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:

«Разработка локальной компьютерной сети»

БГУИР КР 1–40 02 01 01 005 ПЗ

Студент Ситкин К.Е.

Руководитель: Одинец Д.Н.

Минск 2018

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc502008098)

[1 ОБЗОР ЛИТЕРАТУРЫ 4](#_Toc502008099)

[1.1 Общие положения 4](#_Toc502008100)

[1.2 Беспроводные компьютерные сети (WLAN) 5](#_Toc502008101)

[1.3 Топологии локальных компьютерных сетей 8](#_Toc502008102)

[1.4 Туннелирование 10](#_Toc502008103)

[1.5 Механизм 6rd 11](#_Toc502008104)

[2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ 12](#_Toc502008105)

[2.1 Выбор способа организации локальной сети 12](#_Toc502008106)

[2.2 Выбор способа связи между корпусами 12](#_Toc502008107)

[3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ 13](#_Toc502008108)

[3.1 Выбор и настройка беспроводных маршрутизаторов 13](#_Toc502008109)

[3.2 Выбор и настройка коммутаторов 17](#_Toc502008110)

[3.3 Выбор и настройка файлового сервера 19](#_Toc502008111)

[3.4 Клиентская часть настройки сети 21](#_Toc502008112)

[3.5 Перечень используемого оборудования 23](#_Toc502008113)

[3.6 Адресация в локальной сети 24](#_Toc502008114)

[4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ 26](#_Toc502008115)

[4.1 Проведение необходимых монтажных работ 26](#_Toc502008116)

[4.2 Витая пара 26](#_Toc502008117)

[ЗАКЛЮЧЕНИЕ 27](#_Toc502008118)

[СПИСОК ЛИТЕРАТУРЫ 28](#_Toc502008119)

[ПРИЛОЖЕНИЕ А 29](#_Toc502008120)

[ПРИЛОЖЕНИЕ Б 30](#_Toc502008121)

[ПРИЛОЖЕНИЕ В 31](#_Toc502008122)

[ПРИЛОЖЕНИЕ Г 32](#_Toc502008123)

[ПРИЛОЖЕНИЕ Д 33](#_Toc502008124)

# ВВЕДЕНИЕ

В настоящее время на предприятиях и в учреждениях нашли широкое применение ЛВС, основное назначение которых обеспечить доступ к общесетевым (информационным, программным и аппаратным) ресурсам. Кроме того, ЛВС позволяют сотрудникам предприятий оперативно обмениваться друг с другом информацией.

ЛВС применяются для решения таких проблемы как:

* Распределение данных. Данные в локальной сети хранятся на центральном ПК и могут быть доступны на рабочих станциях. В связи с этим не надо на каждом рабочем месте иметь накопители для хранения одной и той же информации.
* Распределение ресурсов. Периферийные устройства могут быть доступны для всех пользователей ЛВС. Такими устройствами могут быть, например, сканер или лазерный принтер.
* Распределение программ. Все пользователи ЛВС могут совместно иметь доступ к программам, которые были централизованно установлены на одном из компьютеров.

Локальная вычислительная сеть (ЛВС) представляет собой соединение нескольких ПК с помощью соответствующего аппаратного и программного обеспечения. В локальных сетях скорость передачи данных высока, протоколы в сравнении с протоколами глобальных сетей относительно просты, отсутствует избыточность каналов связи. В рамках данного курсового проекта будет описано построение локальной компьютерной сети для научно-исследовательской организации, занимающейся исследованиями в области медицины.

Основными требованием являются объединение в одну сеть двух удаленных корпусов и возможность хранить данные на файловом сервере.

# 1 ОБЗОР ЛИТЕРАТУРЫ

В данном разделе будет рассмотрены локальные компьютерные сети, а также сервисы, используемые в них.

## 1.1 Общие положения

Компьютерная сеть – это множество компьютеров, соединенных линиями связи и работающих под управлением специального программного обеспечения.

Под линией связи обычно понимают совокупность технических устройств, и физической среды, обеспечивающих передачу сигналов от передатчика к приемнику. В реальной жизни примерами линий связи могут служить участки кабеля и усилители, обеспечивающие передачу сигналов между коммутаторами телефонной сети. На основе линий связи строятся каналы связи.

Каналом связи обычно называют систему технических устройств и линий связи, обеспечивающую передачу информации между абонентами. Соотношение между понятиями "канал" и "линия" описывается следующим образом: канал связи может включать в себя несколько разнородных линий связи, а одна линия связи может использоваться несколькими каналами (Рис. 1.1).

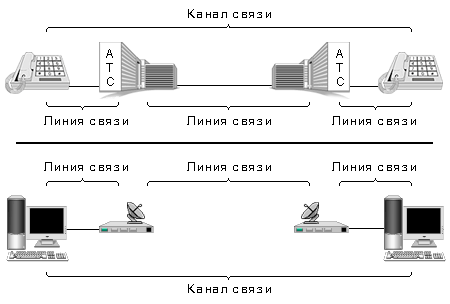


Рис. 1.1. Линии и каналы связи.

К локальным сетям (Local Area Network, LAN) обычно относят сети, компьютеры которых сосредоточены на относительно небольших территориях (как правило, в радиусе до 1-2 км). Классическим примером локальных сетей является сеть одного предприятия, расположенного в одном или нескольких стоящих рядом зданиях. Небольшой размер локальных сетей позволяет использовать для их построения достаточно дорогие и высококачественные технологии, что обеспечивает высокую скорость обмена информацией между компьютерами (Рис 1.2).[2]

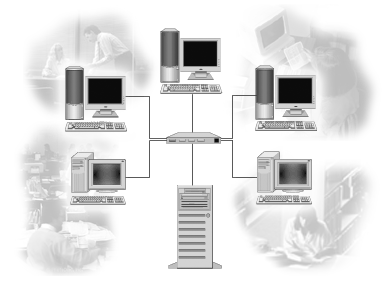


Рис. 1.2. Пример локальной сети.

Интернет является еще одним примером сети, которая уже давно стала всемирной и всеобъемлющей, включающей в себя сотни тысяч различных сетей и сотни миллионов компьютеров. Независимо от того, как вы получаете доступ к Интернету, с помощью модема, локального или глобального соединения, каждый пользователь Интернета является фактически сетевым пользователем. Для работы в Интернете используются самые разнообразные программы, такие как обозреватели Интернета, программы для работы с электронной почтой и многие другие.

