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

Вариант №10

БГУИР КП 1-40 02 01 010 ПЗ

Студент: гр. 950501

Климбасов А. А.

Руководитель: старший преподаватель каф. ЭВМ

Глецевич И. И.

Минск 2022

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 5](#_Toc116461327)

[1 ОБЗОР ЛИТЕРАТУРЫ 6](#_Toc116461328)

[2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ 11](#_Toc116461329)

[ПРИЛОЖЕНИЕ А 13](#_Toc116461330)

[ПРИЛОЖЕНИЕ М 14](#_Toc116461331)

# ВВЕДЕНИЕ

В качестве курсовой работы необходимо создать локальную компьютерную сеть организации, занимающаяся торговлей бытовой химией, обладающей лицензией и на продажу агрессивных моющих средств, то есть предоставить соответствующую документацию. Инфраструктура объекта должна быть приближена к реальности. Проектируемая сеть должна включать как проводную, так и беспроводную составляющие, с возможностью выхода в Internet.

Локальные компьютерные сети используются повсеместно: на заводах и предприятиях, в школах, научных лабораториях, в игровых студиях. Список можно продолжать долго. Именно благодаря сетям наш мир способен бесперебойно работать. Использование локальной сети позволяет создать надлежащие условия для быстрой передачи информации, будь то текстовые сообщения, изображения, аудио или видеофайлы и так далее.

Построение локальной сети является на сегодняшний день наилучшим способом создания на предприятии единой информационной среды, обусловленного современными требованиями быстрого обмена информацией между пользователями, совместного использования различных ресурсов и т. д. Сегодня эффективность построения локальной сети предприятия не вызывает сомнения, поскольку обеспечивает пользователей непрерывным доступом к корпоративным ресурсам: файлам, хранилищам данных, совместным пользованием дорогостоящей оргтехникой (принтеры, сканеры, факсы), быстрым и простым перемещением и добавлением новых рабочих мест и оборудования, обеспечением дополнительной безопасности корпоративных данных особой секретности и другими.

# 1 ОБЗОР ЛИТЕРАТУРЫ

**1.1.** **Подключение сети организации к Internet**

По заданию доступ к сети Internet осуществляется через оптоволокно. В качестве оптоволоконного кабеля для шнура используется zip-cord. Также указан тип оптического разъёма и полировки: LC и UPC соответственно.

Оптический коннектор LC — это малогабаритный вариант SC коннектора. Он имеет прямоугольное сечение корпуса. Конструкция исполняется на пластмассовой основе и снабжена защелкой, подобной защелке, применяющейся в модульных коннекторах медных кабельных систем. Вследствие этого и подключение коннектора производится схожим образом.

UPC ­ это сокращение от Ultra Physicalt, который является улучшением PC оптического разъема с Контактом. UPC имеет лучше отделку поверхности после продолжительной полировки и возвратных потерь, чем PC структура, почти -50 дБ или выше. Хотя он имеет относительно низкое обратное отражение по сравнению с PC разъемом, он недостаточно прочно.

Наконечник изготавливается из керамики и имеет диаметр 1,25 мм. Применяется так же дуплексный вариант LC коннектора — два коннектора объединяются полимерным зажимом.

Исходя из приведенного выше, ввиду большей простоты прокладки сетевой инфраструктуры коммуникацию сетевого оборудования внутри офиса организации выгодно организовывать через витую пару. Следовательно, требуется некоторая аппаратура для преобразования оптического сигала в электрический для коммуникации между оптоволокном и витой парой. В данном случае можно воспользоваться, например, медиаконвертером или gpon-модемом.

**1.2. Требования безопасности**

В задании в качестве требования к безопасности проектируемой сети указано использования технологий VPN и протоколов шифрования SSL и TLS для обеспечения безопасного удалённого подключения пользователей к сети организации.

VPN — это совокупность технологий, позволяющая организовать защищённую виртуальную сеть, объединяющую доверенные сети и узлы, поверх открытой сети с низким уровнем доверия путём использования криптографических способов защиты данных.

