Учреждение образования

«Белорусский Государственный Университет Информатики и Радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовой работе

«Локальная компьютерная сеть, вариант 2»

по дисциплине

«Аппаратное обеспечение компьютерных сетей»

БГУИР КР 1-40 02 01 01 002 ПЗ

Выполнил: Руководитель:

студент группы 550501 Глецевич И. И.

Дмитриев А.С.

Минск 2019

СОДЕРЖАНИЕ

[1 ОБЗОР ИСТОЧНИКОВ 5](#_Toc534856694)

[2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ 8](#_Toc534856695)

[1.1 Административная подсеть 9](#_Toc534856696)

[1.2 Директорская подсеть 10](#_Toc534856697)

[1.3 Печатная подсеть 10](#_Toc534856698)

[1.4 Подсеть отдела IT 10](#_Toc534856699)

[1.5 Подсеть отдела тестирования 10](#_Toc534856700)

[1.1 Гостевая подсеть 10](#_Toc534856701)

[3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ 11](#_Toc534856702)

[3.1 Обоснование выбора сетевой операционной системы 11](#_Toc534856703)

[3.2 Администрирование и серверная часть сети 12](#_Toc534856704)

[**3.2.1** **Выбор оборудования** 12](#_Toc534856705)

[**3.2.2** **Настройка web-сервера** 13](#_Toc534856706)

[3.3 Организация рабочих мест и гостевая часть сети 14](#_Toc534856707)

[3.4 Обоснование выбора среды передачи данных 15](#_Toc534856708)

[3.5 Обоснование выбора активного сетевого оборудования 15](#_Toc534856709)

[**3.5.1** **Настройка DHCP** 16](#_Toc534856710)

[**3.5.2** **NAT** 17](#_Toc534856711)

[1.5 Информационная безопасность локальной компьютерной сети 18](#_Toc534856712)

[1.6 Адресация в локальной компьютерной сети 21](#_Toc534856713)

[4 КАБЕЛЬНАЯ СТРУКТУРА СКС 22](#_Toc534856714)

[ЗАКЛЮЧЕНИЕ 23](#_Toc534856715)

[ПРИЛОЖЕНИЕ А 24](#_Toc534856716)

[ПРИЛОЖЕНИЕ Б 25](#_Toc534856717)

[ПРИЛОЖЕНИЕ В 26](#_Toc534856718)

[ПРИЛОЖЕНИЕ Г 27](#_Toc534856719)

[ПРИЛОЖЕНИЕ Д 28](#_Toc534856720)

[ПРИЛОЖЕНИЕ Е 29](#_Toc534856721)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 30](#_Toc534856722)

ВВЕДЕНИЕ

Сейчас невозможно представить наш мир без наполнения в виде различных компьютерных сетей. Появление сетей и их дальнейшее развитие ускорило многие технологические и научные процессы. Объединив персональные устройства в сложные системы, человечество получило следующий перечень преимуществ:

1. *Распределение ресурсов -* дало возможность рационально задействовать вычислительные мощности, разделив сложные задачи на множество простых, выполняемых одновременно множеством оконечных устройств.
2. *Разделение данных -* предоставило возможность передавать данные между оконечными устройствами, а также хранить и управлять различными данными на любом или из любого оконечного устройства сети, имеющего такие привилегии.
3. *Совместное использование программных средств -* позволило нескольким пользователям одновременно использовать уже установленное на одном из оконечных устройств программное обеспечение.
4. *Удалённое администрирование -* дало доступ оконечным устройствам на управление другими устройствами их сети, при наличии таких привилегий.

В данном курсовом проекте присутствуют разделение данных и удалённое администрированние. Первое обеспечиается сервером компании, а второе отдельно выделенной административной подсетью, дающей возможность системному администратору настраивать различные узлы сети: сервер, L3 коммутатор и беспроводные точки доступа.

По территориальному критерию сети делятся на локальные, региональные и глобальные.

Локальные – это небольшие сети, часто являющиеся внутренними сетями небольших компаний или предприятий, располагающихся на единой территории.

Региональные – это более крупные сети, обычно занимающие территорию города или области.

Глобальные – это крупнейшие сети, обычно располагающиеся на территории одного или нескольких государств, например всемирная сеть Интернет.

В данном курсовом проекте разрабатывается локальная сеть для небольшой компании, занимающей разработкой Java– приложений.

Обычно различными компаниями используются два типа сетей: LAN и WAN.

LAN (Local Area Network) – это локальная сеть с замкнутой инфраструктурой, которая уже затем подключается к каналу поставщика услуг. Это может быть как маленькая офисную сеть, так и сеть крупного предприятия, располагающегося на обширной площади.

WAN (Wide Area Network) – это глобальная сеть, часто включающая в себя несколько локальных сетей, а также иногда и телекоммуникационные сети. Включённые в WAN сети могут иметь различные технические, программные и информационные подходы при решении определённых задач. WAN используются крупными корпорациями и связывают офисы и предприятия из различной степени удалённости точек земного шара. Локальные сети чаще всего являются сетями закрытого типа, и доступны они только определённому кругу пользователей. Глобальные сети также могут быть закрытыми, особенно если это сеть некой корпорации, однако ничего не мешает им быть и открытыми с ориентацией на обслуживание любых пользователей.

В данной же курсовой работе необходимо разработать архитектуру локальной вычислительной сети для небольшой компании, занимающейся разработкой Java-приложений и базирующейся в двухэтажном здании. Потому для решения данной задачи была использована LAN. Список необходимых к созданию чертежей включает в себя структурную и функциональную схемы проектируемой локальной вычислительной сети, а также планы этажей, перечень компонентов и схему адресации.

Все предоставленные по итогу документы позволят реализовать на практике требуемую по условию сеть.

# ОБЗОР ИСТОЧНИКОВ

Для написания данной курсовой работы сначала было изучено различие LAN и WAN сетей.

LAN (Local Area Network) – локальная сеть.

WAN (Wide Area Network) – глобальная сеть.

