СОДЕРЖАНИЕ

[СОДЕРЖАНИЕ 2](#_Toc535393386)

[**ВВЕДЕНИЕ** 4](#_Toc535393387)

[**1** **ОБЗОР ИСТОЧНИКОВ** 6](#_Toc535393388)

[**1.1 Общие положения** 6](#_Toc535393389)

[**1.2 Требования к локальной вычислительной сети** 7](#_Toc535393390)

[**2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ** 9](#_Toc535393391)

[**2.1 Разделение сети на виртуальные подсети** 9](#_Toc535393392)

[**2.2 Выбор топологии сети** 9](#_Toc535393393)

[**2.3 Гостевая подсеть** 11](#_Toc535393394)

[**2.4 Подсеть для сотрудников организации** 11](#_Toc535393395)

[**3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ** 12](#_Toc535393396)

[**3.1 Обоснование выбора сетевой операционной системы** 12](#_Toc535393397)

[**3.2 Обоснование выбора активного сетевого оборудования** 12](#_Toc535393398)

[**3.2.1 Коммутатор Huawei S5720S-12TP-LI-AC** 13](#_Toc535393399)

[**3.2.2 Маршрутизатор EchoLife EG8240H** 15](#_Toc535393400)

[**3.2.3 Точка доступа AP2010DN** 16](#_Toc535393401)

[**3.2.4 Рабочая станция N-Tech King Office S 59585** 17](#_Toc535393402)

[**3.2.5 Многофункциональное устройство HP DeskJet 2630** 18](#_Toc535393403)

[**3.2.6 Принтер Canon PIXMA TS304** 19](#_Toc535393404)

[**3.3 Пассивное сетевое оборудование и кабеля** 20](#_Toc535393405)

[**3.4 Схема адресации** 20](#_Toc535393406)

[**3.5 Настройка точки доступа** 21](#_Toc535393407)

[**3.6 Настройка DHCP** 22](#_Toc535393408)

[**3.7 Настройка коммутаторов** 23](#_Toc535393409)

[**3.8 Настройка NAT и запрет маршрутизации между VLAN** 24](#_Toc535393410)

[**4 ПРИНЦИПИАЛЬНОЕ ПРОЕКТИРОВАНИЕ** 25](#_Toc535393411)

[**4.1 Кабельная подсистема** 25](#_Toc535393412)

[**4.2 Организация рабочих мест** 25](#_Toc535393413)

[**4.3 Физическая защита сетевого оборудования** 25](#_Toc535393414)

[**ЗАКЛЮЧЕНИЕ** 27](#_Toc535393415)

[**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** 28](#_Toc535393416)

[**ПРИЛОЖЕНИЕ Б** 30](#_Toc535393417)

[**ПРИЛОЖЕНИЕ В** 31](#_Toc535393418)

[**ПРИЛОЖЕНИЕ Г** 32](#_Toc535393419)

# **ВВЕДЕНИЕ**

На современном этапе развития человечества крайне важную роль играет глобальный доступ к большим объемам информации. От эффективности получения и работы с ней зависит корректная работа многих сфер деятельности человека. Все это привело к созданию и широкому распространению компьютерных сетей, которые предоставляют пользователям возможность не только быстрого обмена информацией на больших расстояниях, но и получения доступа к огромному количеству вычислительных ресурсов.

Одной из главных особенностей компьютерных сетей является то, что они представляют собой систему, характеристики которой в целом значительно превышают соответствующие характеристики простой суммы составляющих элементов сети при отсутствии связи между ними.

Внедрение сетей на предприятиях приводит к совершенствованию коммуникаций, то есть к улучшению процесса обмена информацией и взаимодействия меж работниками фирмы, а еще его покупателями и поставщиками. Сети понижают надобность компаний в иных формах передачи информации, этих как телефонный аппарат или же обыкновенная почта, которые заметно уступают компьютерным сетям в эффективности.

Все компьютерные сети без исключения имеют одно назначение - обеспечение совместного доступа к общим ресурсам. Ресурсы бывают 3-х видов: аппаратные, программные, информационные.

Аппаратные ресурсы – это, когда все пользователи компьютерной сети получают доступ к одному устройству, к примеру, принтеру или же используют один компьютер с большой емкостью жесткого диска (файловый сервер), на котором хранятся личные архивы или результаты работы.

Компьютерные сети могу позволить и совместно использовать программные ресурсы. Так, к примеру, для выполнения сложных и долгих расчетов вполне уместно подключиться к удаленной мощной вычислительной машине и выполнить какое-либо задание на ней, а по окончании расчетов получить результат работы обратно. Данные, хранящиеся на удаленных компьютерах, образуют информационный ресурс.

Естественно, с распространением во всех сферах деятельности человека компьютерных сетей появилось и большое количество проблем, связанных с ними. Неожиданные условия работы и обстоятельства имеют все шансы вывести из строя или же, в том числе, и полностью уничтожить сетевое оснащение, отрезав доступ к информации, собственно, что во множестве случаях практически означает остановку работы.

Довольно острой задачей стоит утрата данных вследствие людского фактора или же вышеупомянутых непредвиденных ситуаций. Поломка компьютерных сетей влечёт за собой большие убытки и, безусловно, недопустима в современном мире, в следствие этого специалисты по всему миру усердно разрабатывают контрмеры для минимизации и предотвращения неполадок при работе компьютерных сетей. Примерами этих решений можно привести резервное копирование и обеспечение дополнительных путей для доступа к данным, добавление резервных аппаратных средств, которые в случае выхода из строя основных могут заменить их, не прерывая выполнение основных задач.

Впрочем, опасности применения компьютерных сетей не ограничиваются выходом из строя одной или же другой части системы – взломы и хищение данных представляют собой огромную опасность. Тем более острой обстановка стала с повсеместным распространением глобальной сети Интернет. Нередко люди, не принимающие подабающих мер по защите сетей от несанкционированного доступа, работающих станций и серверов, в итоге позволяют получать доступ к личным сетям и данным.

Естественно, с другой стороны, обеспечение безопасности и работоспособности компьютерных сетей может быть довольно дорогостоящей, поэтому всегда стоит находить некий компромисс между всеми этими составляющими, так как не всегда затраченные средства на создание и поддержку компьютерной сети будут превышать полезность ее работы.

