СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4

1 ОБЗОР ЛИТЕРАТУРЫ 5

2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ 8

2.1 Выбор топологии локальной вычислительной сети 10

2.2 Выбор технологии локальной вычислительной сети ………………...…13

3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ 16

3.1 Обоснование выбора сетевой операционной системы …………………16

3.2 Обоснование выбора серверного оборудования …………………….…..16

3.3 Обоснование выбора клиентского оборудования ……………….………17

3.4 Обоснование выбора активного сетевого оборудования ……….........…19

3.5 Выбор аппаратных средств для реализации беспроводного решения…21

3.5.1 Расчет характеристик проектируемой беспроводной сети..............23

3.6 Информационная безопасность локальной компьютерной сети ……....25

3.7 Схема адресации сети организации………………………………………25

4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ

СИСТЕМЫ 28

4.1 Выбор категории кабеля «витая пара» для реализации сети …..………30

ЗАКЛЮЧЕНИЕ 31

[ПРИЛОЖЕНИЕ А. Схема СКС структурная 32](file:///D:\Google_Drive\Study\АОКС\Курсач\Пояснительная%20записка.docx#_Toc470174766)

[ПРИЛОЖЕНИЕ Б. Схема СКС функциональная 33](file:///D:\Google_Drive\Study\АОКС\Курсач\Пояснительная%20записка.docx#_Toc470174767)

[ПРИЛОЖЕНИЕ В. План этажа. Здание первое 34](file:///D:\Google_Drive\Study\АОКС\Курсач\Пояснительная%20записка.docx#_Toc470174768)

[ПРИЛОЖЕНИЕ Г. План этажа. Здание второе 25](file:///D:\Google_Drive\Study\АОКС\Курсач\Пояснительная%20записка.docx#_Toc470174768)

[ПРИЛОЖЕНИЕ Д. Реализация проектируемой сети в Cisco Packet Tracer 36](file:///D:\Google_Drive\Study\АОКС\Курсач\Пояснительная%20записка.docx#_Toc470174769)

[ПРИЛОЖЕНИЕ Е. Конфигурация сетевого оборудования 37](file:///D:\Google_Drive\Study\АОКС\Курсач\Пояснительная%20записка.docx#_Toc470174769)

[ПРИЛОЖЕНИЕ Ж. Перечень оборудования, изделий и материалов 41](file:///D:\Google_Drive\Study\АОКС\Курсач\Пояснительная%20записка.docx#_Toc470174769)

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ…………………………….42

**ВВЕДЕНИЕ**

Большинство существующих организаций для своей работы используют большое количество компьютеров. Современные организации имеют компьютеры для каждого сотрудника и используют их для различных целей, например, программисты для того чтобы разрабатывать программные продукты, редакторы чтобы писать брошюры, бухгалтера чтобы делать платежные ведомости. В самом начале, когда только начали появляться компьютерные сети многие из этих компьютеров работали в изолированности от других, но со временем и требованиями людей, нужно было как-то соединить компьютеры в единую сеть, чтобы было возможно передавать информацию по всей компании.

Посмотрев на эту проблему с общей точки зрения, то наиболее главным вопросом является совместное использование ресурсов. Соответственно, целью – предоставить доступ к данным, программам и оборудованию для любого пользователя сети, в независимости где физически расположен ресурс и пользователь. Но более важной проблемой, чем совместное использование физических ресурсов, таких как принтеры, сканеры, устройства резервного копирования и другого оборудования, является совместное использование информации. В современном мире любая организация, независимо от ее размеров, просто невозможна без данных, представленных в электронном виде. Маленькие и большие организации в наше время зависят от компьютеризированной информации. У большинства организаций в сети находится вся информация, такая как отчеты, информация о продукте, информация о сотрудниках и многое другое.