В основном, локальные сети отличаются от глобальных по следующим признакам:

1. Размер сети. Локальная сеть, как правило включает в себя либо одно здание, либо территорию кампуса – комплекса расположенных рядом зданий. Глобальная сеть может распределяться на гораздо большие расстояния, например, VPN-линк между удалёнными офисами в разных городах – это глобальная сеть.
2. Количество подключенных пользователей. К локальной сети, как правило, подключено большое количество пользователей. Каждый компьютер в офисе – это узел локальной сети. В то же время, WAN обычно имеет меньшее количество узлов: например, в предыдущем примере с удалённым офисом, у нас будет всего два узла: маршрутизатор основного офиса и маршрутизатор удалённого офиса.
3. Типом сервисов, доступных на узлах сети. Например, на узлах локальной сети обычно используются службы доступа к файлам и принтерам (SMB) в то же время, на узлах глобальной сети – маршрутизаторах и службы соответствующие: VPN, маршрутизация и так далее.[5]

Затем были изучены различные топологии сетей.

1. Полносвязная - Сеть, в которой каждый компьютер непосредственно связан со всеми остальными. Однако этот вариант громоздкий и неэффективный, потому что каждый компьютер в сети должен иметь большое количество коммуникационных портов, достаточное для связи с каждым из остальных компьютеров.
2. Неполносвязанная - Неполносвязных топологий существует несколько. В них, в отличие от полносвязных, может применяться передача данных не напрямую между компьютерами, а через дополнительные узлы.
3. Шина - Топология данного типа представляет собой общий кабель (называемый шина или магистраль), к которому подсоединены все рабочие станции. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала.
4. Звезда - В сети, построенной по топологии типа «звезда», каждая рабочая станция подсоединяется кабелем (витой парой) к концентратору, или хабу ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *hub*). Концентратор обеспечивает параллельное соединение ПК и, таким образом, все компьютеры, подключенные к сети, могут общаться друг с другом.
5. Кольцо - В сети с топологией типа «кольцо» все узлы соединены каналами связи в неразрывное кольцо (не обязательно окружность), по которому передаются данные. Выход одного ПК соединяется со входом другого ПК. Начав движение из одной точки, данные, в конечном счете, попадают на его начало. Данные в кольце всегда движутся в одном и том же направлении.
6. Ячеистая - Получается из полносвязной топологии путём удаления некоторых связей. Допускает соединения большого количества компьютеров и характерна для крупных сетей.[6]

Далее было изучено различное сетевое оборудование из перечня, предлагаемого Cisco, и по документации выбран сервер, соответствующий необходимым требованиям к производительности и ценовой категории. После этого было изучено активное оборудование сети, опять же по документации Cisco, и выбран L3-коммутатор как центр топологии. Для него необходимо было настроить DHCP и NAT

DHCP - это протокол динамической настройки узла. DHCP предназначен для настройки хоста через удаленный сервер. DCHP поддерживается по умолчанию большинством современных операционных систем, и этот протокол выступает в качестве отличной альтернативы рутинной ручной настройке параметров сети для сервера или подключаемого устройства.[7]

NAT (Network Address Translation) - это такой механизм, который позволяет роутеру определять какие сервисы находятся за роутером и должны быть доступны из интернета, чтобы пользователи оттуда могли этими сервисами пользоваться. NAT присутствует во всех роутерах и серверных операционных системах в том или ином виде. В роутерах это обычно называется port forwarding, в linux - iptables, а на windows server  - в специальной оснастке.[8]

Следующим шагом был подбор клиентского оборудования. Были выбраны комплектующие оконечных устройств. Для персональных компьютеров были подобраны системные блоки с необходимыми сетевыми картами, мониторы, клавиатуры, мыши, веб-камеры. Также в соответствии с требованиями в топологию были помещены чёрно-белый и цветной принтеры.

Изучив различные категории кабелей и пересмотрев топологию было выявлено, что лучше использовать витую пару RJ-45 прямого типа категории 6 c FTP типом защиты.

CAT6 (полоса частот 250 МГц) — применяется в сетях Fast Ethernet и Gigabit Ethernet, состоит из 4 пар проводников и способен передавать данные на скорости до 1000 Мбит/с. Добавлен в стандарт в июне 2002 года. Существует категория CAT6a, в которой увеличена частота пропускаемого сигнала до 500 МГц. По данным IEEE, 70% сетей, установленных в 2004 году, использовали кабель категории CAT6.

Фольгированная витая пара (FTP — Foiled twisted pair) — также известная как S/UTP, имеет один общий внешний экран.[9]

Также необходим был волоконно-оптический кабель и GPON модем, подключаемый к L3-коммутатору для выхода в глобальную сеть Интернет.

Волоконно-оптический кабель — кабель на основе [волоконных световодов](https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5_%D0%B2%D0%BE%D0%BB%D0%BE%D0%BA%D0%BD%D0%BE), предназначенный для передачи оптических сигналов в [линиях связи](https://ru.wikipedia.org/wiki/%D0%92%D0%BE%D0%BB%D0%BE%D0%BA%D0%BE%D0%BD%D0%BD%D0%BE-%D0%BE%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BB%D0%B8%D0%BD%D0%B8%D1%8F_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8), в виде [фотонов](https://ru.wikipedia.org/wiki/%D0%A4%D0%BE%D1%82%D0%BE%D0%BD) , со скоростью меньшей [скорости света](https://ru.wikipedia.org/wiki/%D0%A1%D0%BA%D0%BE%D1%80%D0%BE%D1%81%D1%82%D1%8C_%D1%81%D0%B2%D0%B5%D1%82%D0%B0) из-за непрямолинейности движения.[10]

Также в топологию был добавлен ПК системного администратора, который получил возможность подключения к L3-коммутатору с помощью консольного кабеля.

Консольный кабель — это разновидность [нуль-модемного](https://ru.wikipedia.org/wiki/%D0%9D%D1%83%D0%BB%D1%8C-%D0%BC%D0%BE%D0%B4%D0%B5%D0%BC%D0%BD%D0%BE%D0%B5_%D1%81%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5) кабеля. Как правило, этот кабель плоский, имеет голубой цвет и разъем RJ45. Один конец этого кабеля обжат по обратной схеме относительно другого. Подключение через данный провод необходимо для удаленного управления активными устройствами сети.[11]

Для сохранения коммерческой тайны, сеть была разделена при помощи VLAN-ов.