В эпоху цифровой информации в любой сфере деятельности нужно применять компьютерные сети, дабы оставаться конкурентоспособными по отношению к другим игрокам в этой области.

Целью данного курсового проектирования является проектирование локальной компьютерной сети для небольшой компании, поставляющей компьютерные комплектующие для клиентов. В его рамках будут рассмотрены вопросы создания топологии, выбора реального оборудования, необходимого для реализации сети, схемы прокладка сети в помещениях, а также схемы адресации.

# **ОБЗОР ИСТОЧНИКОВ**

## **1.1 Общие положения**

Локальная вычислительная сеть – это компьютерная сеть, располагающаяся на небольшой территории.

Классифицируются сети в основном по способу администрирования. Сети бывают:

1. Персональные (PAN) – персональные вычислительные сети

предназначены для взаимодействия устройств, принадлежащих одному владельцу. Обычно включают лишь несколько узлов и очень малы по занимаемой площади.

Такие сети чаще всего включают в себя беспроводные клавиатуры, мыши, смартфоны, беспроводную гарнитуру, принтеры, и многие другие устройства.

Самой распространённой технологией подключения в таких сетях является Bluetooth.

1. Локальные (LAN) – локальные сети покрывают группу зданий или

небольшую территорию. Хотя вовсе не обязательно, чтобы узлы сети были физически близко расположены друг от друга. Локальность в данном контексте значит скорее совместное локальное управление.

В локальных компьютерных сетях наиболее распространённым является проводное соединение. Оно может осуществляться через медный кабель, либо через оптоволоконный.

Наряду с проводными соединениями широко используется беспроводные соединения, соответствующие стандарту IEEE 802.11, более известные, как Wi-fi. Беспроводное соединение уступает по скорости проводному, но получило широкое распространение в быту и в бизнесе ввиду своего удобства.

1. Распределённые – распределённые сети позволяют распределить

имеющуюся вычислительную мощность на множество узлов, исключая наличие центрального сервера.

1. Городские (MAN) – городские сети связывают компьютеры в

пределах одного города.

Самый яркий пример подобной сети – сеть кабельного телевидения, в которой после модернизации появилась возможность передавать цифровые данные, и, как следствие, система стала городской (муниципальной) компьютерной сетью.

1. Глобальные (WAN) – глобальные сети связывают компьютеры на

очень больших территориях и включают в себя большое количество узлов. К примеру, Интернет является глобальной сетью.

Также можно классифицировать сети по способу управления:

1. Клиент-сервер – в таких сетях выделяются узлы, выполняющие

управляющие и обслуживающие функции (серверы). Остальные узлы являются терминальными (клиенты). Обычно конечному пользователю доступен именно клиент. В клиент-серверных сетях часто используется топология типа «звезда», когда множество узлов подключено к главному центральному.

1. Одноранговые сети – в одноранговых сетях все узлы равноправны.

Одним из главных плюсов таких сетей является доступность и сохранение работоспособности при любом количестве любых узлов сети [2].

Физически сети состоят из активного и пассивного сетевого оборудования.

Активное сетевое оборудование питается от электрической сети и выполняет функции преобразования и усиления сигнала. В перечень активного оборудования входят маршрутизаторы, коммутаторы, усилители, сервера, рабочие станции, и другие.

Пассивное же сетевое оборудование не питается от сети, не преобразовывает и не усиливает сигнал. Примерами пассивного сетевого оборудования можно привести кабели, розетки, коммутационные панели, кронштейны, кабельканалы, защитные коробы, коммутационные шкафы, и другие [3].

В разделе 3 используемое в курсовой работе оборудование будет рассмотрено более подробно.

## **1.2 Требования к локальной вычислительной сети**

Любая вычислительная сеть должна обеспечивать надёжный и быстрый доступ к любому ресурсы сети для любых её пользователей. Чтобы выполнять эту функцию, локальная вычислительная сеть должна соответствовать приведённым ниже требованиям.

Главное, и самое очевидное требование – собственно, обеспечение пользователям локальной вычислительной сети доступа к общим ресурсам данной сети и её компьютеров. Все остальные требования, хоть тоже являются крайне важными, влияют лишь на качество выполнения этой задачи.

Локальная вычислительная сеть также должна быть производительна – это требование характеризует возможность параллельной обработки задачи сразу несколькими компьютерами в сети.

Немаловажным требованием также является надёжность локальной вычислительной сети. Она, в свою очередь, делится на три критерия:

1. Вероятность доставки пакета без искажений.
2. Доля времени, в течение которого систему можно использовать.
3. Способность защиты данных от несанкционированного доступа.

Не стоит забывать также про отказоустойчивость. Это требование предполагает доступность сети даже при отказе некоторых её элементов. Отказоустойчивость обычно достигается созданием альтернативных путей данных и наличием резервного оборудования, которое заменяет собой основное в случае неисправности.

Прозрачность сети достигается в том случае, если вся сеть видна пользователю как единая вычислительная система, а не как множество отдельных вычислительных устройств.

Очень важна и расширяемость сети. Данное требование предполагает собой простое наращивание размеров сети – добавление новых узлов, пользователей, рабочих станций, замены устаревшего оборудования на более новое, и так далее.

Важным требованием является управляемость сети. Управляемость сети – это возможность контролировать работу всей локальной вычислительной сети из единого центра управления.

Вычислительные сети также должны поддерживать различные типы трафика. Сюда может входить и традиционный поток бит, а также видео, аудио.

Также вычислительной сети будет сложно существовать без совместимости, когда различное аппаратное и программное обеспечение не конфликтуют и способны сосуществовать и обмениваться информацией в одной сети без специальных конвертирующих мер – даже будучи от различных производителей, или под управлением разных операционных систем [4].

# **2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ**

## **2.1 Разделение сети на виртуальные подсети**

В компании, занимающей продажей компьютерных комплектующих есть несколько различных помещений, доступных как только персоналу, так и работниками вместе с клиентами. Но в требованиях по безопасности для разрабатываемой сети требуется изолировать посетителей от внутренних ресурсов организации, поэтому целесообразно создать две виртуальные локальные подсети. Одна подсеть VLAN 11 – гостевая для покупателей и посетителей компании, другая – VLAN 22 для сотрудников.