VPN создает «туннель», по которому вы можете безопасно отправлять данные, используя инструменты шифрования и аутентификации. Предприятия часто используют VPN-подключения для обеспечения сотрудникам удаленного доступа к частным корпоративным сетям, даже если они работают вне офиса.

VPN позволяет удаленным устройствам, таким как ноутбуки, работать так, как будто они находятся в одной локальной сети. Многие маршрутизаторы VPN могут одновременно поддерживать десятки туннелей с помощью простых инструментов настройки, обеспечивая всем сотрудникам доступ к данным компании, где бы они ни находились.

SSL и TSL — криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет. TLS и SSL используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

SSL — Secure Socket Layer, уровень защищенных сокетов. TLS — Transport Layer Security, безопасность транспортного уровня. SSL является более ранней системой, TLS появился позднее и он основан на спецификации SSL 3.0, разработанной компанией Netscape Communications. Тем не менее, задача у этих протоколов одна — обеспечение защищенной передачи данных между двумя компьютерами в сети Интернет.

Безопасная передача обеспечивается при помощи аутентификации и шифрования передаваемой информации. TLS является преемником SSL, хотя они и могут использоваться одновременно, причем даже на одном и том же сервере. Такая поддержка необходима для того, чтобы обеспечить работу как с новыми клиентами (устройствами и браузерами), так и с устаревшими, которые TLS не поддерживают. Принцип работы SSL и TLS: поверх протокола TCP/IP устанавливается зашифрованный канал, внутри которого передаются данные по прикладному протоколу, например HTTP, FTP. Пакеты прикладного протокола шифруются TLS/SSL, далее уже зашифрованный пакет инкапсулируется в TCP/IP. Также TSL/SSL являются частью протокола HTTPS.

Принцип работы SSL состоит из двух фаз: фаза рукопожатия и фаза передачи данных. Во время фазы рукопожатия клиент и сервер используют шифрование открытым ключом для того, чтобы определить параметры секретного ключа, используемого клиентом и сервером для шифрования во время фазы передачи данных.

Клиент инициирует рукопожатие посылая «hello»-сообщение серверу. Такое сообщение содержит список алгоритмов симметричного шифрования, поддерживаемых клиентом. Сервер отвечает похожим «hello»-сообщением, выбрав при этом наиболее подходящий алгоритм шифрования из полученного списка. Далее сервер отправляет сертификат, который содержит его публичный ключ.

Сертификат — это набор данных, который подтверждает подлинность. Подтвержденная третья сторона, известная как центр сертификации (CA), генерирует сертификат и проверяет его подлинность. Чтобы получить сертификат, сервер должен использовать безопасные каналы для отправки своего публичного ключа в центр сертификации. Он генерирует сертификат, который содержит его собственный ID, ID сервера, публичный ключ сервера и другую информацию. А также центр сертификации создает отпечаток (digest) сертификата, который, по сути, является контрольной суммой. Далее центр сертификации создает подпись сертификата (certificate signature), которая формируется путем шифрования отпечатка сертификата приватным ключом центра сертификации.

Для проверки сертификата сервера клиент использует публичный ключ центра сертификации для расшифровки подписи. Затем клиент самостоятельно считает отпечаток сертификата сервера и сверяет с расшифрованным. Если они не совпадают, то сертификат был подделан. Естественно, для расшифровки подписи у клиента должен быть публичный ключ центра авторизации. Поэтому клиент хранит у себя список публичных ключей подтвержденных центров сертификации. Когда клиент установил подлинность сервера, сервер использует шифрование открытым ключом для определения секретного ключа для обмена информацией.