VLAN (*Virtual Local Area Network*) — виртуальная [локальная компьютерная сеть](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), представляющая из себя группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к [широковещательному домену](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%80%D0%BE%D0%BA%D0%BE%D0%B2%D0%B5%D1%89%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D0%BC%D0%B5%D0%BD), независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным членам группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе [программного обеспечения](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) вместо физического перемещения устройств.[12]

Также для безопасности был добавлен AAA.

AAA – механизм, который позволяет осуществлять аутентификацию, авторизацию и учет пользователей, то есть контролировать доступ и записывать производимые действия. Принцип ААА можно описать так: для совершения какого-либо действия в сети мы должны проследить, кто инициирует это действие (authentication), имеет ли он право на выполнение этого действия (authorization) и что в журнал записаны все действия, которые он совершил (аccounting).[13]

# СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе описывается и проводится обоснование выбора структуры организации локальной вычислительной сети для двух этажей офиса компании, занимающейся разработкой Java-приложений.

Изучив поставленную задачу, мною было принято решение, что для данной локальной сети наиболее подходящая топология – это звезда. Данное решение было принято по следующим соображениям.

Во-первых, в данной сети может максимально находиться 41 оконечное устройство, что может быть вполне выдержано L3-коммутатором на 48 разъёмов.

Во-вторых, данная топология позволяет довольно быстро отслеживать ошибки и обрывы линии, ибо большинство оконечных устройств подключено к центральному узлу напрямую.

В-третьих, использование такой топологии снижает стоимость сети, ибо уменьшает число узлов в ней, а, следовательно, и дополнительного оборудования, ведь не стоит забывать, что каждое добавленное устройство требует и отдельного кабеля, и отдельного его же монтажа.

Для удобства работы с VLAN-ами, беспроводные устройства были разграничены четырьмя беспроводными точками доступа, группирующими устройства по отношению к определённым VLAN-ам. Остальные же устройства остались подключёнными напрямую. По итогу мы получили звезду, в которой четыре подключённых устройства образуют ещё 4 звезды.

Изучив требования к помещениям, а также их площади и то, что здание двухэтажное, я пришёл к следующим выводам:

1. Кабинет директора, комнату для собеседований, серверную и служебное помещение стоит разместить на первом этаже. Это позволит директору иметь быстрый доступ к комнате для собеседований, а также следить, кто посещает и покидает здание. Также это позволит быстро связаться с системным администратором в случае чрезвычайной ситуации, для отключения или перезагрузки системы.
2. Служебное помещение будет использоваться как раздевалка и место под принтер, чтобы работники не несли на второй этаж грязь, способную повредить оборудованию.
3. Комнаты для отдела IT и отдела тестов стоит расположить на втором этаже, чтобы случайный посетитель или запланированный гость не увидели ничего лишнего и не отвлекали работников.
4. Так как площадь здания небольшая, то беспроводных точек доступа хватит четырёх, по две на каждый этаж, по одной на половину этажа по бокам от коридора. Стены всего 10см, а максимальная ширина комнат 5 метров, потому их мощности должно быть достаточно.

Сервер и L3-коммутатор были помещены в одну стойку в серверной, чтобы центральные компоненты системы были под постоянным присмотром системного администратора. В серверную же и был подведён оптический канал от поставщика сетевых услуг.

Как было сказано выше, чёрно-белый принтер был размещён в служебной комнате, но вот цветной в кабинете директора, чтобы ужесточить контроль за расходованием ресурсов и сохранением конфиденциальности разработок.

При прокладке сети использовались кабели шестой категории, про которые будет написано далее. Были выбраны именно они по той причине, что L3-коммутатор, являющийся центром данной топологии, поддерживает разъёмы 10/100/1000. Он также будет описан далее.

При монтаже использовалась модель короба, также описанная в последующем разделе. Кабели прокладывались связками внутри короба вдоль низа и верха стен с переходами от пола к потолку по кабельному каналу при необходимости.

В данной топологии было достаточно прямых кабелей, потому кроссоверные RJ-45 не использовались.

Так как одним из требований заказчика было сохранение коммерческой тайны компании, для поддержания политики безопасности целесообразно было применить виртуальные локальные подсети. В сети, разбитой на виртуальные подсети, удобно применять политики и правила безопасности для каждого VLAN-а, ибо политика будет применена к целой подсети, а не к отдельному устройству.

Также это добавляет удобство адресации и логического разделения среды передачи данных. Для достижения необходимой степени административного контроля, разрабатываемая локальная сеть разделена на 6 сетей VLAN. Распределяются они следующим образом:

1. Административный VLAN– 2
2. Директорский VLAN– 3
3. VLAN отдела IT – 4
4. VLAN отдела тестирования – 5
5. Гостевой VLAN – 6
6. Печатный VLAN – 7
7. Internet VLAN – 8

Далее проводится более подробный разбор каждой единицы структурной схемы (см. приложение А) разрабатываемой локальной сети.

## Административная подсеть

В данной структурной единице локальной сети осуществляется администрирование всей сети посредством программирования центрального коммутатора L3, выступающего в роли DHCP-сервера. Также в одной стойке с ним в прямом доступе системного администратора находятся сервер и GPON-модем.

## Директорская подсеть

В данной структурной единице локальной сети выделено два адреса для подключения ПК директора компании и одного его беспроводного устройства. Данная виртуальная сеть представлена в виде беспроводной точки доступа access point 3 и 2-х подключаемых устройств.

## Печатная подсеть

Данная виртуальная сеть представлена в виде цветного и чёрно-белого принтера и создана для возможности ограничения доступа к принтерам из гостевого VLAN-a.

## Подсеть отдела IT

В данной структурной единице локальной сети выделено 16 адресов для подключения 8 ПК сотрудников IT отдела компании и их 8 беспроводных устройств. Данная виртуальная сеть представлена в виде беспроводной точки доступа access point 1 и 16-ти подключаемых устройств.

