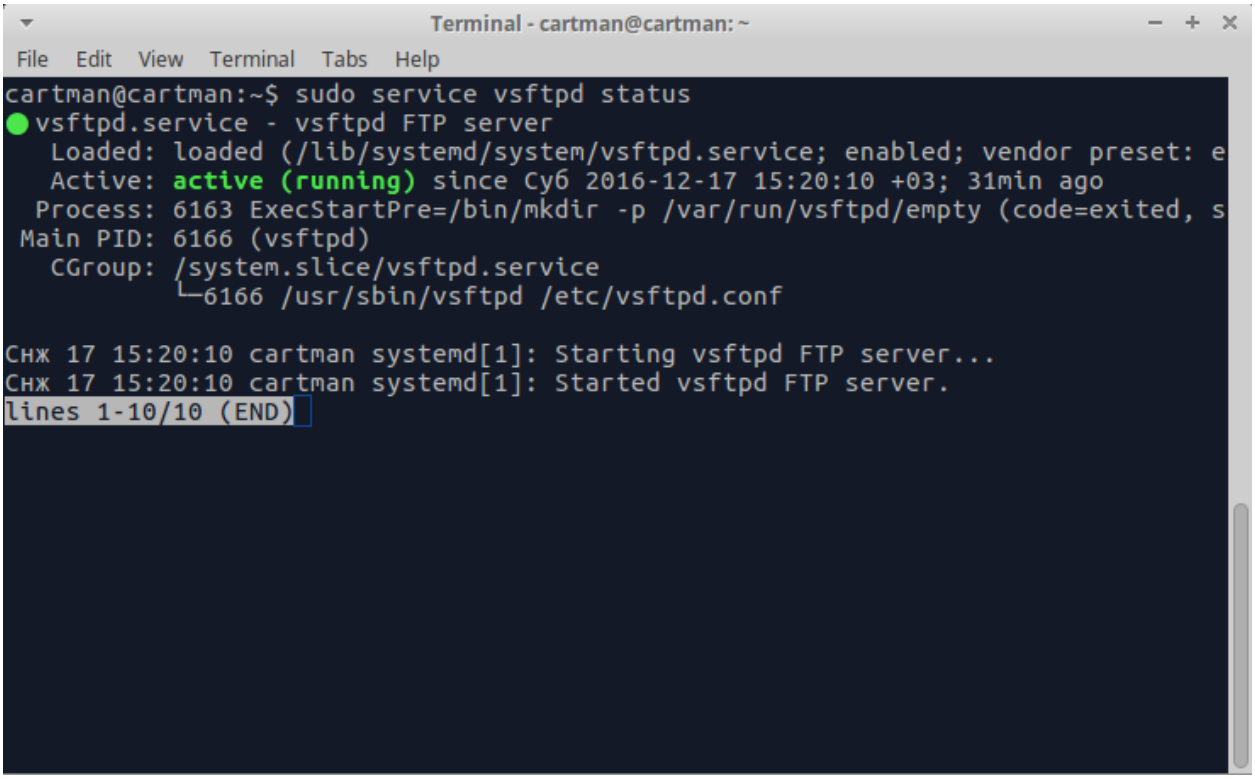

Рисунок 3.3.1 Статус FTP сервера.

В случае, если нужно остановить работу FTP сервера, нужно выполнить следующую команду (см. рисунок 3.3.2):