Фаза рукопожатия завершается отправкой «finished»-сообщений, как только обе стороны готовы начать использование секретного ключа. Начинается фаза передачи данных, в ходе которой каждая сторона разбивает исходящие сообщения на фрагменты и прикрепляет к ним коды авторизации сообщений MAC (message authentication code). Код авторизации сообщения это зашифрованный отпечаток, вычисленный на основе содержимого сообщений. Для получения полноценного SSL пакета каждая из сторон объединяет данные фрагмента, код авторизации сообщения, заголовки сообщения и шифруют с использованием секретного ключа. При получении пакета, каждая из сторон расшифровывает его и сверяет полученный код авторизации сообщения со своим. Если они не совпадают, то пакет был подделан.

**1.3. Прочие оконечное оборудование**

В задании указанно наличие принтеров и цветных принтеров в качестве прочего оконечного оборудования разрабатываемой сети.

В зависимости от возможностей принтера его подключение к локальной сети может происходить по-разному. Существуют принтеры со встроенным Wi-Fi адаптером, осуществляющим беспроводное подключение к сети. Также принтеры со встроенным Ethernet интерфейсами, для проводного подключения. Данные типы принтеров не требуют дополнительного сетевого оборудования для подключения их к сети. Самый распространённый и дешёвый вариант — принтер с USB портом, не адаптированный ни аппаратно, ни программно для подключения его в КС. Такого рода устройства требуют устройства-адаптера для подключения к сети.

# 2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе будет рассмотрена структура локальной сети.

Данный раздел сопровождает чертеж схемы СКС структурной (приложение «А»).

Для уточнения структуры подсети требуется рассмотреть структуру помещений офиса. По заданию офис находится на площади цокольного этажа здания, обладает квадратной площадью в 110 квадратных метров. Помещение обладает высокой влагозащитой и защитой о погодных условиях. В помещении поддерживается комнатная температура. Офис состоит из комнат, каждая из которых закреплена за определённым отделом. Всего в офисе есть 9 комнат, где будет использоваться конечные устройства для подключения к сети:

* склад;
* отдел закупок;
* бухгалтерия;
* отдел сбыта;
* комната руководителя предприятия;
* отдел кадров;
* отдел снабжения.

Также есть отдельное выделенное помещение для размещения сетевого оборудования.

Исходя из вышесказанного, не требуется осуществлять дополнительных мер защиты физической инфраструктуры прокладываемой сети от высоких перепадов температуры и влажности.

# Подключение к корпоративной локальной сети к Internet осуществляется через маршрутизатор. К маршрутизатору будет подключен корневой коммутатор, к которому в свою очередь подключены коммутаторы для обеспечения достаточного количества стационарных подключений. Также 2 коммутатора будут использованы для подключения к web-серверам для повышения надёжности сегмента сети. К ряду коммутаторов будут подключены точки беспроводного доступа для обеспечения требуемого количества мобильных подключений.3 ФУНКЦИОНОЛЬНОЕ ПРОЕКТРИРОВАНИЕ

**3.1 Расчёт покрытия помещений беспроводной сетью**

В соответствии с заданием требуется развернуть беспроводную сеть для обеспечения 20 мобильных подключений в помещениях организации. Для большинства современных точек доступа Cisco такое количество подключений может обслуживаться одним устройством. В помещениях организации отсутствуют ранее установленные WLAN. По периметру этажа помещения имеют железобетонные стены, обеспечивающие хорошую изоляцию от внешнего электромагнитного фона. Как следствие, влияние расположенных поблизости WLAN можно не рассматривать.

Так, как стены между помещениями организации преимущественно являются стенами из гипсокартона и силикатобетона, имеет смысл рассмотреть возможность размещения точек доступа, покрывающих более 1 помещения. Для этого требуется теоретически рассчитать места расположения точек для покрытия всех помещений организации с учётом влияния конструкционных элементов здания.

Для расчёта затухания радиоволн в беспрепятственной воздушной среде используется упрощённая формула:

F – частота сигнала в GHz, D – расстояние в метрах от точки доступа. Чувствительность устройств обычно находится в пределах от -65 до -75 dB.

Так как форма здания квадратная, предположим размещение точки в центре на потолке. Высота потолка – 2,5 м. Рассчитаем затухание у наиболее удалённых точек помещений.