Компьютер, который подключен к сети, называется рабочей станцией. Как правило, с этим компьютером работает человек. В сети присутствуют и такие компьютеры, на которых никто не работает. Они используются в качестве управляющих центров в сети и как накопители информации. Такие компьютеры называют серверами.

Если компьютеры расположены сравнительно недалеко друг от друга и соединены с помощью высокоскоростных сетевых адаптеров то такие сети называются локальными. При использовании локальной сети компьютеры, как правило, расположены в пределах одной комнаты, здания или в нескольких близко расположенных домах.

Для объединения компьютеров или целых локальных сетей, которые расположены на значительном расстоянии друг от друга, используются модемы, а также выделенные, или спутниковые каналы связи. Такие сети носят название глобальные. Обычно скорость передачи данных в таких сетях значительно ниже, чем в локальных. [1]

## 1.2 Беспроводные компьютерные сети (WLAN)

Беспроводные компьютерные сети (Wireless Local Area Network, WLAN) – сети, полностью соответствующие стандартам для обычных проводных сетей (например, Ethernet), построенные без использования кабельной проводки. В качестве носителя информации в таких сетях выступают высокой частоты.

Беспроводные сети используются там, где кабельная проводка затруднена или невозможна. Сеть, развернутая в соответствии со стандартом “RadioEthernet”, представляет собой аналог обычной кабельной сети Ethernet с коллизионным механизмом доступа к среде передачи данных. Разница состоит только в характере этой среды. Radio Ethernet полностью обеспечивает все потребности беспроводной передачи данных внутри помещений.

Как правило, для организации частной группы используется именно WiFi технология, так как она обладает оптимальными характеристиками – достаточно большой радиус действия, доступность (дешевизна) и возможность объединить в одну группу до 200 ПК и ноутбуков. Более того, любой современный ноутбук, смартфон, планшет, телевизор, принтер и другая техника имеет встроенный WiFi модуль. Это делает данную технологию в полной мере универсальной и идеально подходящей для офисов и частных домов или квартир.[3]

Существует несколько типов беспроводных сетей, которые отличаются между собой масштабами:

* PAN – самый простой тип соединения, объединяющий устройства одного хозяина, к примеру, ПК, ноутбук, смарфоны и планшеты, находящиеся в одной квартире;
* LAN – более востребованный тип соединения. AN в данном случае означает Area Network, L – local (локальный). Такие группы объединяют два и больше абонентских устройств (ПК) в одной квартире или даже в целом здании;
* CAN – кампусная связь, которая способна объединить несколько близко расположенных друг от друга зданий;
* MAN – это второй по масштабу тип соединения, который может объединять компьютеры в пределах одного или даже нескольких соседних городов;
* WAN – это так называемая глобальная сеть, которая может связывать абонентские устройства в пределах целых регионов и стран.

Значительным преимуществом беспроводных локальных сетей является то, что их проще и дешевле разворачивать и модифицировать, так как вся громоздкая кабельная инфраструктура оказывается излишней. Также в этот список можно добавить и обеспечение мобильности пользователей. Однако за эти преимущества беспроводные сети расплачиваются длинным перечнем проблем, которые несет с собой неустойчивая и непредсказуемая беспроводная среда.

Помехи от разнообразных бытовых приборов и других телекоммуникационных систем, атмосферные помехи и отражения сигнала создают серьезные трудности для надежного приема информации. Если сеть строится в здании, это создает дополнительные проблемы. Неравномерное распределение интенсивности сигнала приводит не только к битовым ошибкам передаваемой информации, но и к неопределенности зоны покрытия беспроводной локальной сети. В проводных локальных сетях такой проблемы нет, поскольку только те устройства, которые подключены к кабельной системе здания или кампуса, получают сигналы и участвуют в работе LAN. Беспроводная локальная сеть не имеет точной области покрытия. Часто используемое изображение такой области в форме шестиугольника или круга является не чем иным, как абстракцией. В действительности, сигнал может быть настолько ослаблен, что устройства, находящиеся в предполагаемых пределах зоны покрытия, вообще не могут принимать и передавать информацию.

Главная причина уязвимости пользовательских данных, когда эти данные передаются через сети Wi-Fi, заключается в том, что обмен происходит по радиоволне. А это дает возможность перехвата сообщений в любой точке, где физически доступен сигнал WiFi. Упрощенно говоря, если сигнал точки доступа можно уловить на дистанции 50 метров, то перехват всего сетевого трафика этой Wi-Fi сети возможен в радиусе 50 метров от точки доступа. В соседнем помещении, на другом этаже здания, на улице.

Точка доступа, включает в свою WiFi сеть только то устройство, которое пришлет правильный (указанный в настройках точки доступа) пароль. При этом пароль тоже пересылается зашифрованным, в виде хэша. Хэш это результат необратимого шифрования. То есть данные, которые переведены в хэш, расшифровать нельзя. Если злоумышленник перехватит хеш пароля он не сможет получить пароль.

Тем, не менее, не смотря на то, что наиболее современный метод защиты WiFi сети (WPA2) надежен, эта сеть может быть взломана. Есть две методики доступа к сети под защитой WPA2: подбор пароля по базе паролей (так называемый перебор по словарю) и использование уязвимости в функции WPS.

В первом случае злоумышленник перехватывает хеш пароля к точке доступа. Затем по базе данных, в которой записаны тысячи, или миллионы слов, выполняется сравнение хешей. Из словаря берется слово, генерируется хеш для этого слова и затем этот хеш сравнивается с тем хешем который был перехвачен. Если на точке доступа используется примитивный пароль, тогда взлом пароля, этой точки доступа, вопрос времени. Например пароль из 8 цифр (длина 8 символов это минимальная длина пароля для WPA2) это один миллион комбинаций. На современном компьютере сделать перебор одного миллиона значений можно за несколько дней или даже часов.

Во втором случае используется уязвимость в первых версиях функции WPS. Эта функция позволяет подключить к точке доступа устройство, на котором нельзя ввести пароль, например принтер. При использовании этой функции, устройство и точка доступа обмениваются цифровым кодом и если устройство пришлет правильный код, точка доступа авторизует клиента. В этой функции была уязвимость - код был из 8 цифр, но уникальность проверялась только четырьмя из них. То есть для взлома WPS нужно сделать перебор всех значений которые дают 4 цифры. В результате взлом точки доступа через WPS может быть выполнен буквально за несколько часов, на любом, самом слабом устройстве.