В маленьких организациях обычно все оборудование и компьютеры находятся в пределах одного офиса или одного здания. Если же говорить о больших организациях, то и вычислительная техника, и работники могут находится в различных офисах в разных странах мира. Но несмотря на большое расстояние, работник, находящийся в Минске, может сразу же получить информацию необходимую ему для работы, имеющую на сервере в Москве. В данном случае для соединения сетей, которые расположенных в разных местах, могут быть использованы сети под названием VPN (Virtual Private Networks – виртуальные частные сети). Более простыми словами это значит, что если пользователь находится от физического хранилища данных на очень большом расстоянии, то расстояние никак не ограничивает его возможности доступа к данным.

Таким образом информационная система организаций в общих случаях представлена как совокупность баз данных и некоторого количества работников, которым удаленно предоставляется информация. В этом случае данные хранятся на серверах.

**1 ОБЗОР ЛИТЕРАТУРЫ**

Для выполнения данной курсовой работы были использованы научная и учебно-методическая литература, статьи в периодических изданиях Республики Беларусь, стран СНГ, а также зарубежная литература.

Книга «Компьютерные сети» [9] является самой авторитетной по современным сетевым технологиям, написанной признанным экспертом в этой области Эндрю Таненбаумом в соавторстве с профессором Вашингтонского университета Дэвидом Уэзероллом. Первая версия этого классического труда появилась на свет в далеком 1980 году, и с тех пор каждое издание книги неизменно становилось бестселлером и использовалось в качестве базового учебника в ведущих технических вузах. В книге последовательно изложены основные концепции, определяющие современное состояние и тенденции развития компьютерных сетей. Авторы подробнейшим образом объясняют устройство и принципы работы аппаратного и программного обеспечения, рассматривают все аспекты и уровни организации сетей – от физического до уровня прикладных программ. Изложение теоретических принципов дополняется яркими, показательными примерами функционирования Интернета и компьютерных сетей различного типа. Пятое издание полностью переработано с учетом изменений, происшедших в сфере сетевых технологий за последние годы и, в частности, освещает такие аспекты, как беспроводные сети стандарта 802.12 и 802.16, сети 3G, технология RFID, инфраструктура доставки контента CDN, пиринговые сети, потоковое вещание, Интернет-телефония и многое другое.

В книге Андрея Семенова «Волоконная оптика в локальных и корпоративных сетях» [6] приводятся физические принципы функциониро-вания волоконно – оптических сетей связи. Рассматриваются пассивные компоненты волоконно-оптической кабельной системы: кабели, оконечные разделочные устройства, шнуры, коннекторы и т.д. Анализируются волоконно-оптические технологии в сетях FDDI, Ethernet, Fast Ethernet и т.д. Дается методика инженерного расчета, рекомендации по проектированию, монтажу и эксплуатации оптических подсистем локальных и корпоративных сетей.

Учебное пособие Виктора Олифера «Компьютерные сети. Принципы, технологии, протоколы» [5] является один из лучших учебников по сетям. Со времени выхода предыдущего издания она претерпела значительные переработки, включив в себя изменения, которые произошли в области компьютерных сетей за последние шесть лет:

- преодоление локальными и глобальными сетями рубежа скорости в 100 Гбит/c и освоение терабитных скоростей;

- повышение эффективности и гибкости первичных оптических сетей за счет появления реконфигурируемых мультиплексоров ввода-вывода (ROADM) и применения супер-каналов DWDM, работающих на основе гибкого частотного плана;

- развитие техники виртуализации сетевых функций и услуг, приведшей к распространению облачных сервисов;

- выход на первый план проблем безопасности.

Учебное пособие «Основы локальных сетей» [3] представляет собой краткое пособие по локальным компьютерным сетям, в котором рассматрива-ются ключевые принципы, лежащие в основе архитектуры локальных сетей, базовые функции локальных сетей, а также алгоритмы реализации этих функций. Приводятся рекомендации по проектированию наиболее распространенных сетей Ethernet и Fast Ethernet. Также разбираются вопросы подключения локальных сетей к глобальной сети Интернет с помощью модемов.