Расстояние до самых удалённых точек помещений (углов этажа):

Пусть частота точки будет 5 GHz как наиболее быстро затухающая, тогда затухание на таких точках:

Рассчитанное затухание сигнала удовлетворительно с учётом мощности излучения точки доступа 20 дБ. Тогда стоит рассмотреть затухание на конструкционных элементах здания. Наиболее серьёзное препятствие для распространения сигнала представляется в виде трёх стен из гипсокартона. Суммарно, такое препятствие даёт затухание .

Также стоит учесть возможное затухание за счёт взаимного размещения оборудования .

Тогда максимальное затухание сигнала в помещениях организации составляет:

Тогда минимальная мощность сигнала в помещении будет равна:

Такой показатель сигнала является удовлетворительным, что позволяет воспользоваться одной точкой доступа с мощностью излучения не менее 20 дБ для покрытия всех помещений WLAN.

**3.2 Выбор оборудования**

**3.2.1 Принтер**

В задании оговорено наличие принтеров и цветных принтеров в качестве прочего оконечного оборудования. В данном случае стоит выбор между принтерами, подключающимися к другому оконечному оборудованию, выступающему в роли принт-сервера, принтера со встроенной сетевой картой для подключения к сети через витую пару, беспроводным принтером и принтером со встроенным программным обеспечением, не требующего подключения управляющего оборудования.

Принтеры без встроенной сетевой карты не будут иметь возможность функционировать без принт-сервера. В качестве принт-сервера может использоваться как рабочая станция или отдельное одноимённое сетевое устройство. Использование рабочей станции не удобно в контексте организации, так как отдельная станция используется работниками организации также как основное рабочее устройство и, как следствие, подвержено различного рода уязвимостям в случае некорректного использования, что повлечёт и прекращение работы принтера. Использование принт-сервера куда более надёжно, однако его использование требует источника питания, что приводит либо к увеличению количества требуемых PoE портов коммутатора, либо к большему количеству требуемых силовых розеток. В случае сетевого принтера, подключаемого витой парой, вышеперечисленных проблем не возникает, однако это требует прокладки дополнительных кабелей для подключения. Беспроводной вариант требует наличия WLAN в месте работы принтера и его функционирование будет зависеть от функционирования точек доступа. Также усложняется построение виртуальной сети для беспроводных устройств. Принтеры со встроенным по наиболее удобны, так как на их работоспособность не влияют ни состояние управляющей машины, ни локальной сети в целом. Для такого рода принтеры требуется только подключение к питанию для функционирования. Недостатком такого рода устройств является их стоимость.

Ввиду достаточного бюджета и простоты использования организацией был выбран вариант принтера со встроенным программным обеспечением.

Выбранная модель – Epson WorkForce WF-7015 в качестве цветного принтера и Epson WorkForce Pro WF-M5299 в качестве чёрно-белого.

**3.2.2 Маршрутизатор**

Для выбора маршрутизатора необходимо определится с требуемой скоростью интернет-соединения, так как требования не оговаривают эту характеристику. Так как по заданию в сети присутствует web-сервер для внутреннего и внешнего использования. Для нормального функционирования корпоративной сети выбрана технология 10Gb. Подключение к оптоволокну осуществляется через медиа конвертер, для которого требуется sfp порт для поддержки стандарта 1000base-t. Также требуется поддержка TCL-VPN.

Поскольку аппаратные решения Cisco IOS SSL VPN на момент выполнения работы устарели, для обеспечения SSL VPN потребуется приобретение и установка лицензии. По этой причине критерий поддержки SSL VPN снимается выбираемого роутера. Тогда требуется только поддержка IPSec протокола.

Ввиду малого количества конечных устройств и малой нагрузки при interVLAN маршрутизации для организации виртуальных локальных сетей используется Router-on-Stick. Тогда к маршрутизатору требуется подключить и web-сервер для внешнего пользования.

В качестве маршрутизатора был выбран A901-12C-FT-D.