Точка доступа может работать в одном из двух режимов - открытом или защищенном. В случае открытого доступа, подключиться к точке досутпа может любое устройство. В случае защищенного доступа подключается только то устройство, которое передаст правильный пароль доступа.

Существует три типа (стандарта) защиты WiFi сетей:

* WEP (Wired Equivalent Privacy). Самый первый стандарт защиты. Сегодня фактически не обеспечивает защиту, поскольку взламывается очень легко благодаря слабости механизмов защиты.
* WPA (Wi-Fi Protected Access). Хронологически второй стандарт защиты. На момент создания и ввода в эксплуатацию обеспечивал эффективную защиту WiFi сетей. Но в конце нулевых годов были найдены возможности для взлома защиты WPA через уязвимости в механизмах защиты.
* WPA2 (Wi-Fi Protected Access). Последний стандарт защиты. Обеспечивает надежную защиту при соблюдении определенных правил. На сегодняшний день известны только два способа взлома защиты WPA2. Перебор пароля по словарю и обходной путь, через службу WPS.

Таким образом, для обеспечения безопасности сети WiFi необходимо выбирать тип защиты WPA2. Однако не все клиентские устройства могут его поддерживать. Например Windows XP SP2 поддерживает только WPA.[4]

MAC-фильтр – определяет список MAC-адресов устройств, которые будут иметь доступ к Вашей сети, либо для которых доступ к сети будет запрещен. MAC-фильтр наряду с шифрованием, аутентификацией и ключом шифрования (паролем от Wi-Fi сети) является дополнительной мерой защиты Вашей беспроводной сети. К примеру, если Вы хотите ограничить доступ посторонним лицам к Вашей сети, или разрешить доступ только своим устройствам. Иногда его используют в качестве функции «родительский контроль» и запрещают подключение к сети устройствам ребенка. В качестве исходных данных для того, чтобы задать правило, используется MAC-адрес устройства, которому Вы хотите разрешить или запретить доступ. Для беспроводных адаптеров серии DWA MAC-адрес устройства обычно указан на упаковке устройства, либо же на стикере расположенном на нижней части адаптера.[5]

1.3 Топологии локальных компьютерных сетей

Топологией сети называется физическую или электрическую конфигурацию кабельной системы и соединений сети. В топологии сетей применяют несколько специализированных терминов:

* узел сети - компьютер, либо коммутирующее устройство сети;
* ветвь сети - путь, соединяющий два смежных узла;
* оконечный узел - узел, расположенный в конце только одной ветви;
* промежуточный узел - узел, расположенный на концах более чем одной ветви;
* смежные узлы - узлы, соединенные, по крайней мере, одним путём, не содержащим никаких других узлов.

Одним из подходов к классификации топологий ЛКС является выделение двух основных классов топологий: широковещательные и последовательные. В широковещательных топологиях ПК передает сигналы, которые могут быть восприняты остальными ПК. К таким топологиям относятся топологии: общая шина, дерево, звезда.

В последовательных топологиях информация передается только одному ПК. Примерами таких топологий являются: произвольная (произвольное соединение ПК), кольцо, цепочка.

При выборе конкретного типа сети важно учитывать ее топологию. Основными сетевыми топологиями являются: шинная (линейная) топология, звездообразная, кольцевая и древовидная.

«Звезда» – такая топология, в которой каждый компьютер подключается отдельным кабелем к общему устройству, называемому концентратором, который находится в центре сети (Рис. 1.3).



Рис. 1.3. Топология «Звезда»

В функции концентратора входит направление передаваемой компьютером информации одному или всем остальным компьютерам сети. Главное преимущество этой топологии перед общей шиной - существенно большая надежность. Любые неприятности с кабелем касаются лишь того компьютера, к которому этот кабель присоединен, и только неисправность концентратора может вывести из строя всю сеть. Кроме того, концентратор может играть роль интеллектуального фильтра информации, поступающей от узлов в сеть, и при необходимости блокировать запрещенные администратором передачи.

К недостаткам топологии типа звезда относится более высокая стоимость сетевого оборудования из-за необходимости приобретения концентратора. Кроме того, возможности по наращиванию количества узлов в сети ограничиваются количеством портов концентратора. В настоящее время иерархическая звезда является самым распространенным типом топологии связей как в локальных, так и глобальных сетях.[6]

## 1.4 Туннелирование

Туннелирование — процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов. Туннелирование представляет собой метод построения сетей, при котором один сетевой протокол инкапсулируется в другой. От обычных многоуровневых сетевых моделей (таких как OSI или TCP/IP) туннелирование отличается тем, что инкапсулируемый протокол относится к тому же или более низкому уровню, чем используемый в качестве тоннеля.Суть туннелирования состоит в том, чтобы «упаковать» передаваемую порцию данных, вместе со служебными полями, в новый «конверт» для обеспечения конфиденциальности и целостности всей передаваемой порции, включая служебные поля. Туннелирование может применяться на сетевом и на прикладном уровнях. Комбинация туннелирования и шифрования позволяет реализовать закрытые виртуальные частные сети (VPN). Туннелирование обычно применяется для согласования транспортных протоколов либо для создания защищённого соединения между узлами сети.

Инициатор туннеля встраивает (инкапсулирует) пакеты в новый пакет, содержащий наряду с исходными данными новый заголовок с информацией об отправителе и получателе. Несмотря на то, что все передаваемые по туннелю пакеты являются пакетами IP, инкапсулируемые пакеты могут принадлежать к протоколу любого типа, включая пакеты немаршрутизируемых протоколов. Маршрут между инициатором и терминатором туннеля определяет обычная маршрутизируемая сеть IP, которая может быть и сетью, отличной от Internet. Терминатор туннеля выполняет процесс, который является обратным инкапсуляции — он удаляет новые заголовки и направляет каждый исходный пакет в локальный стек протоколов или адресату в локальной сети. Инкапсуляция сама по себе никак не влияет на защищенность пакетов сообщений, передаваемых по туннелю VPN. Но инкапсуляция даёт возможность полной криптографической защиты инкапсулируемых пакетов. Конфиденциальность инкапсулируемых пакетов обеспечивается путём их криптографического закрытия, т. е. зашифровывания, а целостность и подлинность — путём формирования цифровой подписи. Так как существует множество методов криптозащиты данных, необходимо чтобы инициатор и терминатор туннеля использовали одни и те же методы и могли согласовывать друг с другом эту информацию. Более того, для возможности расшифровывания данных и проверки цифровой подписи при приеме инициатор и терминатор туннеля должны поддерживать функции безопасного обмена ключами. Чтобы туннели VPN создавались только между уполномоченными пользователями, конечные стороны взаимодействия требуется аутентифицировать.