sudo service vsftpd stop

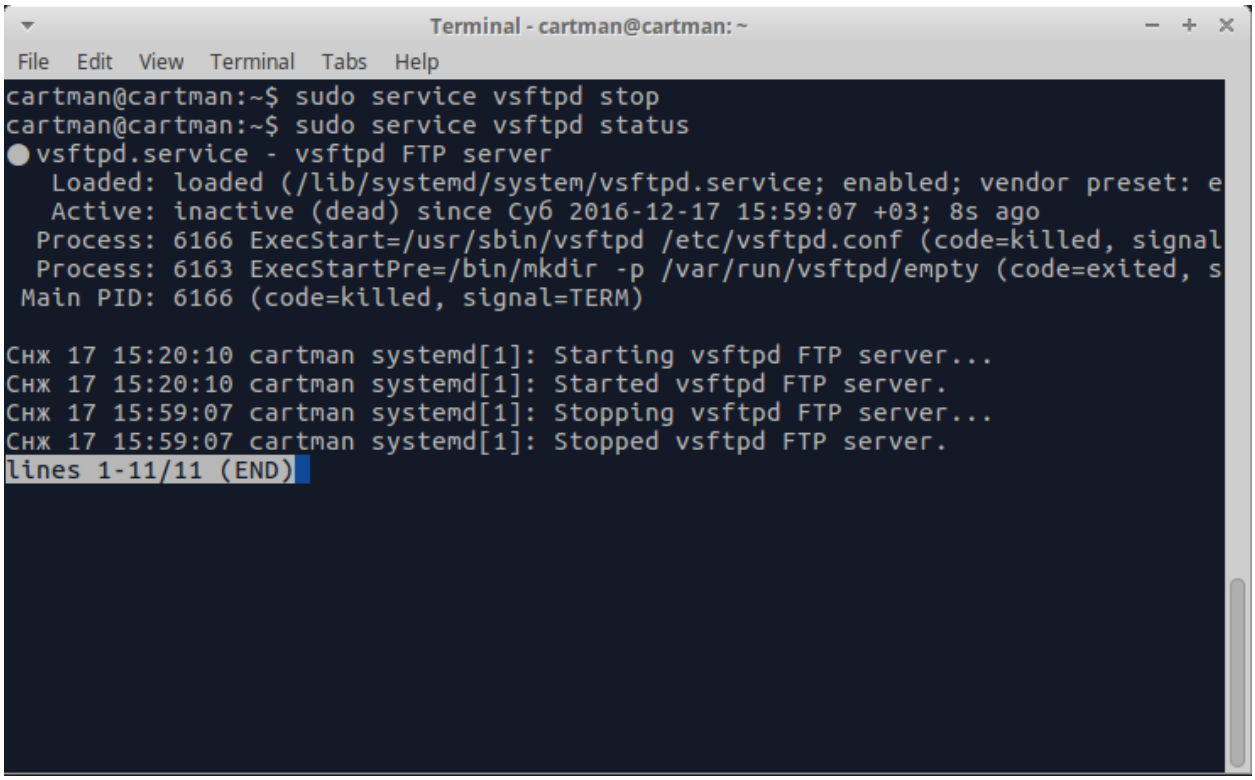

Рисунок 3.3.2 Остановка работы FTP сервера.

Теперь все файлы, которые загружают и скачивают анонимные пользователи можно увидеть в директории srv/ftp/. Клиенты FTP сервера могут увидеть файлы и папки, хранящиеся на FTP сервере через файловый менеджер или браузер, просто введя в строку адреса адрес серверной машины (см. рисунок 3.3.3).

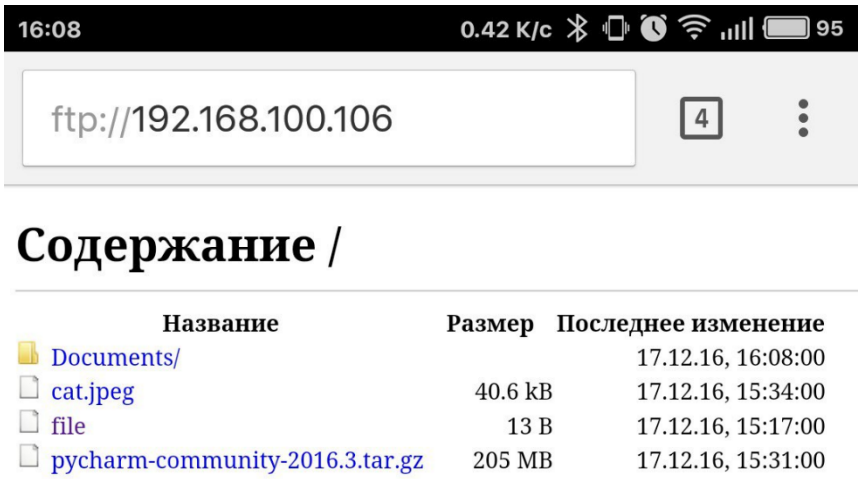

Рисунок 3.3.3 Директория FTP сервера с мобильного телефона

3.4 Перечень сетевого оборудования

В качестве точки доступа используется маршрутизатор MT-PON-AT-4.

Характеристики маршрутизатора:

1. Для устройства рабочий диапазон температур: от плюс 10 до 400 С. Влажность от 20 до 80% без конденсации.
2. Размеры: (208x47,7x162) мм.
3. Вес: не более 0,5 кг.
4. Электропитание: 230 В переменного тока на входе и 12 В постоянного тока на выходе.
5. Потребляемая мощность: 12 Вт.
6. Установка: настольная, настенная.