Книга «Компьютерные сети: нисходящий подход» [2] идеально подойдет начинающим изучение сетевых технологий. Она знакомит с основами построения и функционирования компьютерных сетей на примере пятиуровневой архитектуры сети Интернет. В ней описаны базовые компоненты сети, основные принципы передачи данных, технологии взаимодействия сетей между собой. Отдельная глава посвящена особенностям беспроводных сетей. Весь материал книги сопровождается примерами и материалом для самостоятельного выполнения упражнений. Пособие универсально и подойдет как студентам, так и системным администраторам, а также всем желающим начать изучение компьютерных сетей или улучшить свои знания в этой области.

В учебном пособии Андрея Сергеева «Основы локальных компьютерных сетей» [7] рассматриваются теоретические основы и технологии по локальным компьютерным сетям и их построению. Излагаются вопросы:

- базовых понятий, моделей и способов построения компьютерных сетей;

- организации стека протоколов TCP/IP (IPv4 и IPv6);

- создания серверов общего доступа и служб для IP-сетей (DNS, электронная почта, веб и др.)

Отдельное внимание уделяется вопросам организации локальных сетей на Windows (рабочая группа и домен), физического построения кабельных и беспроводных локальных сетей.

В учебном пособии «Технологии современных беспроводных сетей Wi-Fi» [4] изложены основные сведения о современных технологиях беспровод-ных сетей Wi-Fi и показано поэтапное проектирование беспроводных сетей – от планирования производительности и зоны действия до развертывания и тестирования сети. Подробно рассмотрен стандарт IEEE 802.11, включая управление доступом к среде, а также физический уровень 802.11. Описаны особенности радиочастотного спектра, принципы модуляции, приведены варианты спецификаций 802.11, технологии повышения производительности и механизмы защиты. Подробно рассмотрено подключение клиента к беспроводной сети в инфраструктурном режиме - сканирование, методы аутентификации и ассоциации, а также вопросы безопасности передачи данных в беспроводных сетях (WEP, TKIP, CCMP, WPA, WPA2, WPS). Приведены оценка беспроводной линии связи и пример расчета. Представленные в учебном пособии теоретические положения дополнены лабораторными работами по всем рассмотренным в книге темам.

Учебное пособие по подготовке к сертификационным экзаменам Cisco Уэнделла Одома [9] знакомит с фундаментальными концепциями настройки сетей, поиска и устранения неисправностей. Автор бестселлеров и опытный преподаватель Уэнделл Одом делится советами по подготовке к экзамену, помогая выявить свои слабые стороны, улучшить концептуальные знания и практические навыки по сетям.

Для новичков в сертификации Cisco данное введение начинается с обсуждения основ. Настоящая книга относится к серии Official Cert Guide Series издательства Cisco Press. Книги этой серии являются официальным первоисточником для подготовки к экзамену, предоставляют теоретические и практические материалы, которые помогут кандидатам на сертификат Cisco Career Certification выявить свои слабые стороны.

Книга «Беспроводная сеть дома и в офисе» [1] поможет начинающему администратору домашней или офисной сети в кратчайшие сроки развернуть, настроить или модернизировать беспроводную сеть. Кратко изложены основы компьютерных сетей. Описаны беспроводные сети стандартов 802.11а, 802.11b, 802.11g, а также новейшего стандарта 802.11n. На практических примерах показано построение сети Wi-Fi, GPRS-соединение с Интернетом, а также объединение проводной и беспроводной сети Ethernet, реализация совместного доступа к Интернету, дан обзор технологии Power Line Communication (Интернет «из розетки»). Рассмотрены вопросы защиты с помощью антивирусов, брандмауэров, и на основе технологии виртуальных частных сетей даны рекомендации по повышению производительности сети.

# СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данной главе описаны этапы разработки структурной схемы компью-терной локальной сети, производится выбор топологии сети, обосновывается выбор отдельных структурных частей.

По варианту задания на курсовую работу необходимо создать компьютерную сеть научно-исследовательской организации в сфере медицины, в которую входит 14 персональных компьютеров, личные ноутбуки, смартфоны, файловый сервер (для обмена файлами и хранения персональных фай-лов), 2 цветных принтера. В качестве технологии канального уровня будет использоваться FastEthernet, коммутационное оборудование представляет собой коммутаторы, физическая среда – витая пара. Назначение IP-адресов – динамическое. Также должно быть настроено DHCP, которое можно настроить на самих маршрутизаторах.