## Подсеть отдела тестирования

В данной структурной единице локальной сети выделено 16 адресов для подключения 8 ПК сотрудников IT отдела компании и их 8 беспроводных устройств. Данная виртуальная сеть представлена в виде беспроводной точки доступа access point 2 и 16-и подключаемых устройств.

## Гостевая подсеть

В данной структурной единице локальной сети выделено 3 адреса для подключения 3 беспроводных устройств гостей. Данная виртуальная сеть представлена в виде беспроводной точки доступа access point 0 и 3-х подключаемых устройств.

## Internet VLAN

Данная структурная единица локальной сети отделяет выход в глобальную сеть Интернет от остальной сети, для того, чтобы лишь те подсети, которым это необходимо могли обращаться наружу сети.

# ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

На этапе функционального проектирования в данном разделе описывается функционирование программной и аппаратной составляющей разрабатываемой локальной компьютерной сети. Более детально изучить топологию и компоненты разрабатываемой локальной сети можно в приложении Б.

## Обоснование выбора сетевой операционной системы

Так как большая часть оборудования в курсовом проекте производится компанией Cisco, то и выбор операционной системы не заставляет себя ждать. Взор падает конечно же на Cisco IOS. Среди оборудования курсового проекта данная операционная система используется на сервере, четырёх беспроводных точках доступа и коммутаторе третьего уровня. Перечень оборудования можно увидеть в приложении Д. В задачи Cisco IOS входят сетевая организация, маршрутизация,коммутация и передача данных.

Интерфейс Cisco IOS представлен стандартной командной строкой с возможностью ввода множества команд для тонкой настройки оборудования под определённые нужды.Всем командам приписывается определённый уровень привилегий от 0 до 15, и к ним могут обратиться только пользователи с соответствующим уровнем привилегий. Для настройки есть несколько уровней доступа, каждый из которых даёт свой перечень возможностей и уровень привилегий:

1. User EXEC или пользовательский режим. Базовый уровень доступа, получаемый при запуске оборудования Cisco. Уровень привилегий 1 по умолчанию, может быть изменён.
2. Privileged EXEC или привилегированный режим. Получается после указания команды enable. Уровень привилегий 15.
3. Global Configuration или режим глобальной конфигурации. Получается после указания команды configure terminal в привилегированном режиме. Уровень привилегий 15.

Для каждого уровня можно установить логин и пароль в целях безопасности.

Удобства добавляет автодополнение команд. Оно позволяет не писать команды полностью, что сильно ускоряет настройку.

Дополнительные возможности IOS реализованы в четырех типах сетевых служб:

1. Возможности надежной динамической маршрутизации.
2. Процессы оптимизации WAN.
3. Менеджмент и сервисы безопасности.
4. Сервисы масштабируемости.

Как любая операционная система на любом компьютере, Cisco IOS управляет аппаратными и программными ресурсами маршрутизатора, включая выделение памяти, процессы, безопасность и файловые системы. Cisco IOS является многозадачной операционной системой, которая интегрирована с маршрутизацией, коммутацией, межсетевым взаимодействием и телекоммуникационными функциями.

Обычно IOS содержится в едином файле в памяти маршрутизатора, называемом образом. Образы могут довольно сильно различаться для различных устройств и моделей устройств Cisco.Также отличается и функционал образов. Обычно, чем больше функций в IOS, тем больше образ IOS, и поэтому, больше флэш-памяти и RAM, которая обязана хранить и загружать IOS.

## Администрирование и серверная часть сети

### **Выбор оборудования**

В качестве сервера используется Cisco UCS C4200 Series Rack Server Chassis. Данный сервер обеспечивает отличную производительность в условиях ограниченного пространства. Поддержка до четырех 2-х-сокетных серверных узлов Cisco UCS C125 M5 обеспечивает лидирующие в отрасли производительность и эффективность для широкого спектра рабочих нагрузок, в том числе для масштабируемых и требующих большого объема вычислений. Данные серверы могут быть развернуты как автономные серверы или как часть Cisco Unified Computing System (CiscoUCS).

Оборудование имеет следующие характеристики:

1. Процессоры AMDEPYC серии 7000, до 32 ядер на сокет
2. До 2 ТБ оперативной памяти с использованием шестнадцати 128-ГБ модулей памяти DDR4 для конфигурации с 2 сокетами(восемь модулей DIMM / каналов памяти на процессор)
3. Более 45 ТБ дискового пространства, до шести 2,5-дюймовых дисков прямого подключения малого форм-фактора (SFF) с прямым подключением к узлу
4. Дополнительные карты памяти SD или модульное хранилище M.2 для увеличения емкости накопителя или загрузочного диска
5. Поддержка RAID-контроллера Cisco 12-G 9460-8i PCIe SAS с 2-ГБ кэш-памятью с флэш-поддержкой(FBWC)
6. Сетевой слот OCP 2.0, поддерживающий скорость до 100 Гбит/с
7. Поддержка платы виртуального интерфейса PCIe четвертого поколения Cisco (VIC)

Для задач данной курсовой работы достаточно одного данного сервера в минимальной комплектации с одним узлом, одним модулем памяти DDR4 и одним диском. Дополнительные карты памяти или модульное хранилище не требуются.

Данное устройство используется именно как web-сервер, потому его вычислительных мощностей достаточно.

### **Настройка web-сервера**

Настройка осуществляется для IIS OS MS Windows 10

Алгоритм следующий:

1. Открыть Панель управления > Программы и компоненты > Включение или отключение компонентов Windows.

2. Раскрыть раздел Службы IIS > Службы Интернета и установить флажки в чекбоксах следующих компонентов:

a. Безопасность. Выбрать все компоненты кроме Проверка подлинности с сопоставлением сертификата клиента, Проверка подлинности с сопоставлением сертификата клиента IIS, Централизованная поддержка SSL – сертификата.

b. Компоненты разработки приложений. Не устанавливать компоненты.

c. Общие функции HTTP. Отметить все компоненты.

d. Проверка работоспособности и диагностика. Выбрать компоненты Ведение журнала HTTP и Монитор запросов.

e. Функции повышения быстродействия. Отметить все компоненты.

f. Средства управления веб-сайтом. Отметить компонент Консоль управления IIS.