## 1.5 Механизм 6rd

6rd — переходный механизм, позволяющий интернет-провайдерам предоставлять клиентам IPv6 подключение поверх своей IPv4 сети. Этот механизм похож на 6to4, но действует в пределах сети интернет-провайдера, что позволяет избежать крупных архитектурных проблем, связанных с дизайном 6to4. Интернет-провайдер, желающий предоставить своим клиентам доступ к IPv6-интернету, но не имеющий возможности замены несовместимого с IPv6 оборудования, может установить 6rd-шлюз и выделить для каждого IPv4-адреса своей сети IPv6-подсеть. При этом клиенты, находящиеся в одном 6rd-сегменте, будут обмениваться данными напрямую, минуя 6rd-шлюз.

Интернет-провайдер должен передать клиентам IPv6-префикс 6rd-сегмента, длину IPv4-префикса сети и IPv4-адрес 6rd-шлюза. Настройки клиентам можно передать с помощью DHCP или же через TR-069. Клиент используя длину IPv4-префикса сети, отбрасывает не уникальные биты своего IPv4-адреса. Прибавив уникальные биты IPv4-адреса к IPv6-префиксу 6rd-сегмента и длину 6rd-префикса к количеству уникальных бит, получается персональный IPv6-префикс.

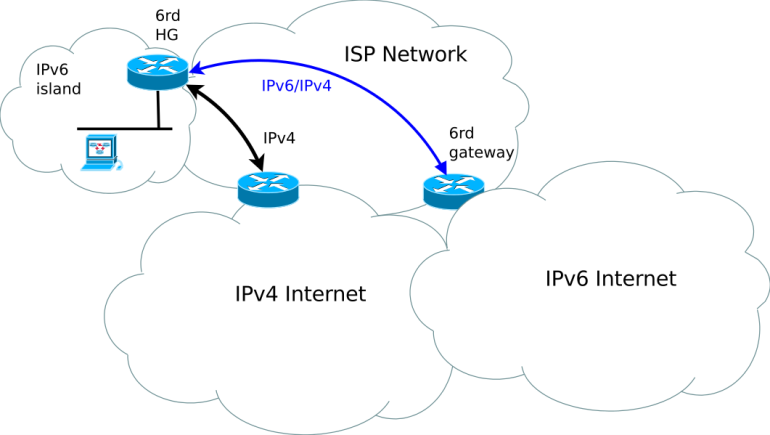


Рис. 1.4. Механизм 6rd

6rd-узел желающий отправить IPv6-пакет инкапсулирует его в IPv4-пакет и проверяет находится ли получатель в том же 6rd-сегменте, если нет, то пакет отправляется 6rd-шлюзу провайдера, который извлекает IPv6-пакет и передаёт его дальше по IPv6-сетям. Если получатель находится в том же 6rd-сегменте, то IPv4-адрес получателя создаётся дополнением IPv4 префикса битами из IPv6 адреса получателя не входящими в 6rd-префикс.

# 2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе описывается структура и порядок ее выбора локальной сети, а также способ подключения её к Internet.

## 2.1 Выбор способа организации локальной сети

При организации WLAN-сетей значительную роль играет 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 случае помещений организации, для которой разрабатывается сеть, расстояние до всех беспроводных устройств будет небольшим. Будет использоваться сеть стандарта 802.11n.

Персональные компьютеры будут подключены к коммутаторам, а коммутаторы к маршрутизаторам.

Связь коммутаторов с маршрутизаторами и с персональными компьютерами будет произведена с помощью кабелей Ethernet. Сетевые принтеры будет подключены к маршрутизатору с помощью USB-кабелей.

Проектируемая локальная сеть будет состоять из 14 персональных компьютеров, 3-х ноутбуков, 17 смартфонов, 2-х принтеров, 4-х 2-х маршрутизаторов с доступом в Internet, 2-х коммутаторов и файлового сервера.

## 2.2 Выбор способа связи между корпусами

Для объединения двух удаленных зданий в единую сеть можно создать физическое соединение, арендовать его у провайдера или создать туннель через публичную сеть. Прокладывание физического соединения слишком дорогое и требует множества разрешений, а арендовать его у провайдера нельзя, т. к. провайдер предоставляет подключение через ADSL2+. Таким образом, единственным вариантом остается создание туннеля через сеть Internet.

# 3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

Все устройства, находящиеся в одном здании, должны входить в одну подсеть. В качестве адресов были выбраны 192.168.1.0/24 и 192.168.2.0/24 соответственно. На маршрутизаторе должен быть настроен сервис DHCP для быстрого и простого подключения сторонних устройств к локальной сети, а также для обеспечения масштабируемости.

## 3.1 Выбор и настройка беспроводных маршрутизаторов

В качестве беспроводного маршрутизатора был выбран маршрутизатор TP-Link Archer D20 (рис. 3.1).



Рис. 3.1. Маршрутизатор TP-Link Archer D20.

Настройка беспроводного маршрутизатора будет проходить в 6 этапов:

1. Смена пароля на маршрутизаторе.
2. Настройка локальной сети.
3. Настройка подключения к Internet.
4. Настройка Wi-Fi.
5. Создание IPv6 туннеля.
6. Подключение принтера.

Для входа в интерфейс маршрутизатора необходимо ввести в веб-браузере *http://tplinkmodem.net*. Откроется страница установки пароля на маршрутизатор. Нужно дважды ввести новый пароль, после чего нажать на кнопку «Save» (Рис. 3.2). После этого нужно ввести новый пароль и нажать кнопку «Login».