Проектирование сети производится в программе моделирования сетей Cisco Packet Tracer. В качестве хостов будем использовать компьютеры, в программе моделирования – PC-PT. В каждом компьютере по условию установлена плата Fast Ethernet. В качестве коммутаторов, которые будут соединять между собой компьютеры, выберем Switch 2960. Для соединения между собой подсетей будем использовать маршрутизаторы 2911. В качестве точки доступа к сети Интернет используется маршрутизатор, подключённый к АТС через ADSL2+-фильтр. К маршрутизатору по проводной сети подключены персональные компьютеры, все остальные устройства подключены по беспроводной сети.

Для работы в качестве сервера будем использовать элемент Server-PT. Он будет использован для роли DNS и FTP. Все остальные службы, предоставляемые данным устройством, можно сразу отключить.

Реализация проектируемой сети в Cisco Packet Tracer представлен в приложении «Д» и конфигурация сетевого оборудования в приложении «E».

Начнем строить структурную схему сети. В двух удаленных друг от друга (11 км) одноэтажных зданиях. Первое здание: лаборатория (22 м2) – 4 стационарных компьютера и 8 мобильных подключений, кабинет директора (10 м2) – 1 станция и 1 мобильное подключения, 2 служебных помещения (5, 10 м2). Второе здание: лаборатория (42 м2) – 8 стационарных компьютера и 10 мобильных подключений, бухгалтерия (10 м2) – 1 стационарный компьютер и 1 мобильное подключение, 1 служебное помещение (3 м2). В первом здании располагается сервер. Для работоспособности каждой из подсетей необходимо провести настройку сервера и назначить IP-адреса компьютерам.

По заданию два здания научно-исследовательской организации нам необходимо соединить в одну сеть – локальную сеть офиса. Раньше для связи двух пунктов возникала необходимость в выделении отдельной линии для безопасной передачи данных. Для организации таких отдельно выделенных линий необходимы большие затраты. Развитие сетевых технологий не стоит на месте и с появлением виртуальных частных сетей появилась возможность пользователям безопасного доступа к ресурсам сети организации через Интернет или другие сети без необходимости выделения отдельной линии.

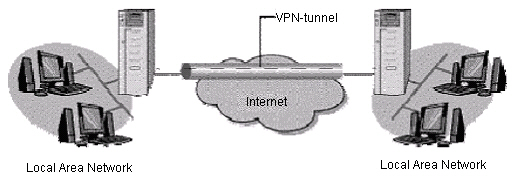


Рис. 2.1 – Структурная схема VPN для двух офисных сетей

*Источник: http://www.old.optivera.ru/support/VPN.files/image002.jpg*

В общем виде VPN (см. рис 2.1) представляет собой совокупность технологий управления доступом и контролем, аутентификации, туннелиро-вания, используемых для защиты и безопасной передачи данных через Интернет. Использовать виртуальные частные сети, более целесообразно и много причин доказывающие это. Во-первых, безопасность и защита данных. Процедура аутентификации позволяет получателю сообщения, являющего пользователем виртуальной частной сети, обеспечить целостность данных и отследить источник полученных пакетов. Гарантируется конфиденциальность пользовательских данных, которая достигается с помощью средств защиты данных в виртуальных частных сетях. Во-вторых, стоимость. Уменьшаются количество линий доступа и расходы на телефонную связь. Создание виртуальной частной сети позволяет организации передавать данные через линии доступа к Интернету, при этом позволяя отказаться от отдельно выделенных линий или уже существующих линий.

Поскольку организации обычно получают услуги от Интернет-провайдера, то при создании виртуальной частной сети уменьшаются расходы на междугороднюю телефонную связь (работникам, находящимся в офисах в различных города не нужно совершать междугородний звонок для установления прямой связи).