3. После установки необходимых компонентов, перезагрузить сервер.

4. Открыть Панель управления > Администрирование > Диспетчер служб IIS или Управление компьютером > Службы и приложения > Диспетчер служб IIS.

5. В окне Подключения выбрать папку Сайты

6. Выбрать сайт Default Web Site и остановить его.

7. В окне Подключения выбрать папку Сайты

8. В окне Действия нажать на ссылку Добавить веб-сайт…

9. В мастере создания веб-сайта указать

a. Название

b. Расположение (по умолчанию c:\inetpub\wwwroot)

c. В проверке подлинности указать пользователя Studc паролем 1945(если ранее создавалась другая учетная запись, включенная в группу Администраторы, указать ее)

d. Произвести проверку соединения, нажав на кнопку Тест настроек…

e. Остальные поля оставить без изменений > OK.

10.Проверить работоспособность созданного сайта. Открыть браузер и в адресной строке ввести <http://localhost>.

11. Открыть браузер на оконечном устройстве сети и в адресной строке набрать <http://192.168.6.1>

## Организация рабочих мест и гостевая часть сети

Под рабочим местом понимается часть производственной площади с размещенным на ней технологическим оборудованием и инвентарем, необходимыми для эффективного выполнения поставленных перед работником задач. Рабочее место является первичной ячейкой производственной структуры компании.

Организация рабочего места в данной курсовой работе представляет из себя наличие персональных компьютеров и возможности подключения беспроводных устройств сотрудников к сети компании. Далее оба устройства должны иметь возможность выхода в глобальную сеть Интернет. В качестве персонального компьютера для работы с Java-приложениями и удобного выхода в сеть, может использоваться любая машина, имеющая среднюю производительность, и качественную сетевую карту. Также одним из условий было наличие web-камер, установленных на мониторах сотрудников.

Для подключения ПК к локальной сети достаточно воткнуть в разъём сетевой карты подведённую к рабочему месту витую пару прямого типа RJ-45. Гостевые устройства могут подключаются по беспроводному каналу на первом этаже. Также работники могут подключиться по беспроводному каналу в помещениях своих отделов на втором этаже.

По условию требовалось установить в здание два принтера, один чёрно-белый, а второй цветной. Оба они также подключены витой парой прямого типа RJ-45, как и пользовательские станции.

Перечень выбранного оконечного оборудования можно найти в приложении Д.

Для ПК и принтеров необходимо прописать default-gateway на L3-коммутатор. Прописывается адрес того VLAN-а, к которому относится устройство.

Для подключения беспроводных устройств используется точка доступа Cisco (WAP561-A-K9) с двумя радиомодулями Wireless-N.

Оборудование имеет следующие характеристики:

1. Интерфейсы: 10/100/1000 BASE-T с автоматическим определением (RJ45)
2. Радио: 802.11n с двумя параллельными радиомодулями
3. Беспроводная связь: 802.11n, 3 х 3 с несколькими входами и несколькими выходами (MIMO)
4. Режимы работы: режим точки доступа, мост системы беспроводной связи (WDS), мост рабочей группы

Данные точки доступа пассивны и питаются от напряжения L3-коммутатора, специально подобранного для удержания необходимой нагрузки.

На каждой точке доступа необходимо настроить следующие основные параметры: Host Name, Configuration Server Protocol, IP Address, IP Subnet Mask, Default Gateway, SNMP Community. После назначения базовых параметров точке доступа необходимо настроить параметры безопасности для предотвращения несанкционированного доступа к сети. Для быстрой настройки безопасности доступны следующие параметры: No Security, Static WEP Key, EAP Authentication, WPA and WPA2.

Выполняя следующие действия, можно удалить текущую конфигурацию:

1. Открыть интернет-браузер. Необходимо использовать Microsoft Explorer.

2. Ввести IP-адрес точки доступа в адресную строку браузера и нажать кнопку ввод. Откроется окно.

3. Ввести имя пользователя в поле User Name.

4. Ввести пароль в поле Password и нажать Enter.

5. Нажать System Software. Откроется страница System Software.

6. Нажать System Configuration. Откроется страница System Configuration.

7. Нажать Reset to Defaults или Reset to Defaults (Except IP).

8. После перезагрузки точки доступа, настроить заново ее согласно требованиям.

## Обоснование выбора среды передачи данных

Среда передачи данных – это физическая [субстанция](https://ru.wikipedia.org/wiki/%D0%A1%D1%83%D0%B1%D1%81%D1%82%D0%B0%D0%BD%D1%86%D0%B8%D1%8F), по которой происходит [передача](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B0_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) той или иной [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) от источника к приёмнику.

В данной курсовой работе среда передачи данных представлена медью, оптикой и радиоволнами. Выражены они в витой паре прямого типа RJ-45, волоконным-оптическим кабелем и консольным кабелем.

Первым соединяются почти все устройства в топологии. Второй используется для соединения GPON-модема с провайдером. Третий для прямого доступа администратора к активному оборудованию сети.

## Обоснование выбора активного сетевого оборудования

В качестве L3-коммутатора используется Cisco Catalyst WS-C2960X-48LPS-L 48-портовый Ethernet-коммутатор с 370 Вт PoE.

Оборудование имеет следующие характеристики:

1. 48 портов Gigabit Ethernet с высокой скоростью переадресации
2. 2 фиксированных 10 Gigabit Ethernet SFP + восходящих канала
3. Поддержка PoE + с пределом до 370 Вт и постоянным PoE
4. Управление устройством с помощью веб-интерфейса, беспроводного доступа через Bluetooth, интерфейса командной строки (CLI), простого протокола управления сетью (SNMP) и консольного доступа RJ-45 или USB
5. Управление сетью с помощью Cisco Prime, Cisco Network Plug and Play и Cisco DNA Center
6. Функции уровня 3 с маршрутизируемым доступом (Open Shortest Path First [OSPF]), статической маршрутизацией и протоколом маршрутизации (RIP)
7. Видимость с системой доменных имен в качестве авторитетного источника (DNS-AS) и полного (гибкого) Net Flow
8. Защита с помощью 802.1X, анализатора последовательного порта (SPAN) и Bridge Protocol Data Unit (BPDU) Guard

Данный коммутатор является центром топологии и благодаря своим характеристикам справляется с текущим через него трафиком такого количества устройств. Всего в сети 41 оконечное устройство, 21 из которых подключено напрямую, а остальные 20 через беспроводные точки доступа. Также коммутатор сам запитывает пассивные беспроводные точки доступа.