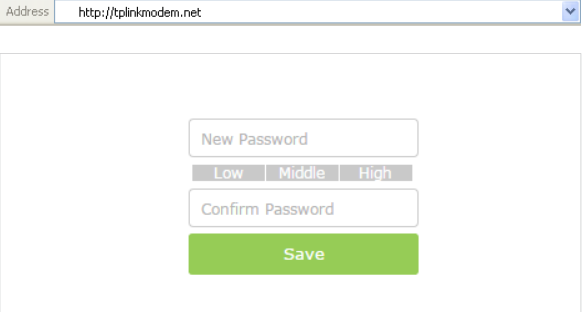


Рис. 3.2. Смена пароля на маршрутизаторе.

Следующим шагом будет настройка локальной сети. Для начала, необходимо перейти на страницу Advanced > Network > LAN Settings и выбрать IPv4. Там нужно ввести IP-адрес маршрутизатора и маску подсети (Рис. 3.3). Далее повторить аналогичные действия с IPv6.

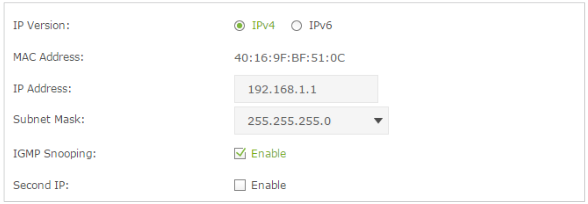


Рис. 3.3. Настройка адреса IPv4.

После этого следует настроить DHCP-сервер. Для этого нужно включить DHCP, назначить список предлагаемых IP-адресов, указать маршрут по умолчанию (рис. 3.4).

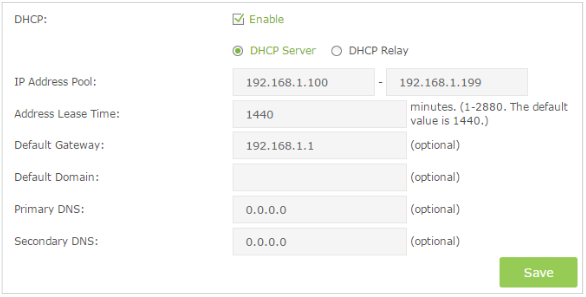


Рис. 3.4. Настройка DHCP.

Указывать статические маршруты не требуется, т. к. на обоих маршрутизаторах будет указан маршрут по умолчанию на противоположный.

Далее следует настроить подключение к сети Internet. На странице Internet вкладки Basic необходимо выбрать провайдера, а также ввести логин и пароль, указанные в договоре с провайдером (рис. 3.5).

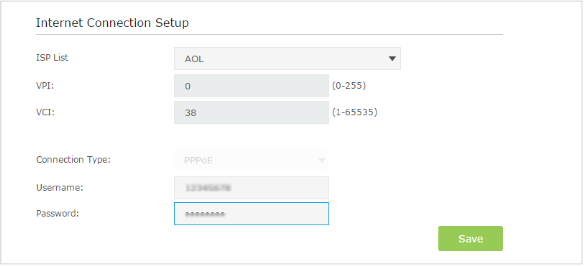


Рис. 3.5. Ввод параметров подключения.

Для настройки подключения по IPv6, необходимо войти в Advanced > Network > Internet, где выбрать нужный WAN-интерфейс и нажать кнопку «Изменить». Тип адресации выставляется исходя из данных, предоставляемых провайдером.

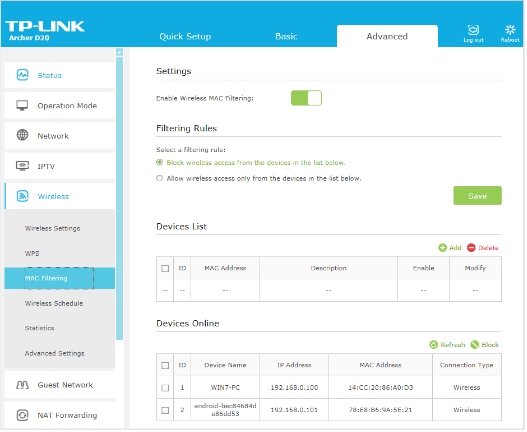


Рис. 3.6. Настройка фильтра MAC-адресов.

После получения доступа к сети Internet и защиты web-интерфейса необходимо настроить Wi-Fi. В веб-интерфейсе необходимо выбрать Quick Setup > Wireless settings, где нужно указать новый SSID (идентификатор сети) и настроить защиту подключения WPA-PSK/WPA2-PSK, ввести пароль.

Для дополнительной защиты сети необходимо в ручном режиме внести mac-адреса всех беспроводных устройств в таблицу фильтра mac-адресов, выбрать режим разрешения доступа перечисленным устройствам. Это делается во вкладке Advanced > Wireless > MAС Filtering. Там нужно разрешить фильтрацию по MAC-адресу, выбрать правило фильтрации «Allow wireless access only from the device in thelist below» (Рис. 3.6).

Чтобы добавить адрес в список, необходимо нажать кнопку «Add», ввести MAC-адрес (его можно скопировать в списке подключенных устройств, если нужное устройство сейчас подключено) и сохранить.

Для установки соединения между зданиями, необходимо использовать VPN туннель. Поскольку публичный адрес провайдером предоставляется только для IPv6, это будет IPv6 туннель по технологии 6rd. Для его настройки необходимо зайти на страницу Advanced > Network > IPv6 Tunnel. Там нужно включить IPv6 туннель, выбрать технологию 6rd, выбрать ручную установку настроек. Ввести соответствующий IPv6 префикс и его длину, а также граничный адрес IPv4 (Рис. 3.7).

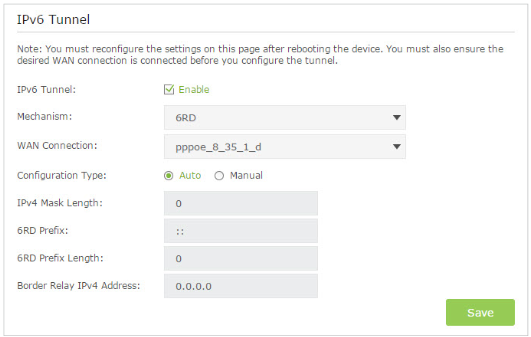


Рис. 3.7. Создание IPv6 туннеля.