Структурная схема проектируемой сети представлена в приложении «А».

## **2.2 Выбор топологии сети**

Сетевая топология – это конфигурация графа, вершинами которого являются конечные узлы сети и коммуникационное оборудование – вычислительные машины и маршрутизаторы соответственно, – а рёбрам – информационные или физические связи между вершинами.

Компьютерные сети весьма и весьма удобно представлять именно в виде графов.

Наиболее вероятные кандидаты для использования в курсовом проекте:

1. Шинная – связь между любыми двумя узлами устанавливается через

один общий путь (шину). Данные, передаваемые одной станцией, становятся доступны для всех других, подключённых к этой шине. Такая топология проста, но влечёт за собой ряд проблем – например, проблему одновременной попытки доступа сразу нескольких узлов к одной и той же шине (рисунок 2.1).

1. Кольцевая – узлы связаны кольцевой линией передачи – к каждому

узлу подключены две линии. Проходя по кольцу, данные становятся доступны всем узлам (рисунок 2.2). Такая топология решает проблему одновременной попытки доступа сразу нескольких узлов к одной и той же шине, однако передача данных от одного узла к другому замедляется, поскольку данные должны пройти через несколько узлов прежде, чем попадут к адресату.

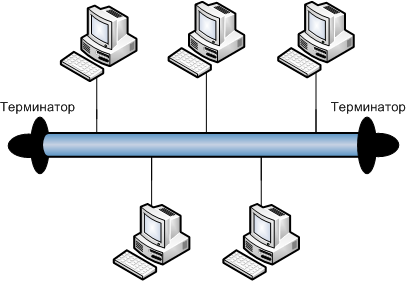
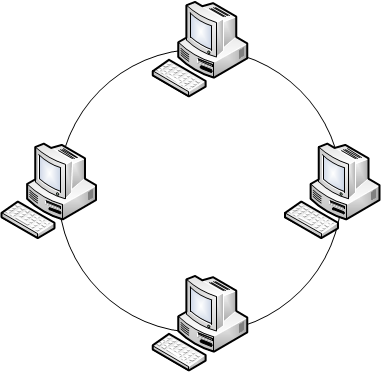
1. Звезда – к центральному узлу подключены все остальные

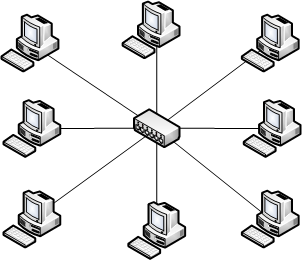
(рисунок 2.3). Основным минусом данной топологии, пожалуй, является большая нагрузка на центральный узел.

Сама топология подразумевает под собой физическое расположение компьютеров, кабелей, маршрутизаторов, коммутаторов и прочих компонентов в сети.

Стоит отметить, что различные типы топологий решают различные типы задач, так что необходимо тщательно подойти к её выбору. Он может зависеть от следующих факторов:

1. Состав имеющегося сетевого оборудования
2. Характеристики сетевого оборудования
3. Возможность расширения сети
4. Способ управления сетью

  
Рисунок 2.1 – Шинная топология  
  
  
Рисунок 2.2 – Кольцевая топология

  
Рисунок 2.3 – Топология «звезда»

На основе данного варианта и вышеприведённого материала, было принято решение использовать топологию «звезда».

## **2.3 Гостевая подсеть**

В компании имеется несколько различных помещений, из которых посетителю должен быть предоставлен доступ в интернет. В то же время, клиенты должны быть ограничены в доступе ко внутренним ресурсам организации, в связи с чем создается отдельная виртуальная подсеть VLAN 11, для беспроводного доступа покупателей к сети Интернет.

## **2.4 Подсеть для сотрудников организации**

Сотрудники компании по продаже компьютерного комплектующего работают в нескольких помещениях, в которых должны получать как беспроводной, так и проводной доступ в сеть Интернет. Поэтому для них будет создана единая виртуальная подсеть VLAN 22.

# **3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ**

## **3.1 Обоснование выбора сетевой операционной системы**

Для реализации разрабатываемое локальной компьютерной сети используется сетевое оборудование компании Huawei. В качестве операционной системы на коммутаторах и маршрутизаторах данной компании используется VRP (Versatile Routing Platform).

Сетевая ОС компании Huawei – VRP – оптимизирована для работы на многоядерных процессорах и имеет механизмы виртуализации, которые позволяют обеспечить изоляцию процессов и достичь высокой скорости обработки сетевых событий. В частности, возможность использовать протокол BFD для большинства технологий гарантирует быструю сходимость сетей, построенных на основе оборудования Huawei и ОС VRP.

Данная сетевая ОС имеет Cisco-подобный интерфейс для конфигурации (аналог CLI). Командная строка в VRP ОС имеет два основных режима:

* system-view – режим конфигурирования (для знакомых с Cisco CLI аналог conf t). В этом режиме приглашение командной строки для коммутаторов выглядит как: [Switch].
* user-view –непривилегированный режим. Режим приглашения для коммутаторов выглядит так: <Switch>.

В user-view режиме, например, доступны многие функции, в частности можно сбросить запущенные процессы. Подключения по telnet и ssh так же доступны только из user-view.

Ниже приведены основные команды, использующиеся при работе с командной строкой операционной системы VRP:

* system-view – переход из режима конфигурирования user-view в привилегированный режим system-view.
* save – запись текущих настроек в энергонезависимую память устройства.
* display current-configuration – вывод текущего файла конфигурации.
* display current-configuration configuration XXXX – вывод настроек секции XXXX.
* display this – вывод конфигурации текущей секции.
* quit – выход из текущей секции в родительскую.

## **3.2 Обоснование выбора активного сетевого оборудования**

Активное сетевое оборудование - это оборудование, содержащее электронные схемы, получающее питание от электрической сети или других источников и выполняющее функции усиления, преобразования сигналов и иные. Такое оборудование может обрабатывать сигнал по установленным алгоритмам.

В сетях данные передаются по пакетам. Каждый пакет содержит данные и техническую информацию: сведения об источнике и приёмнике, проверку целостности данных, и многое другое. Эта информация делает возможной исправную доставку адресату.