В качестве GPON-модема был выбран Cisco ME4600 OLT 1RU Chassis with 8 x GPON, 4 x GE and 4 x 10GE.

Оборудование имеет следующие характеристики:

1. Локальное управление через CLI и HTTP или HTTPS веб-браузер
2. Удаленное управление с использованием Telnet или SSH и SNMPv1 / v2 / v3
3. CPE удаленное управление через OMCI и TR-69
4. Прямое исправление ошибок (FEC)
5. До 128 ONT или ONU на PON

В данной курсовой работе GPON-модем является мостом между L3-коммутатором и сетью провайдера. Для его корректной работы достаточно провести настройку через браузер в соответствии с инструкциями провайдера. Также на оптическом интерфейсе необходимо отключить все протоколы, порождающие побочный трафик в сеть.

### **Настройка DHCP**

В данной курсовой работе внутренняя сеть использует локальную IPv4 адресацию, в которой, для выдачи динамических адресов беспроводным устройствам, необходимо настроить DHCP.

Для настройки DHCP использовались следующие шаги:

Назначаем vlan интерфейсам ip-адреса.

Switch(config)#int vlan 3

Switch(config-if)#ip address 192.168.5.1 255.255.255.224

И так для всех интерфейсов.

VLAN 4 - 192.168.1.1 255.255.255.224

VLAN 5 - 192.168.2.1 255.255.255.224

VLAN 6 - 192.168.3.1 255.255.255.224

Включаем ip routing и создаем пулы адресов DHCP

Switch(config)#ip routing

Switch(config)#ip dhcp pool v3

Switch(dhcp-config)#network 192.168.5.0 255.255.255.224

Switch(dhcp-config)#default-router 192.168.5.1

Аналогично повторяем для каждого VLAN-а. Исключаем адреса интерфейсов из пула.

Switch(config)#ip dhcp excluded-address 192.168.1.1 192.168.2.1 192.168.3.1 192.168.5.1

Аналогично для всех устройств со статическими адресами.

Switch(config)#ip dhcp excluded-address 192.168.1.2 192.168.1.3 … 192.168.1.9 192.168.2.2 192.168.2.3 … 192.168.2.9 192.168.5.2

Для DHCPv6 проводим такие же операции, заменив адреса v4 на v6 по таблице адресации (Приложение Е). Также необходимо заменить ip routing на ipv6 unicast-routing, а часть команды ip на ipv6.

### **NAT**

В данной курсовой работе внутренняя сеть использует локальную IPv4 адресацию, которая требует трансляции адресов для доступа в глобальную сеть Интернет.

При динамической трансляции создаётся пул возможных внутренних адресов и устанавливается критерий соответствия, для определения того, какие внутренние IP-адреса должны транслироваться с помощью NAT.

Для указания частных IP-адресов, подлежащих трансляции, динамическая трансляция NAT использует списки управления доступом [ACL](http://netclo.ru/nastroyka-acl-v-cisco/), а также определяет пул зарегистрированных открытых IP-адресов, которые будут выделяться для этого. Алгоритм настройки динамической трансляции следующий:

1. Настроить интерфейсы, которые будут находиться во внутренней подсети, с помощью команды ip nat inside.
2. Настроить интерфейсы, которые будут находиться во внешней подсети, с помощью команды ip nat outside.
3. Настроить список ACL, соответствующий пакетам, поступающим на внутренние интерфейсы, для которых должна быть применена трансляция NAT.
4. Настроить пул открытых зарегистрированных IP-адресов с помощью команды режима глобального конфигурирования ip nat pool (имя) (первый адрес) (последний адрес) netmask (маска подсети).
5. Включить динамическую трансляцию NAT, указав в команде глобального конфигурирования ip nat inside source list (номер acl) pool (имя пула)

В данной курсовой работе NAT настраивался следующим образом:

Переходим в расширенный режим.

Switch>enable

Переходим в режим конфигурации.

Switch#configure terminal

Настройка интерфейса в сторону частной сети.

Switch(config)#interface fa0/0

Задаем шлюз по-умолчанию.

Switch(config-if)#ip address 192.168.1.1 255.255.255.224

Включаем интерфейс физически.

Switch(config-if)#no shutdown

Настраиваем интерфейс как внутренний.

Switch(config-if)#ip nat inside

Switch(config-if)#exit

Повторяем для всех интерфейсов L3-коммутатора, к которым подключены VLAN-ы.

Настройка интерфейса в сторону провайдера.

Switch(config)#interface fa0/1

Задаем IP и маску

Switch(config-if)#ip address 178.122.77.59 255.255.255.252

Включаем интерфейс физически

Switch(config-if)#no shutdown

Настраиваем интерфейс как внешний

Switch(config-if)#ip nat outside

Switch(config-if)#exit

Создаем динамический пул

Switch(config)#ip nat pool inPool 192.168.1.1 192.168.7.1 netmask 255.255.248.0

Создаем список доступа 1, в котором разрешаем транслировать IP-адреса из подсети 192.168.1.0/21

Switch(config)#access-list 1 permit 192.168.1.1 0.0.0.224

Включаем динамическую трансляцию

Switch(config)#ip nat inside source list 1 pool inPool

Статический маршрут в сторону провайдера

Switch(config)#ip route 0.0.0.0 0.0.0.0 178.122.77.59

## Информационная безопасность локальной компьютерной сети

AAA (Authentication Authorization and Accounting) - система аутентификации авторизации и учета событий, встроенная в операционную систему Cisco IOS. Она предоставляет пользователям безопасный удаленный доступ к сетевому оборудованию Cisco, а также предлагает различные методы идентификации и авторизации пользователя, и сбора информации с отправкой на сервер.