Последним шагом нужно подключить принтер. Для этого нужно скачать с официального сайта и установить утилиту TP-LINK USB Printer Controller. В ней необходимо выбрать нужный принтер. В меню «Автоподключение» выбрать «Установить автоподключение к принтеру» (Рис. 3.8).

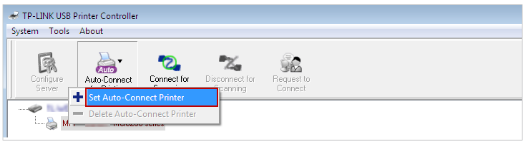


Рис. 3.8. Настройка подключения к принтеру.

## 3.2 Выбор и настройка коммутаторов

В качестве коммутаторов был выбран TP-Link TL-SL2218 (Рис. 3.9).



Рис. 3.9 Коммутатор TP-Link TL-SL2218.

Для настройки коммутатора необходимо подключиться к нему через кабель. Открыть браузер и перейти по адресу http://192.168.0.1. Откроется окно входа в Web-интерфейс коммутатора. Там необходимо ввести логин и пароль admin (Рис. 3.10).



Рис. 3.10. Вход в веб-интерфейс коммутатора.

Во вкладке System > System Info > System IP нужно указать IP-адрес коммутатора, маску подсети и маршрут по умолчанию, после чего нажать «Apply» (Рис. 3.11).

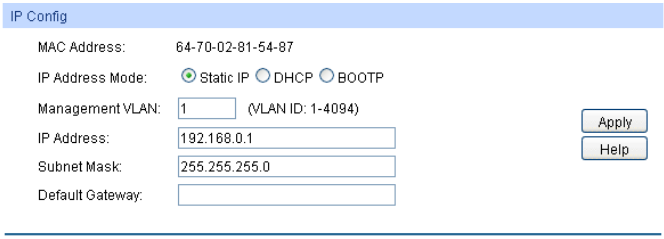


Рис. 3.11. Настройка IP-адреса коммутатора.

В меню System > User management > User config следует выбрать изменение учетной записи администратора (Рис. 3.12), где сменить пароль, что необходимо для защиты доступа к коммутатору.

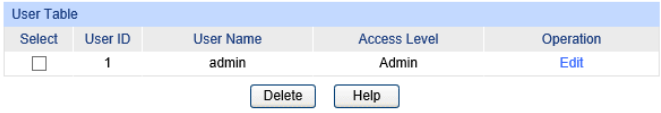


Рис. 3.12. Таблица пользователей.

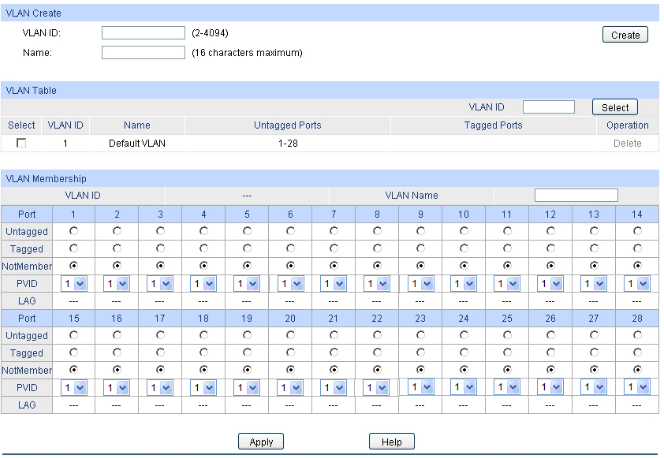


Рис. 3.13. Таблица VLAN.

Во вкладке VLAN > 802.1Q VLAN > VLAN Config нужно создать VLAN, для чего ввести его ID и нажать Create. Далее для созданного VLAN в портах, ведущих к оконечным устройствам, выбрать Untagged, а порт, ведущий к маршрутизатору настроить как Tagged (Рис. 3.13).

## 3.3 Выбор и настройка файлового сервера

В качестве файлового сервера был выбран ELSYS D100 Mini G3 (рис. 3.14).



Рис. 3.14. Файловый сервер ELSYS D100 Mini G3.

Сначала необходимо открыть Диспетчер серверов. Он может быть запущен из панели быстрого запуска. Выбрать меню Управление > Добавить роли и компоненты. В открывшемся окне выбрать «Установка ролей и компонентов» и нажимать «Далее». (Рис. 3.15)



Рис. 3.15. Выбор установки ролей и компонентов.

В следующем окне требуется выбирать нужный сервер и нажимать Далее. Среди ролей найти «Файловые службы и службы хранилища», раскрыть ее и проверить, что установлены галочки напротив таких компонентов, как службы хранения и файловый сервер.

Если данные службы не установлены, необходимо выбирать их и нажать «Далее». В открывшемся окне «Подтверждение установки компонентов» нажать Установить и после окончания процесса перезагрузить сервер.

Далее нужно создать общие папки, которые будут предоставлены в общее использование и перейти в ее свойства. В открывшемся окне перейти на вкладку Доступ и нажимать Расширенная настройка (Рис. 3.17).

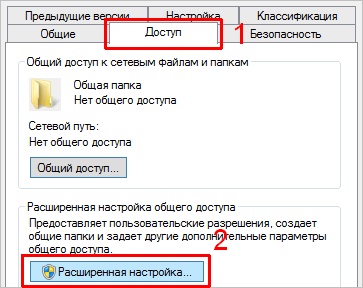


Рис. 3.17. Переход к расширенной настройке.

В расширенной настройке следует открыть общий доступ к этой папке и перейти к разрешениям (Рис. 3.18).

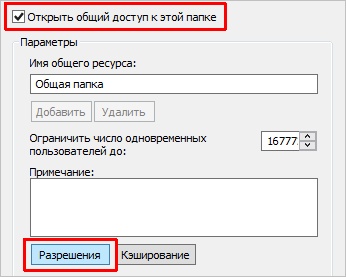


Рис. 3.18. Расширенные настройки общей папки.

Во вкладке разрешений необходимо задать права для каждой из групп пользователей (Рис. 3.19).