Активное сетевое оборудование не просто улавливает и передаёт сигнал, но и обрабатывает техническую информацию в соответствии со встроенными алгоритмами.

В данном курсовом проекте используется следующее активное сетевое и клиентское оборудование:

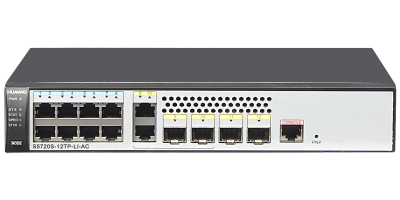
1. Коммутаторы Huawei S5720S-12TP-LI-AC
2. Маршрутизатор EchoLife EG8240H
3. Точка доступа AP2010DN
4. Рабочие станции N-Tech King Office S 59585
5. Принтер Canon PIXMA TS304
6. Многофункциональное устройство HP DeskJet 2630

Полный перечень оборудования представлен в приложении «Г».

## **3.2.1 Коммутатор** **Huawei S5720S-12TP-LI-AC**

Сетевой коммутатор – активное сетевое устройство, предназначенное для соединения нескольких узлов вычислительной сети между собой. Соединение происходит в пределах одного или нескольких сегментов сети. Коммутаторы можно рассматривать как многопортовые мосты. Стоит отметить, что работают они на втором уровне модели OSI.

В качестве коммутатора для разрабатываемой сети был выбран Huawei S5720S-12TP-LI-AC. Данной модели на 8 портов вполне хватит для всех узлов сети.

  
Рисунок 3.1 – Huawei S5720S-12TP-LI-AC [6]

Одним из важнейших критериев при выборе была управляемость коммутатора. Все коммутаторы делятся на управляемые и неуправляемые: неуправляемые не располагают своим собственном процессором, так что вносить изменения в их конфигурацию не представляется возможным.

Управляемые же коммутаторы, помимо возможности тонкой ручной настройки, обладают обширным рядом функций: мониторингом сети, механизмами управления трафиком, возможностью создавать виртуальные локальные сети, и многими другими. Соединение коммутаторов с роутером представлено в приложении «Б».

Конечно, управляемые коммутаторы на порядок дороже, но полностью оправдывают свою цену широким спектром возможностей.

Характеристики выбранного коммутатора:

Таблица 3.1 – Характеристика коммутатора Huawei S5720S-12TP-LI-AC

|  |  |
| --- | --- |
| Характеристика | Значение |
| Интерфейсы | 8 портов 10/100/1000 Base-TX |
| 2 порта SFP |
| 2 комбо-порта 10/100/1000 Base-TX |
| Таблица MAC-адресов | Таблица MAC-адресов 8К |
| Добавление и удаление записи из таблицы MAC-адресов вручную |
| Установка срока жизни MAC-адреса |
| Отключение распознавания MAC-адресов на определенном интерфейсе |
| Ограничение количества изученых MAC-адресов на интерфейсе |
| VLAN | Поддержка максимум 4K VLAN в соответствии с требованиями IEEE 802.1Q |
| Guest VLAN и Voice VLAN |
| GVRP |
| Назначение VLAN на основе типа порта, MAC-адреса, протокола, IP, политики, 1:1 и N:1 VLAN mapping |
| Маршрутизация | Static route, RIP, RIPng |
| Безопасность | Защита от DoS, ARP и ICMP атак |
| Иерархическая система доступа и управления Коммутатор Huaweiом |
| Привязка пользователя по критериям: IP, MAC, номер порта, VLAN |
| Поддержка изоляции интерфейсов |
|  | Поддержка IEEE 802.1x аутентификации и ограничение максимального количества пользователей на порте |
| Поддержка защиты IP-источника |

*Продолжение таблицы 3.1*

|  |  |
| --- | --- |
|  | Поддержка аутентификации AAA, включая RADIUS и HWTACACS+ |
| Поддержка фильтрации пакетов |
| Поддержка фильтрации МАС-адресов |
| Поддержка подавления многоадресной передачи, широковещания и неизвестных однонаправленных пакетов |
| Поддержка ограничения количества распознанных МАС-адресов Поддержка защиты CPU |
| Потребляемая мощность(максимальная) | 12.85 Вт |
| Протоколы предотвращение петель | RRPP, SEP, ERPS (G.8032), STP(IEEE 802.1d), RSTP(IEEE 802.1w), MSTP(IEEE 802.1s), BPDU protection, root protection, and loop protection |
| Сетевое управление | iStack,Virtual Cable Test (VCT) |
| Поддержка автоматического конфигурирования |
| Конфигурирование при помощи командной строки |
| Поддержка конфигурирования посредством Telnet |
| Поддержка SNMPv1/v2c/v3 |
| Поддержка RMON, SSHv2, LLDP/LLDP-MED |
| Поддержка WEB eSight NMS 802.3az EEE |

## **3.2.2 Маршрутизатор** **EchoLife EG8240H**

Маршрутизатор – это специализированный сетевой компьютер, имеющий несколько сетевых интерфейсов, который занимается пересылкой пакетов между разными сегментами сети, а также может связывать разнородных сетей с разными архитектурами. Для принятия решений о пересылке пакетов, используется различная информация о топологии сети и определённых правилах, которые устанавливаются администраторами. Работают на сетевом уровне модели OSI.

Выбор данного маршрутизатора обусловлен достаточным функционалом, необходимым для организации разрабатываемой локальной компьютерной сети, и относительно небольшой стоимостью в связи с дополнительными требованиями к малым затратам по финансам.