Аутентификация (Authentication) - предоставляет методы идентификации пользователей, включающие диалог "логин-пароль", вызовы и ответы, различные сообщения, зависящие от метода.

**Авторизация (Authorization)** - предоставляет методы для удалённого доступа, включающие одновременную авторизацию или авторизацию для каждого сервиса, пользовательские аккаунты и профили, пользовательские группы, поддержку IP, IPX, ARA и Telnet.

**Аккаунтинг (Accounting)** — служит для сбора и отправки информации на сервер. Используется для биллинга, аудита и отчётности. Может включать следующую информацию: идентификация пользователей, время остановки и запуска, запуск выполняемых команд (таких как PPP), число пакетов и количество байт.

В данном курсовом проекте AAA настраивалось по следующему алгоритму:

Включаем шифрование паролей.

servicepassword-encryption

Задаем пароль для привилегированного режима.

enablesecret \*\*\*\*\*\*\*

AAA работает таким образом, что если не получен ответ от сервера, клиент предполагает аутентификацию неуспешной. Потому обязательно создаем локального пользователя на случай, если RADIUS сервер недоступен по какой-либо причине.

username recover password \*\*\*\*\*\*\*\*\*

Включаем ААА.

aaa new-model

Баннер о том, что это закрытая система.

aaa authentication banner ^ Access only for persons explicitly authorized. All rights reserved. ^

Сообщение на случай неуспешной аутентификации.

aaa authentication fail-message ^ Authentication failed. ^

Создаем профиль аутентификации, а также не забываем как резервный указать локальный способ аутентификации.

aaa authentication login login-RADIUS group radius local

Создаем профиль авторизации.

aaa authorization exec auth-RADIUS-exec group radius local

По умолчанию клиент ААА трижды пытается авторизоваться через RADIUS. Чтобы не блокировать учетные записи в AD, ставим 1 попытку.

radius-server retransmit 1

Указываем наш RADUIS сервер.

radius-server host 2a00:1760:4231:f020::2

Задаем ключ для шифрования.

radius-server key javaforever

Включаем созданные профили для виртуальных консолей.

line vty 0 15

exec-timeout 15 0

login authentication login-RADIUS

authorization exec auth-RADIUS-exec

timeout login response 180

no password

Для работы данного сервиса используется сервер, выбранный в перечне сетевого оборудования ранее.

Далее необходимо реализовать структуру VLAN, описанную в разделе структурного проектирования. Делается это следующим образом:

Для создания VLAN на центральном коммутаторе прописываем следующее:

Switch>en

Switch#conf t

Switch(config)#vlan 'номер vlan-a'

Switch(config-vlan)#name 'имя vlan-a'

Прописываем для всех 7 vlan-ов. Далее, так как у нас топология звезда, мы можем построить почти всё на access-портах:

Switch(config-vlan)#ex

Switch(config)#interface 'Id интерфейса'

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 'номерvlan-a'

Таким образом настраиваем выходы ко всем ПК и беспроводным точкам доступа в сети. Access point 1 и access point 2 будут относиться к тем же vlan-ам, к которым подключены ПК отдела IT и отдела тестирования соответственно.

Далее даём доступ к принтерам всем vlan-ам кроме гостевого.

Switch(config)# interface range 'Id интерфейса младший – Id интерфейса старший'

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 'номера vlan-ов'

В целях безопасности прописываем port-security (только на интерфейсе, предназначенном для администратора):

switchport port-security

switchport port-security maximum 1

switchport port-security violation restrict

switchport port-security mac-address

Записываетсямак-адрес того устройства, которое нужно защитить.

Доступность данных в сети регулируется настроенным AAA-сервисом с помощью AAA-сервера. Доступ к данным разрешен только для клиентских машин, данные о которых размещаются в административной подсети на сервере (см. приложение Б).

## Адресация в локальной компьютерной сети

Адресация в разрабатываемой локальной сети осуществляется с помощью протокола IPv4 и IPv6. IPv4 использует 32-[битные](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82) (четырёх[байтные](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D0%B9%D1%82)) адреса, ограничивающие [адресное пространство](https://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81) 4 294 967 296 (232) возможными уникальными адресами.Традиционной формой записи [IPv4 адреса](https://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81) является запись в виде четырёх [десятичных чисел](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%81%D1%8F%D1%82%D0%B8%D1%87%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F) (от 0 до 255), разделённых точками. Через дробь указывается длина [маски подсети](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%81%D0%BA%D0%B0_%D0%BF%D0%BE%D0%B4%D1%81%D0%B5%D1%82%D0%B8). IPv6 же использует длину адреса 128 [бит](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82) вместо 32, а маска указывается через ‘/’.

Для каждого VLAN выделена своя локальная подсеть. По условию провайдер выдаёт один глобальный IPv4 адрес и IPv6 подсеть. Первый используется на коммутаторе, как адрес оптического интерфейса, обращённого к провайдеру. Подсеть же используется на коммутаторе и сервере, чтобы тот был доступен как из внутренней сети, так и из внешней. Остальные же устройства вынесены в локальные IPv4 и IPv6 подсети. Настройка для IPv4 NAT и DHCP была описана выше.

Обязательно должны быть прописаны IP для всех VLAN-ов на L3-коммутаторе. Там же необходимо прописать ip routing и ipv6 unicast-routing.

Таблица адресации представлена в Приложении Е.

## Подсчёт стоимости сети

Сервер – 2398$

L3-коммутатор – 1319$

Беспроводные точки доступа – 102 \* 4 = 408$

GPON-модем – 468$

Серверная стойка – 292$

Волоконно-оптический кабель – 10$

ПК – 18 \* 923 = 16614$

Витая пара прямого типа RJ-45 – 126$

Монтажный короб – 56$

Чёрно-белый принтер – 124$

Цветной принтер – 202$

Консольный кабель – 11$

Суммарная стоимость = 22028

Как видно, большую часть стоимости ушло на пользовательские станции, следовательно подобранное активное и сетевое оборудование не избыточно.