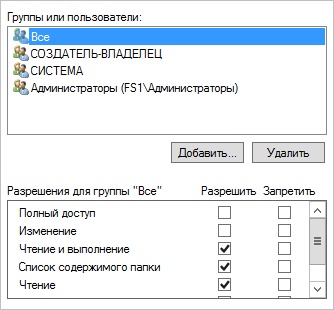


Рис. 3.19. Выбор прав для групп пользователей.

## 3.4 Клиентская часть настройки сети

Стационарные ПК подключаются посредством Ethernet, т. о. они должны иметь сетевой адаптер с разъёмом 8P8C. Ноутбуки и смартфоны подключаются посредством Wi-Fi.

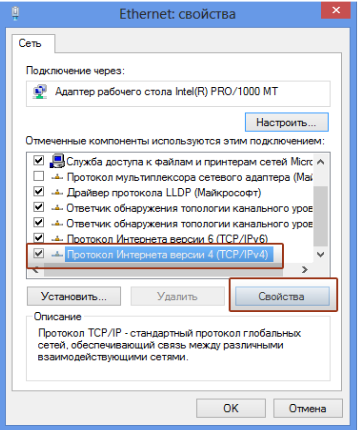


Рис. 3.20. Переход к свойствам IPv4.

В панели управления персонального компьютера необходимо выбрать раздел «Просмотр состояния сети и задач», там выбрать пункт меню «Изменение параметров адаптера». Зайти в свойства подключения по локальной сети. Открыть свойства протокола Интернета версии 4 (TCP/IPv4) (Рис. 3.20). Выбрать опции «Получть IP-адрес автоматически» и «Получить адрес DNS-сервера автоматически» (Рис. 3.21). Аналогичные действия повторить для протокола Интернета версии 6.

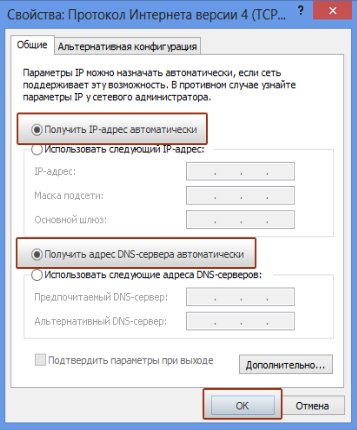


Рис. 3.21. Выбор настроек IPv4.

На мобильных устройствах необходимо выбрать нужную сеть и ввести требуемый пароль.

Для подключения сетевого принтера необходимо в Панели управления войти в раздел «Устройства и принтеры», где нажать «Добавить принтер». В следующем окне выбрать «Создать новый порт», а из выпадающего списка – «Standart TCP/IP port» (Рис. 3.22).

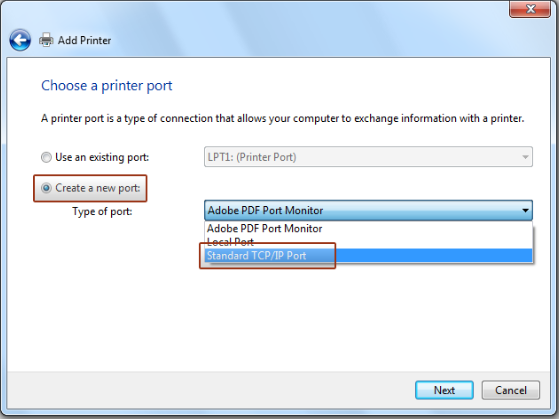


Рис. 3.22. Создание нового порта.

В поле «Имя или IP address» нужно ввести IP-адрес роутера. Далее следует выбрать производителя и модель принтера, ввести имя, под которым он будет отображаться. В следующем окне выбрать «Do not share this printer». Принтер будет отображаться как локальный. Далее повторить процедуру на всех компьютерах, которые должны иметь доступ к этому принтеру.

## 3.5 Перечень используемого оборудования

3.5.1. Маршрутизатор TP-Link Archer D20

Характеристики:

* Поддержка DSL: ADSL, ADSL2, ADSL2+.
* Стандарты беспроводных сетей: IEEE 802.11b/g/n 2,4 ГГц, IEEE 802.11a/n/ac 5 ГГц
* Защита информации: 64/128-битное WEP, WPA/WPA2, WPA-PSK/WPA2-PSK шифрование, фильтрация MAC-адресов
* Фильтрация трафика: MAC-адреса, сайты (URL), IP-адреса.
* Порты Ethernet: 3\*LAN, LAN/WAN, RJ11, USB.

3.5.2. Коммутатор TP-Link TL-SL2218.

Характеристики:

* Стандарты и протоколы: IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z, IEEE 802.3ad, IEEE 802.3x, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1p.
* 16 портов RJ45 10/100 Мбит/с (автосогласование/авто-MDI/MDIX), 2 порта RJ45 10/100/1000 Мбит/с (автосогласование/авто-MDI/MDIX), 2 комбинированных гигабитных разъёма.
* Функции 2-го уровня: IGMP Snooping V1/V2/V3, 802.3ad LACP, Spanning Tree STP/RSTP/MSTP, BPDU Filtering/Guard, TC/Root Protect, Loop back detection, 802.3x Flow Control.
* Виртуальные сети: Одновременная поддержка до 512 VLAN (из 4000 VLAN ID).

3.5.3 Файловый сервер ELSYS D100 Mini G3.

Описание:

* Процессор: Intel Xeon Processor E3-1220 v3 (4 ядра, 3.1 GHz).
* Оперативная память: 4Gb DDR3.
* Жесткие диски: 2x 1000Gb SATA 6Gb/s 7200rpm Enterprise.
* Контроллер RAID: Intel® Rapid Storage Technology SW RAID 0/1/5/10

3.5.4. Компьютер Jet MultiOffice 3C324D8H1IS50

Описание:

* Процессор: CPU Intel Core i3 3240 3400 МГц.
* Оперативная память: DDR3 8 ГБ.
* Хранение данных: HDD 1000 ГБ.
* Видеокарта: Intel HD Graphics 2500.



Рис. 3.23. Компьютер Jet MultiOffice 3C324D8H1IS50.

3.5.5. Принтер HP LaserJet CP1025 color.

Описание:

* Формат: A4.
* Тип: лазерный.
* Поддержка цветов: цветной.
* Интерфейсы: USB.