EchoLife EG8240H обладает следующими характеристиками:

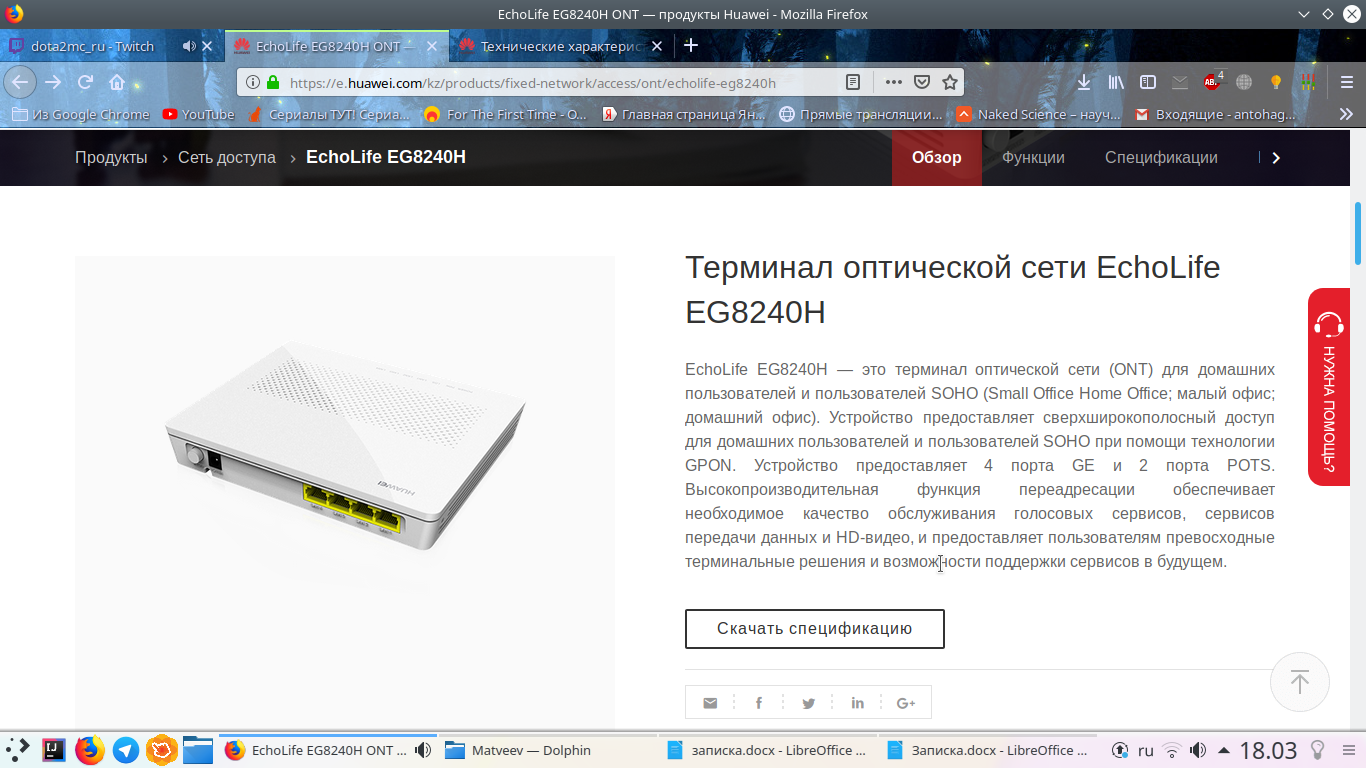
* Порты: 2xPOTS FXS, 4xGE
* Поддержка технологии GPON
* Статическая потребляемая мощность: 4 Вт
* Максимальная потребляемая мощность: 7.8 Вт
* Безопасность: фильтрация MAC-адресов
* Снижение энергопотребления незадействованных компонентов в энергосберегающем режиме
* Обнаружение и изоляция активных и пассивных неисправных ONT
* 802.1ag Ethernet OAM
* Диагностика и измерение показателей оптической линии
* Резервирование данных ПО и возврат к предыдушей версии на базе сдвоенной системы
* OMCI, пользовательский веб-интерфейса
* IGMP snooping v2, v3
* MDL snooping v1, v2
* VLAN с технологией QinQ

Рисунок 3.2 - EchoLife EG8240H [7]

## **3.2.3 Точка доступа** **AP2010DN**

Точка доступа ‑ это беспроводная базовая станция, предназначенная для обеспечения беспроводного доступа к уже существующей сети (беспроводной или проводной) или создания новой беспроводной сети.

Точки доступа призваны выполнять самые разнообразные функции, как для подключения группы компьютеров (каждый с беспроводным сетевым адаптером) в самостоятельные сети (режим Ad-hoc), так и для выполнения функции моста между беспроводными и кабельными участками сети (режим Infrastructure).



Рисунок 3.3 - WiFi точка доступа AP2010DN [8]

Характеристики выбранной точки доступа:

Таблица 3.2 – Основные характеристики Huawei AP2010DN

|  |  |
| --- | --- |
| Входное напряжение | Питание PoE соответствует стандарту IEEE 802.3af/at |
| Максимальная потребляемая мощность | 8,7 Вт |
| Температура эксплуатации | 0°C ~ +40°C |
| Тип антенны/Усиление антенны | Встроенная антенна/2,4 ГГц: 2 дБи, 5 ГГц: 3 дБи |
| Максимальное количество одновременных пользователей | ≤ 64 |
| Максимальная мощность передачи на радиопорт | 21 дБм |
| MIMO: пространственные потоки | 2 x 2:2 |
| Протоколы беспроводной связи | 802.11a/b/g/n |
| Максимальная скорость | 1,167 Мбит/с |

## **3.2.4 Рабочая станция** **N-Tech King Office S 59585**

Рабочие станции будут использоваться сотрудниками компании для доступа в Интернет и выполнения повседневных работ.

При выборе данной станции для работников организации бралось в расчет специфика работы компании – продажа компьютерного комплектующего. Никаких сложных вычислительных задач выполнять на таких машинах не требуется, к тому же при проектировании сети в качестве одного из требований указывается относительно небольшая стоимость оборудования, этим и обусловлен выбор данной рабочей станции. Она имеет следующие технические характеристики:

Таблица 3.3 – Основные характеристики N-Tech King Office S 59585

|  |  |
| --- | --- |
| Характеристика | Значение |
| Процессор | Intel Celeron J1800 2410 МГц |
| ОЗУ | 4 Гб |
| SSD | 120 Гб |
| Графический адаптер | Intel HD Graphics |
| Блок питания | 450 Вт |
| LAN | 1 Гигабит |

Работать данная станция будет под управлением операционной системы Windows 10 Enterprise. Данная ОС была выбрана из-за своей распространённости на рынке и простоты по сравнению с аналогами.