**3.2.3 Коммутатор**

От коммутаторов требуется обеспечивать 15 подключений, одно из которых должно поддерживать PoE+ для питания точки доступа. Также стоит учесть надобность в резервировании портов для дальнейшего расширения сети организации. Предполагается резервирование портов в размере равном требующимся на момент проектирования сети. В данном случае был выбран коммутатор CBS220-48P-4X ввиду наличия требуемого количества портов с учётом резервирования и поддержкой PoE+.

**3.3.3 Точка доступа**

Для снижения нагрузки на коммутатор и отказа от покупки контроллера точек доступа решено использовать точки доступа со встроенным контроллером. Это также объясняется малым количеством точек доступа, требуемого для развёртывания WLAN организации. Требование к точке доступа, исходя из расчета затухания сигнала в пункте 3.1. – это мощность излучения более 20 дБ. Также из соображений безопасности требуется обеспечить аутентификацию мобильных пользователей.

Имеет смысл рассматривать точки доступа из серий, рекомендованных Cisco для развёртывания BSS для малого бизнеса. Из наиболее распространённых решено рассмотреть серии Cisco Catalyst 9115 и Cisco Aironet 1815m. С учётом вышеописанных требований из данных семейств подходят по требованиям модели C9115AXI-EWC-I и AIR-AP1815m-I-K9.

В таблице приведён анализ требуемых характеристик вышеуказанных точек доступа. В данном случае ля модели C9115AXI-EWC-I не специфицировано максимальное количество подключений, поэтому в качестве точки доступа выбрана модель AIR-AP1815m-I-K9.

Таблица 3.Х – сравнение характеристик рассматриваемых точек доступа.

|  |  |  |
| --- | --- | --- |
| Наименование | C9115AXI-EWC-I | AIR-AP1815m-I-K9 |
| Мощность, W | 20.4 | 13.9 |
| Максимальная мощность передачи 2.4 GHz, дБм | 23 | 27 |
| Максимальное количество подключений | Не указана в спецификации | 200 |
| Протокол безопасности | 802.11i, Wi-Fi Protected Access 3 (WPA3), WPA2, WPA | 802.11i, WPA3, WPA2, WPA |

**3.3.4 Медиаконвертер**

Для подключения маршрутизатора к сети Интернет 10Gb через оптоволокно требуется конвертация оптического сигнала в электрический. Этого можно достичь использованием либо внешнего 10GPON модема, либо маршрутизатора со встроенным 10GPON модемом, либо медиаконвертером с подключением в SFP+. В отличие от PON модемов, медиаконвертеры представлены в более широком ассортименте. Найти требующийся медиаконвертер с учётом типа коннектора оптоволокна легче. Медиаконвертер соединяется с сетевым устройством при помощи SFP порта, что делает медиаконвертер более универсальным решением, отвязывая сетевое оборудования от типа присоединяемого коннектора.

Выбор остановился на использовании медиаконвертера ввиду большей гибкости при выборе маршрутизатора. Была выбрана модель SFP-10G-T-X. Выбор данной модели обусловлен соответствием требованием подключаемой внешний среды передачи данных.

**3.3.5 Web-сервер**

В соответствии с заданием в локальной сети требуется присутствие web-сервера для внутреннего и внешнего использования. Из соображений оптимизации доступа к ресурсу сервера предполагается использование сервера с двум сетевыми картами, одна из которых будет нацелена на использование со стороны внутренней подсети, другая – со стороны внешней.

в

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

[1] А.Т. Доманов, Н.И. Сорока/ Предварительный стандарт предприятия. Дипломные проекты(работы). Общие требования. СТП П–01–2008. Минск БГУИР, 2010.

[2] И.И. Глецевич, В.А. Прытков, А.В. Отвагин, Методические указания по дипломному проектированию для студентов специальности 40 02 01 «Вычислительные машины, системы и сети» всех форм обучения. – Минск, 2009.

# ПРИЛОЖЕНИЕ А

*(обязательное)*

**Схема структурная**

# ПРИЛОЖЕНИЕ М

*(обязательное)*

**Ведомость документов**