Рабочие станции представляют собой 5 ноутбуков. В программное обеспечение рабочих станций входит:

1. Операционная система - Windows 10 или Manjaro Linux.
2. Антивирусная программа - Windows Defender
3. Пакет программ - Microsoft Office.
4. Пользовательские программы

Функциональная схема представлена в приложении «Б».

4 ПРОЕКТИРОВАНИЕ СТРУКТУРНОЙ КАБЕЛЬНОЙ СХЕМЫ

Структурированная кабельная система (СКС) представляет собой иерархическую кабельную среду передачи электромагнитных сигналов в здании, разделённую на структурные подсистемы и состоящую из элементов - кабелей и разъемов. По сути СКС состоит из набора медных и оптических кабелей, кросс-панелей, соединительных шнуров, кабельных разъёмов, модульных гнёзд информационных розеток и вспомогательного оборудования. СКС обеспечивает подключение локальной АТС, одновременную работу компьютерной и телефонной сети и предоставляет возможность гибкого изменения конфигурации кабельной системы. Кабели, оснащенные разъемами и проложенные по определенным правилам, образуют линии и магистрали. Линии, магистрали, точки подключения и коммутации составляют функциональные элементы СКС.

Универсальность СКС подразумевает использование ее для различных систем:

1. Компьютерная сеть;
2. Телефонная сеть;
3. Охранная система;
4. Пожарная сигнализация.

Такая кабельная система независима от оконечного оборудования, что позволяет создать гибкую коммуникационную инфраструктуру.

Структурированная кабельная система - это совокупность пассивного коммуникационного оборудования:

Кабель - этот компонент используется как среда передачи данных СКС.

Розетки - этот компонент используют как точки входа в кабельную сеть здания.

Коммутационные панели - используются для администрирования кабельных систем в коммутационных центрах этажей и здания в целом.

Коммутационные шнуры - используются для подключения офисного оборудования в кабельную сеть здания, организации структуры кабельной системы в центрах коммутации.

СКС - охватывает все пространство здания, соединяет все точки средств передачи информации, такие как компьютеры, телефоны, датчики пожарной и охранной сигнализации, системы видеонаблюдения и контроля доступа. Все эти средства обеспечиваются индивидуальной точкой входа в общую систему здания. Линии, отдельные для каждой информационной розетки, связывают точки входа с коммутационным центром этажа, образуя горизонтальную кабельную подсистему. Все этажные коммутационные узлы специальными магистралями объединяются в коммутационном центре здания. Сюда же подводятся внешние кабельные магистрали для подключения здания к

глобальным информационным ресурсам, таким как телефония, интернет и т.п. Такая топология позволяет надежно управлять всей системой здания, обеспечивает гибкость и простоту системы.

В каждом конкретном здании в общем случае присутствуют три подсистемы СКС: вертикальная кабельная подсистема, горизонтальная кабельная подсистема и подсистема рабочих мест. Для достаточно крупных зданий, с большим количеством рабочих мест на этажах, все эти три подсистемы присутствуют в явном виде. Для относительно небольших зданий с ограниченным количеством рабочих мест рекомендуется организовывать один узел коммутации СКС, куда сходится вся горизонтальная кабельная разводка. В этом случае вертикальная кабельная подсистема может отсутствовать либо носить вырожденный характер, при котором вертикальная кабельная подсистема представляется совокупностью коммутационных шнуров, соединяющих порты "этажных" коммутаторов ЛВС (коммутаторов для подключений рабочих мест) с портами центрального (магистрального) коммутатора.

Расположение ЭВМ и протяжка кабелей представлена в приложении «В».

Для реальных сетей важен такой показатель производительности, как показатель использования сети (network utilization), который представляет собой долю в процентах от суммарной пропускной способности (не поделенной между отдельными абонентами). Он учитывает коллизии и другие факторы. Рабочие станции не содержат средств для определения показателя использования сети, для этого предназначены специальные, не всегда доступные из-за высокой стоимости аппаратно-программные средства типа анализаторов протоколов.

Считается, что для загруженных систем Ethernet и Fast Ethernet хорошим значением показателя использования сети является 30%. Это значение соответствует отсутствию длительных простоев в работе сети и обеспечивает достаточный запас в случае пикового повышения нагрузки. Однако если показатель использования сети значительное время составляет 80...90% и более, то это свидетельствует о практически полностью используемых (в данное время) ресурсах, но не оставляет резерва на будущее.

Для проведения расчетов и выводов следует рассчитать производительность в каждом сегменте сети.