  
Рисунок 3.4 – N-Tech King Office S 59585 [9]

## 3.2.5 Многофункциональное устройство HP DeskJet 2630

При выборе копировального аппарата в качестве главного требования была невысокая цена при базовом функционале. Неплохим выбором в данной категории стал многофункциональный аппарат от компании HP – DeskJet 2630.

## **3.2.6 Принтер** **Canon PIXMA TS304**

Для принтера в требованиях при разработке локальной сети не стояло каких-либо особых требований к характеристикам. Поэтому был выбран простой бюджетный принтер от всемирно известного производителя подобного оборудования Canon. Некоторые характеристики принтера приведены ниже:

Таблица 3.5 – Характеристики Canon PIXMA TS304

|  |  |
| --- | --- |
| Формат | A4 (210x297 мм) |
| Технология печати | Струйный |
| Количество цветов | 4 |
| Скорость ч/б печати (А4) | 7.7 стр/мин |
| Скорость цветной печати (А4) | 4 стр/мин |
| Время печати 10x15см | 65 с |
| Ресурс картриджа | 180 стр  (черный, стандартный) |
| Операционная система | Windows 10, Windows 8.1, Windows 7 SP1, OS X 10.10.5 ~ OS X 10.11, macOS 10.12, iOS, Android, Windows 10 Mobile |
| Уровень шума при работе | 45 дБ(А) |
| Максимальное разрешение (dpi) | 4800 x 1200 |
| Интерфейсы | Wi-Fi(802.11b, 802.11g, 802.11n), USB, Bluetooth |

  
Рисунок 3.6 – Canon PIXMA TS304 [10]

## **3.3 Пассивное сетевое оборудование и кабеля**

Пассивным сетевым оборудованием называется сетевое оборудование, не питающееся от электрической сети, не преобразующее сигнал и выполняющее функции по его усилению.

Примерами такого оборудования можно представить различные кабели, информационные розетки, монтажные шкафы, монтажные стойки, телекоммуникационные шкафы, и многое другое.

В данной курсовой работе была использована неэкранированная витая пара категории 5e. Для нее характерны максимальная длинна в 100 метров, максимальная скорость до 1 Гбит/с, поддержка Power over Ethernet. Категория обусловлена тем, что всё оборудование использует Gigabit Ethernet.

Экранирование же применяется лишь в специализированных цехах, где велико электромагнитное излучение, либо электромагнитное излучение самой витой пары способно повлиять на работу каких-либо устройств. В компании, занимающейся продажей компьютерных комплектующих, как правило, нет сильных источников такого излучения или особо чувствительного оборудования, поэтому экранирование витой пары применяться не будет.

Других особых требований к пассивному оборудованию нет, так что после анализа имеющихся на рынке вариантов были выбраны витая пара Hyperline UUTP4-C5E-S24-IN-LSZH-GY, коннектор RJ-45 Cabeus 8P8C-SH-С7-TWP, и компьютерная информационная розетка Glossa GSL000181K RJ45, соответствующие стандарту 5e.

## **3.4 Схема адресации**

Адресация осуществляется по протоколу IPv4 и IPv6. Вся сеть компании разделена на две виртуальные подсети:

* VLAN 11 – сеть для посетителей
* VLAN 22 – сеть для сотрудников

Таблица 3.5 – Соответствие виртуальных подсетей и IP-адресов и масок

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN № | ip address | subnet mask | IPv6 address |
| 11 | 192.168.11.0 | 255.255.255.0 | 2001:0aa8:2239:0012::/64 |
| 22 | 192.168.22.0 | 255.255.255.0 | 2001:0aa8:2239:0013::/64 |

В таблице 3.5 указаны номер виртуальных сетей и соответствующие им адреса и маски.

По условию IPv6 адреса назначаются только для стационарных ПК, которые размещаются во всех рабочих помещениях. Поэтому имеет смысл прописать статические адреса на каждой рабочей станции. На подинтерфейсе роутера, соответствующего VLAN 22 прописываем IPv6 адрес:

int [Подинтерфейс, соответсвующий VLAN22]

ipv6 address 2001:0aa8:2239:0012::1/64

В таблице 3.7 указаны номера персональных компьютеров и соответствующие им IPv6 адреса и маски.

Таблица 3.7 - Соответствие номера ПК IPv6 адресам и маскам

|  |  |
| --- | --- |
| PC № | IPv6 address |
| 11 | 2001:0aa8:2239:0012::2/64 |
| 21 | 2001:0aa8:2239:0012::3/64 |
| 22 | 2001:0aa8:2239:0012::4/64 |
| 31 | 2001:0aa8:2239:0012::5/64 |
| 32 | 2001:0aa8:2239:0012::6/64 |
| 33 | 2001:0aa8:2239:0012::7/64 |
| 34 | 2001:0aa8:2239:0012::8/64 |
| 41 | 2001:0aa8:2239:0012::9/64 |
| 42 | 2001:0aa8:2239:0012::a/64 |
| 43 | 2001:0aa8:2239:0012::b/64 |
| 44 | 2001:0aa8:2239:0012::c/64 |
| 51 | 2001:0aa8:2239:0012::d/64 |

## **3.5 Настройка точки доступа**

Устанавливаются во всех рабочих помещениях. Так как для сотрудников и посетителей компании должен быть раздельный доступ к беспроводной сети. В режиме конфигурирования точки доступа зададим и настроим два SSID (Service Set Identifier – уникальный идентификатор беспроводной сети). Один как Guest, другой как Corporative. Для сети Corporative включим авторизацию с помощью алгоритма шифрования wpa, установим ключ сети KEY (в том виде, в котором он будет вводиться при авторизации в данной Wi-Fi сети). Для сети Guest авторизацию включать не нужно, так как подключаться к ней должен абсолютно любой посетитель компании.

Далее создаем две виртуальных сети VLAN 11 – для гостевого доступа и VLAN 22 для корпоративного, которые необходимо связать с соответствующими SSID: Guest и Corporative. После этого точка доступа готова к работе.

## **3.6 Настройка DHCP**

DHCP – это сетевой протокол, позволяющий компьютерам в сети получать ip и другие параметры для работы в сети автоматически. Это позволяет легко расширять существующие сети и не проделывать большое количество монотонной работы.