3.5.6 Монитор Acer K202HQLb

Описание:

* Диагональ: 19,5".
* Разрешение: 1600х900.
* Угол обзора по горизонтали: 90 °.
* Угол обзора по вертикали: 65 °.
* Интерфейс подключения: D-Sub (VGA)

## 3.6 Адресация в локальной сети

Адресация осуществляется с помощью протоколов IPv4 и IPv6. Сеть компании разделена на две виртуальные сети:

* Сеть первого здания – VLAN 33.
* Сеть второго здания – VLAN 94.

В таблице 3.1 указаны номера виртуальных сетей и соответствующие им IP адреса и маски.

Таблица 3.1— Соответствие номеров виртуальных сетей IP адресам и маскам

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN № | ip address | subnet mask | IPv6 address |
| 33 | 192.168.1.0 | 255.255.255.0 | 2001:0aa8:2239:0012::/64 |
| 94 | 192.168.2.0 | 255.255.255.0 | 2001:0aa8:2239:0013::/64 |

В таблице 3.2 указаны номера ПК и соответствующие им IP адреса и маски.

Таблица 3.2— Соответствие номеров ПК IP адресам и маскам

|  |  |  |  |
| --- | --- | --- | --- |
| PC № | ip address | subnet mask | IPv6 address |
| 1 | 192.168.1.10 | 255.255.255.0 | 2001:0aa8:2239:0012::a/64 |
| 2 | 192.168.1.11 | 255.255.255.0 | 2001:0aa8:2239:0012::b/64 |
| … | … | … | … |
| 5 | 192.168.1.14 | 255.255.255.0 | 2001:0aa8:2239:0012::e/64 |
| 6 | 192.168.2.10 | 255.255.255.0 | 2001:0aa8:2239:0013::a/64 |
| 7 | 192.168.2.11 | 255.255.255.0 | 2001:0aa8:2239:0013::b/64 |
| … | … | … | … |
| 14 | 192.168.1.18 | 255.255.255.0 | 2001:0aa8:2239:0013::12/64 |

В таблице 3.3 указаны другие устройства и соответствующие им IP адреса и маски.

Таблица 3.3— Адреса и маски маршрутизаторов и сервера.

|  |  |  |  |
| --- | --- | --- | --- |
| Устройство | ip address | subnet mask | IPv6 address |
| Router 1 | 192.168.1.1 | 255.255.255.0 | 2001:0aa8:2239:0012::1/64 |
| Router 2 | 192.168.2.1 | 255.255.255.0 | 2001:0aa8:2239:0013::1/64 |
| Server | 192.168.1.5 | 255.255.255.0 | 2001:0aa8:2239:0012::5/64 |

Беспроводные устройства получают адреса из пулов адресов, предоставляемых маршрутизатором.

Функциональная схема представлена в приложении «Б».

# 4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

## 4.1 Проведение необходимых монтажных работ

Поскольку здания НИИ одноэтажные и небольшие, вертикальная кабельная подсистема будет отсутствовать. Таким образом вся задача по построению кабельной системы сводится к проектированию и постройке горизонтальной кабельной подсистемы.

Поскольку маршрутизаторы находятся рядом с коммутаторами, они будут соединены короткими кабелями Ethernet, лежащими на столе. Точно также будет подключен сервер к маршрутизатору.

Одиночные кабели от коммутаторов до компьютеров директора и бухгалтера будут проложены вдоль стены.

Кабели, идущие от коммутаторов к компьютерам в лабораториях, будут проложены вдоль стены в лотках. Возле каждого компьютера предусмотрена информационная розетка.

Принтеры будут подключены к маршрутизаторам с помощью USB кабелей по столам.

Остальные устройства подключаются к сети посредством Wi-Fi и не требуют монтажных работ.

## 4.2 Витая пара

Учитывая нестандартные длины кабелей Ethernet, необходимо их укоротить до нужной длины и сделать обжим витой пары.

Поскольку кабели, которые придется укорачивать, соединяют коммутаторы и персональные компьютеры, необходимо использовать вариант разводки, называющийся прямой кабель.

Из двух вариантов обжима витой пары был выбран вариант T568B, так как он является более распространенным.

# ЗАКЛЮЧЕНИЕ

В ходе выполнения курсового проекта была разработана локальная компьютерная сеть для научно-исследовательской организации. В результате была получена завершённая структурированная кабельная система, а также произведены все настройки, необходимые для взаимодействия оконечных устройств сети.

Созданная локальная сеть получилась настолько простой, насколько это возможно в поставленных условиях и легко расширяемой. Она полностью решает все поставленные задачи:

* Доступ всех сотрудников в интернет.
* Интернет подключен с помощью ADSL2+.
* К сети имеют доступ только сотрудники.
* Все пользователи могут хранить файлы на файловом сервере.
* Два удаленных здания соединены в одну сеть защищенным персистентным соединением.

СПИСОК ЛИТЕРАТУРЫ

1. Cайт о компьютерных сетях. [Электронный ресурс] – Основные сетевые сервисы. – Режим доступа: http://embedded.ifmo.ru/embedded\_old/ETC/REFERAT/crc/crc.htm
2. Компьютерные сети. [Электронный ресурс] – Сетевые технологии – Режим доступа: http://net.e-publish.ru/p216aa1.html
3. Беспроводные сети: виды, характеристики [Электронный ресурс] – Все, что важно знать о беспроводных сетях – Режим доступа: http://bezprovodoff.com/seti/informaciya/kakie-byvayut-besprovodnye-seti.html
4. Создание сайтов [Электронный ресурс] – Защита и безопасность WiFi сети – Режим доступа: http://ru.d-ws.biz/articles/security-wifi.shtml
5. D-link [Электронный ресурс] – D-link – Режим доступа: http://www.dlink.ru/r/faq/110/1631.html
6. Информатика [Электронный ресурс] – Топология сетей – Режим доступа: http://inf.e-alekseev.ru/text/Topolog\_setey.html

# ПРИЛОЖЕНИЕ А

(обязательное)

Схема СКС структурная

# ПРИЛОЖЕНИЕ Б

(обязательное)

Схема СКС функциональная

# ПРИЛОЖЕНИЕ В

(обязательное)

План этажа первого здания

# ПРИЛОЖЕНИЕ Г

(обязательное)

План этажа второго здания

# ПРИЛОЖЕНИЕ Д

(обязательное)

Перечень оборудования, изделий и материалов