Вычислим полезную нагрузку Рп:

$$P_n = (N \times R_1) \times G_1 + (N \times R_2) \times G_2 \text{, Мбит/с,} \quad (1)$$

где N – количество компьютеров в сегменте;

G_1, G_2 – производительность рабочей станции первого и второго видов соответственно;

R_1, R_2 – количество рабочих станций первого вида (PC, notebook) и второго вида (smartphone), поддерживающих производительность G_1 и G_2 соответственно.

$P_п$ = (5*5) * 0,6 + (0*0) * 0,4 = 15+ 0 = 15 Мбит/с

Далее необходимо определить общую нагрузку $P_о$:

$$P_o = P_n \times n \text{, Мбит/с,} \qquad (2)$$

где n – количество сегментов проектируемой сети.

P_0 = 15*1= 15 Мбит/сек

Полная фактическая нагрузка $P_ф$ рассчитывается с учетом коллизий и величины задержек доступа к среде передачи данных:

$$P_\phi = P_o \times (1 + \kappa) \text{, Мбит/с,} \qquad (3)$$

где к – задержка доступа к среде передачи данных: для семейства технологий Ethernet – 0,4, для Token Ring – 0,6, для FDDI – 0,7.

$P_ф$ = 15*(1+0.4) = 21 Мбит/с

Т. к. фактическая нагрузка $P_ф$ > 10 Мбит/с, то, как и предполагалось ранее, данную сеть невозможно реализовать с помощью стандарта Ethernet, необходимо применить технологию Fast Ethernet (100 Мбит/с) или GPON (1.5 Гбит/с).

Т.к. данной в сети мы не используем концентраторы, то рассчитывать время двойного оборота сигнала не требуется. Сигнал коллизий отсутствует.

ЗАКЛЮЧЕНИЕ

Для надёжной работы и повышения производительности сети следует вносить изменения в структуру сети только с учётом требований стандарта.

Для защиты данных от вирусов необходимо установить антивирусные программы (например, NOD32 Antivirus System, Kaspersky Internet Security, либо стандартная программа – Windows Defender).

Для восстановления повреждённых или ошибочно удалённых данных следует использовать специальные утилиты (например, утилиты, входящие в состав пакета Norton System Works).

Хотя сеть построена с запасом производительности, всё равно следует беречь сетевой трафик, и с помощью программы для администрирования следить за целевым использованием внутрисетевого и интернет-трафика.

Благотворно на производительности сети скажется использование служебных приложений Norton System Works (таких как дефрагментация, чистка реестра, исправление текущих ошибок с помощью WinDoctor), а также регулярной антивирусной проверки в нерабочее время.

СПИСОК ЛИТЕРАТУРЫ

1. Сайт – справочник [Электронный ресурс] – Определения основных терминов, связанных с локальными компьютерными сетями. – 2012. – Режим доступа: https://en.wikipedia.org/wiki/Local_area_network

2. Сайт с лекциями о локальных компьютерных сетях. [Электронный ресурс] – Классификация локальных компьютерных сетей. – 2014. – Режим доступа: https://sites.google.com/site/websitecomputernetworks/home/lection/2

3. Сайт дистанционного обучения. [Электронный ресурс] – Топологии локальных компьютерных сетей. – 2012. – Режим доступа: http://www.lessons-tva.info/edu/telecom-loc/m1t4_3loc.html

4. Сайт центра промышленной автоматизации. [Электронный ресурс] – Типы кабелей и проводов. – 2014. – Режим доступа: http://ruaut.ru/content/publikacii/electro/tipy-kabeley-i-provodov-silovoy-koaksialnyy-optovolokonnyy-kabel-i-vitaya-para.html

5. Информационный портал. [Электронный ресурс] – Статья об оптоволоконных кабелях. – 2016. – Режим доступа: https://habrahabr.ru/company/ua-hosting/blog/267859/

6. Сайт о беспроводных компьютерных сетях. [Электронный ресурс] – Беспроводные компьютерные сети, стандартные протоколы передачи данных и защиты соединения. – 2015. – Режим доступа: http://wi-fi.na.by/

7. Сайт сервиса предоставляющего услуги по настройке Wi-fi. [Электронный ресурс] – Безопасность в сетях Wi-fi. – 2015. – Режим доступа: http://www.getwifi.ru/psecurity.html

8. Сайт о компьютерных сетях. [Электронный ресурс] – Основные сетевые сервисы. – 2013. – Режим доступа: http://embedded.ifmo.ru/embedded_old/ETC/REFERAT/crc/crc.htm

ПРИЛОЖЕНИЕ А

Схема СКС структурная

ПРИЛОЖЕНИЕ Б

Схема СКС функциональная

ПРИЛОЖЕНИЕ В

План этажа