Всего для рассматриваемой сети понадобится два IPv4 DHCP пула для виртуальной подсети посетителей и для виртуальной подсети сотрудников. Для настройки DHCP требуется подключиться к роутеру и прописать в конфигурационном режиме на обоих подинтерфейсах, соответствующих виртуальным подсетям VLAN 11 и VLAN 22 следующие команды:

* Включите службу DHCP:

<HUAWEI> system-view

[HUAWEI] sysname Router

[Router] dhcp enable

* Добавьте подинтерфейс к VLAN 11:

[Router] vlan 11

[Router] vlan 22

[Router] interface gigabitethernet [subinterface для VLAN 11]

[Router –GigabitEthernet] port link-type hybrid

[Router –GigabitEthernet] port hybrid pvid vlan 11

[Router –GigabitEthernet] port hybrid untagged vlan 11

[Router -GigabitEthernet] quit

* Добавьте подинтерфейс к VLAN 22:

[Switch] interface gigabitethernet [subinterface для VLAN 22]

[Switch-GigabitEthernet] port link-type hybrid

[Switch-GigabitEthernet] port hybrid pvid vlan 22

[Switch-GigabitEthernet] port hybrid untagged vlan 22

[Switch-GigabitEthernet] quit VLANIF:

* Настроить IP-адрес для VLANIF 11:

[Switch] interface vlanif 11

[Switch-Vlanif11] ip address 192.168.11.1 24

[Switch-Vlanif11] quit

* Настроить IP-адрес для VLANIF 22:

[Switch] interface vlanif 22

[Switch-Vlanif22] ip address 192.168.22.1 24

[Switch-Vlanif22] quit

* Настроить IP-адреса и соответствующие сетевые параметры пула глобального адреса pool11:

[Switch] ip pool pool11

[Switch-ip-pool-pool11] network 192.168.11.0 mask 255.255.255.0

[Switch-ip-pool-pool11] gateway-list 192.168.11.1

[Switch-ip-pool-pool11] quit

* Настроить IP-адреса и соответствующие сетевые параметры пула глобального адреса pool22:

[Switch] ip pool pool22

[Switch-ip-pool-pool11] network 192.168.22.0 mask 255.255.255.0

[Switch-ip-pool-pool11] gateway-list 192.168.22.1

[Switch-ip-pool-pool11] quit

* Включить DHCP-сервер на VLANIF 11:

[Switch] interface vlanif 11

[Switch-Vlanif11] dhcp select global

[Switch-Vlanif11] quit

* Включить DHCP-сервер на VLANIF 22.

[Switch] interface vlanif 22

[Switch-Vlanif22] dhcp select global

[Switch-Vlanif22] quit

Это создаст два IPv4 DHCP пула для каждого из VLAN. Чтобы на рабочей станции происходило подключение по DHCP, надо отметить автоматическое получение IP в центре управления сетями.

## **3.7 Настройка коммутаторов**

На каждом из коммутаторов в созданной сети, необходимо зайти в конфигурационный режим посредством CLI и создать необходимые виртуальные подсети VLAN 11 и VLAN 22 с помощью следующих команд:

* Создание VLAN на коммутаторе Huawei:

[Huawei] System-view

[Huawei] vlan 11

[Huawei-vlan11] quit

[Huawei] vlan 22

[Huawei-vlan22] quit

* Настройка access-port режима на интерфейсах коммутатора, ведущих к пользовательским станциям:

[Huawei] interface GigabitEthernet {порт}

[Huawei-GigabitEthernet{порт}] port link-type access

[Huawei-GigabitEthernet{порт}] port default vlan {номер вилана}

[Huawei-GigabitEthernet{порт}] quit

* Для некоторых портов настроить работу в режиме trunk:

[Huawei-GigabitEthernet{порт}] port link-type trunk

* Добавляем номера VLAN в trunk через пробел

[Huawei-GigabitEthernet{порт}] port trunk allow-pass vlan {11 22}

## **3.8 Настройка NAT и запрет маршрутизации между VLAN**

Для настройки доступа в интернет для пользователей обоих подсетей, на маршрутизаторе необходимо настроить NAT. На роутере в CLI режиме system-view нужно прописать следующие команды:

[Huawei] acl 22

[Huawei-basic-22]  rule 100 permit source 192.168.22.0 0.0.0.255

[Huawei-basic-22]  quit

[Huawei] acl 11

[Huawei-basic-11]  rule 100 permit source 192.168.11.0 0.0.0.255

[Huawei-basic-11]  quit

[Huawei] interface Ethernet{Интерфейс, выходящий в интернет}

[Huawei- GigabitEthernet {Интерфейс}] nat outbound 22

[Huawei- GigabitEthernet {Интерфейс}] nat outbound 11

[Huawei- GigabitEthernet t{Интерфейс}] quit

Для запрета маршрутизации между VLAN и изоляции посетителей от внутренних ресурсов компании используем ACL:

[Huawei] acl 111

[Huawei-basic-111]  deny source 192.168.11.0 0.0.0.255 192.168.22.0 0.0.0.255

[Huawei-basic-111] permit source any any

[Huawei] acl 122

[Huawei-basic-122]  deny source 192.168.22.0 0.0.0.255 192.168.11.0 0.0.0.255

[Huawei-basic-122] permit source any any

[Huawei] int GigabitEthernet {порт.11}

[Huawei-GigabitEthernet{порт.11}] traffic-policy 111 inbound

[Huawei] int GigabitEthernet {порт.22}

[Huawei-GigabitEthernet{порт.22}] traffic-policy 122 inbound

# **4 ПРИНЦИПИАЛЬНОЕ ПРОЕКТИРОВАНИЕ**

## **4.1 Кабельная подсистема**

Витая пара проложена при помощи защитных коробов по коридорам помещения. Где возможно, кабель ведётся по плинтусу прямо к информационным розеткам, расположенным в непосредственной близости от оконечных устройств.

Результат проектирования плана компании по продаже компьютерного комплектующего представлен в приложении «В».

## **4.2 Организация рабочих мест**

В компании есть пять основных помещений, доступных сотрудникам. Кроме того, присутствует несколько коридорных помещений.