# 4 КАБЕЛЬНАЯ СТРУКТУРА СКС

Как уже было сказано, основным типом соединения в построенной топологии является витая пара прямого типа RJ-45. Из-за топологии звезда кабеля потребовалось довольно много. На все соединения ушло около 200 м кабеля. Ещё 5 было добавлено в перечень (Приложение Д) с учётом на обрезки и порчу кабеля.

Витая пара — это вид кабеля связи, представляющий из себя одну или несколько пар изолированных проводников, скрученных между собой и покрытых пластиковой оболочкой. Свивание проводников производится с целью повышения связи проводников одной пары. Благодаря этому электромагнитная помеха одинаково влияет на оба провода пары и компенсирует сама себя. Для снижения связи отдельных пар кабеля в кабелях UTP категории 5 и выше провода пары свиваются с различным шагом.

В данной курсовой работе используются кабели FTP категории 6. Описание данных типов было указано в обзоре литературы. Используются они по той причине, что разъёмы активного и серверного оборудования поддерживают Gigabit Ethernet. Также из-за прокладки в одном коробе нескольких кабелей им желательно экранирование. Данного кабеля необходимо 200 м из-за топологии звезда, требующей обширного количества кабеля. Ещё 5 метров добавлено с учётом обрезков и порчи кабеля при монтаже. Полная модель кабеля - витая пара FUTP Cat 6е RJ-45. Витые пары помещены связками или по одному, в зависимости от расположения в здании по чертежу (Приложение В и Г), внутрь монтажного короба. Параметры короба - материал ПВХ, размер 100х40. Короб проложен вдоль стен, внизу или вверху в зависимости от чертежа (Приложение В и Г).

Для соединения административной рабочей станции Admin’s PC c L3-коммутатора используется консольный кабель Cisco DB9 - RJ45. Его достаточно в количестве 5 метров единым кабелем.

Волоконно-оптического кабеля используется 10м для подключения GPON-модема к внешней магистрали. Его модель Gembird CFO-LCLC-OM2-10M.

Все кабели тянутся из серверной на первом этаже, где расположена серверная стойка. Внутри неё находятся L3-коммутатор, сервер и GPON-терминал.

В необходимых местах необходимо просверлить стены для удобной прокладки кабеля. Беспроводные точки доступа закреплены на стенах, на высоте 1.5 метра. К ним ведут спуски или подъёмы в кабельных каналах в зависимости от того, внизу или вверху стены находится ближайший короб с необходимой витой парой, идущей к L3-коммутатору.

# ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы получены практические и теоретические навыки проектирования вычислительной локальной сети. Во время выполнения курсовой работы создана локальная сеть небольшой компании, занимающейся разработкой Java-приложений.

Для написания данной курсовой работы сначала было изучено различие LAN и WAN сетей. Затем, после изучения различных топологий и заданных условий была выбрана топология звезда. Далее было изучено различное сетевое оборудование из перечня, предлагаемого Cisco, и по документации выбран сервер, соответствующий необходимым требованиям к производительности и ценовой категории. После этого было изучено активное оборудование сети, опять же по документации Cisco, и выбран L3-коммутатор как центр топологии.

Следующим шагом был подбор клиентского оборудования. Были выбраны комплектующие оконечных устройств. Для персональных компьютеров были подобраны системные блоки с необходимыми сетевыми картами, мониторы, клавиатуры, мыши, веб-камеры. Также в соответствии с требованиями в топологию были помещены чёрно-белый и цветной принтеры.

Изучив различные категории кабелей и пересмотрев топологию было выявлено, что достаточно использовать RJ-45 прямого типа категории 6 c FTP типом защиты. Также необходима была оптика и сам оптический интерфейс для L3-коммутатора.

Также в топологию было добавлено место для системного администратора, который получил возможность подключения к серверной стойке, где установлен L3-коммутатор с помощью консольного кабеля.

В курсовой работе представлены необходимое оборудование, структурная, функциональная схемы, планы этажей и спецификация оборудования и материалов, необходимых для построения локальной вычислительной сети. Выбранное оборудование соответствует всем стандартам качества, надежности и зарекомендовало себя как одно из лучших во множестве организаций.

# ПРИЛОЖЕНИЕ А

(обязательное)

Схема СКС структурная

# ПРИЛОЖЕНИЕ Б

(обязательное)

Схема СКС функциональная

# ПРИЛОЖЕНИЕ В

(обязательное)

План первого этажа

# ПРИЛОЖЕНИЕ Г

(обязательное)

План второго этажа

# ПРИЛОЖЕНИЕ Д

(обязательное)

Перечень оборудования, изделий и материалов

# ПРИЛОЖЕНИЕ Е

(обязательное)

Схема адресации

# 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. LAN и WAN — [Электронный ресурс]. — Электронные данные. — Режим доступа:

<http://ciscotips.ru/wan-lan>

6. Сетевые топологии — [Электронный ресурс]. — Электронные данные. — Режим доступа:

<https://ru.wikipedia.org/wiki/Сетевая_топология>

7. DHCP — [Электронный ресурс]. — Электронные данные. — Режим доступа:

<https://greendail.ru/node/chto-takoe-dhcp-i-kak-rabotaet-obyasnenie-osnovnyh-principov>

8. NAT — [Электронный ресурс]. — Электронные данные. — Режим доступа:

<https://sonikelf.ru/vse-chto-vy-xoteli-znat-o-nat-no-boyalis-sprosit-nat-pat-snat-dnat/>

9. Категории витой пары — [Электронный ресурс]. — Электронные данные. — Режим доступа:

https://www.legrand2.ru/rjcategory.html

10. Волоконно-оптический кабель — [Электронный ресурс]. — Электронные данные. — Режим доступа:

https://ru.wikipedia.org/wiki/Волоконно-оптический\_кабель

11. Консольный кабель — [Электронный ресурс]. — Электронные данные. — Режим доступа:

https://ru.wikipedia.org/wiki/Консольный\_кабель

12. VLAN — [Электронный ресурс]. — Электронные данные. — Режим доступа:

https://ru.wikipedia.org/wiki/VLAN

13. AAA — [Электронный ресурс]. — Электронные данные. — Режим доступа:

https://vasexperts.ru/blog/autentifikaciya-avtorizaciya-i-uchet-aaa-radius-ili-tacacs/