Все рабочие помещения оборудованы стационарными точками доступа (суммарно двенадцать): одна в кабинете директора, две в бухгалтерии, по четыре в каждом из залов с консультантами и одна точка на складе с товарами. Кроме того к одной из рабочих станций в бухгалтерии подключен принтер и многофункциональное устройство (ксерокс). Для беспроводного подключения, как посетителей, так и сотрудников, в каждом рабочем помещении находится беспроводная точка доступа с возможность как гостевого, так и корпоративного доступа.

Коридорные помещения не содержат никакого сетевого оборудования и лишь разграничивают доступ ко всем остальными помещения в компании.

Подключение сервера и рабочих станций осуществляется посредством выхода неэкранированных витых пар категории 5е с поддержкой Gigabit Ethernet через отверстия в стенах. Все кабели сходятся в защитный пятимиллиметровый пластиковый короб, берегущий их от внешнего воздействия. В конечном итоге он выходит за пределы кафедры и подключается к силовым сетям.

## 

## **4.3 Физическая защита сетевого оборудования**

В качестве одного из требования при разработке сети указано физическая защита сетевого оборудования. Данный тип защиты подразумевает защиту оборудования от нежелательного стороннего вмешательства и его повреждения. Это, как правило, обеспечивается путем установки оборудования в специально предназначенных для этого монтажных шкафах, стойках, телекоммуникационных шкафах (рис 4.1).

Для физической защиты сетевого оборудования все активное сетевое оборудование (роутер, коммутаторы) устанавливаются в настенных телекоммуникационных шкафах, специально предназначенных для размещения подобного оборудования, доступ к которому возможен только ограниченному кругу лиц, например сетевому администратору, так как шкафы запираются на ключ. Это позволяет защитить оборудование от внешних механических повреждений и несанкционированного доступа к нему.



Рисунок 4.1 – Настенный телекоммуникационный шкаф

Кроме этого прокладка кабеля в коридорах и местах, где наиболее вероятно повреждение кабеля, его прокладка осуществляется в коробе, что дает дополнительную защиту от внешних воздействий и повреждений.

Точки беспроводного доступа размещаются во всех основных рабочих помещениях здания, поэтому необходимо предусмотреть и их защиту от внешних физических воздействий. Для этого точки доступа размещаются под потолком в небольших корпусах, сделанных из пластика или дерева, так как металлические корпуса могут заметно ухудшать беспроводной сигнал.

# **ЗАКЛЮЧЕНИЕ**

В ходе выполнения курсовой работы была разработана локальная компьютерная сеть для компании, занимающейся продажей компьютерных комплектующих. Кроме того были получены и закреплены практически теоретические знания по проектированию локальных вычислительных сетей.

Были исследованы рекомендации производителей, имеющееся на рынке сетевое оборудование в разных ценовых сегментах, стандарты и требования к проектируемой сети.

В курсовой работе были разработаны структурная, функциональная схемы локальной вычислительной сети, план помещений компании, спецификация перечня материалов и оборудования, необходимых для построения и реализации сети, включая такое оборудование как: рабочие станции, маршрутизатор, коммутаторы, беспроводные точки доступа, принтер и многофункциональное устройство (копировальный аппарат). Выбранное оборудование соответствует основным стандартам качества, надёжности, и показывает себя на одних из лучших позициях в своем классе и ценовом сегменте, и используется при построении локальных компьютерных сетей во многих сферах деятельности.

Данная курсовая работа позволила значительно пополнить знания о вычислительных сетях, их разработке, структуре, прикладном использовании, выборе оборудования и еще раз подчеркнуть, что правильно разработанная локальная вычислительная сеть для компании или организации в современном мире во многом определяет, насколько успешно она будет выполнять свои функции и развиваться в дальнейшем.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

[1] Н. Г. Рожнова, Н. А. Искра, И. И. Глецевич «Вычислительные машины, Системы и Сети. Дипломное проектирование» - Минск БГУИР 2014 — [Электронный ресурс]. — Режим доступа:

https://www.bsuir.by/m/12\_100229\_1\_87625.pdf

[2] Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – 5-е издание – Санкт-Петербург [и другие] : Питер, Питер Пресс, 2017. – 955 с.

[3] CompBegin [электронный ресурс]. – Режим доступа: http://www.compbegin.ru/articles/view/\_100

[4] Чекмарёв Ю. В. Локальные вычислительные сети / Ю. В. Чекмарёв. – М.: ДМК-Пресс, 2014. – 250 с.

[5] Настройка VLAN, trunk и access на коммутаторах Huawei [электронный ресурс]. – Режим доступа: http://admin-gu.ru/device/huawei/nastrojka-vlan-rezhimy-trunk-hybrid-access-na-kommutatorakh-huawei-s2300-s5300

[6] Huawei S5720S-12TP [электронный ресурс]. – Режим доступа: https://e.huawei.com/kz/products/enterprise-networking/switches/campus-switches/s5720s-li-model

[7] EchoLife EG8240H [электронный ресурс]. – Режим доступа: https://e.huawei.com/kz/products/fixed-network/access/ont/echolife-eg8240h

[8] Huawei AP2010DN [электронный ресурс]. – Режим доступа: https://e.huawei.com/ru/products/enterprise-networking/wlan/indoor-access-points/ap2010dn

[9] N-Tech King Office S 59585 [электронный ресурс]. – Режим доступа: https://catalog.onliner.by/desktoppc/ntech/59585

[10] Canon PIXMA TS304 [электронный ресурс]. – Режим доступа: https://catalog.onliner.by/printers/canon/pixmats304

[11] HP DeskJet 2630 [электронный ресурс]. – Режим доступа: https://catalog.onliner.by/printers/hp/v1n03c

[12] Настройка DHCP-сервера [электронный ресурс]. – Режим доступа:

http://support.huawei.com/enterprise/ru/doc/EDOC1100027116?section=j04g

**ПРИЛОЖЕНИЕ А**

(обязательное)

Схема СКС структурная

# **ПРИЛОЖЕНИЕ Б**

(обязательное)

Схема СКС функциональная

# **ПРИЛОЖЕНИЕ В**

(обязательное)

План компании

# **ПРИЛОЖЕНИЕ Г**

(обязательное)

Перечень оборудования, изделий и материалов