Использование туннелирования обеспечивает безопасность при передаче данных. При этом передача по сети протокольных пакетов сети одного типа инкапсулируются в протокольные пакеты другой сети. Туннелирование необходимо из-за того, что в сетях, использующих протокол IP, имеется уязвимость. В тот момент, когда разрабатывался протокол IP, разработчики особо не задумывались о каких-либо функциях безопасности на уровне IP. И некоторые особенности реализации данного протокола позволят легко подделать и перехватить данные в сетях использующих данный протокол.

Независимо от того, какую форму VPN выберет организация, конечный результат всегда будет одинаковым. VPN создают «туннели» через незащищенные публичные сети, чтобы установить безопасные соединения с частной сетью. Используя стандартные, но надежные средства безопасности, такие как шифрование данных и аутентификация конечных точек, VPN могут предотвращать несанкционированный доступ к этим туннелям и, в конечном итоге, к сети организации на другом конце. В настоящее время существует два популярных типа VPN, которые отличаются по уровням безопасности и способам подключения для пользователей. Для объединения двух зданий научно-медицинской организа-ции в единую сеть будем использовать протокол IPsec.

IPSec VPN изначально предназначался для подключения типа «точка-точка» и предполагал удаленный доступ к сети через стандартный клиент или приложение. Эти VPN были в основном разработаны для постоянных удаленных сайтов для доступа к одной центральной сети.

Клиентское приложение VPN – это то, что позволяет получить доступ к сети и создает туннель. Клиентское приложение устанавливается на удаленном устройстве работника, а другом конце, VPN «терминатор». Как правило, VPN «терминатор» может быть аппаратным или программным брандмауэром, используемым для защиты сети.

VPN «терминатор» или брандмауэр должен быть подготовлен для разрешения подключений удаленного рабочего. Для этого «терминатор» должен быть настроен на принятие определенных критериев безопасности. Обычно это имя группы или общий пароль.

Конечно, если клиент, установленный на компьютере удаленного работника, не настроен с соответствующими критериями безопасности, им не будет разрешен доступ.

Преимуществами IPSec VPN являются, во-первых, постоянная связь между локациями, во-вторых, поскольку IPSec работает на «уровне протокола» Интернета, то любой протокол на основе IP может быть отправлен через сеть. Это означает, что можно использовать IPSec для обоих приложений данных, использующих протоколы TCP и UDP.

**Главным недостатком IPSec VPN является то, что** после создания туннеля удаленные пользователи могут получить доступ практически к любому корпоративному ресурсу в сети, и поэтому может быть сложно или невозможно ограничить определенный доступ.

VPN-соединение IPSec лучше всего использовать для глобально распределенных групп с удаленными офисами, которые должны подключаться к одной крупной сети центрального офиса.

# 2.1 Выбор топологии локальной вычислительной сети

Под топологией компьютерной сети подразумевается схема физической связи, используемая для подключения устройств в сети. Основными типами топологий компьютерной сети являются «шина», «кольцо», «звезда», «дерево», а также так называемая беспроводная топология. Более сложные сети, могут быть построены как гибридные, используя две или более основных топологий.

Топология «звезда» (см. рисунок 2.2) является одной из наиболее распространенных сетевых топологий. В данной топологии каждый узел подключается к центральному сетевому устройству, такому как коммутатор или компьютер. Центральное сетевое устройство действует как сервер, а периферийные устройства действуют как клиенты. В зависимости от типа сетевой карты, используемой на каждом компьютере со звездообразной топологией, для соединения компьютеров используется коаксиальный кабель или сетевой кабель RJ-45.

Преимущества топологии «звезда»:

- централизованное управление сетью через центральный компьютер или коммутатор;

- легко добавить еще один компьютер в сеть;

- если один компьютер в сети выходит из строя, остальная сеть продол-жает нормально функционировать.

Недостатки топологии «звезда»:

- может потребоваться более высокая стоимость реализации, особенно при использовании коммутатора или маршрутизатора в качестве устройства центральной сети;

- центральное сетевое устройство определяет производительность и количество узлов, которые может обрабатывать сеть;

- в случае сбоя центрального компьютера или коммутатора вся сеть отключается и все компьютеры отключаются от сети.

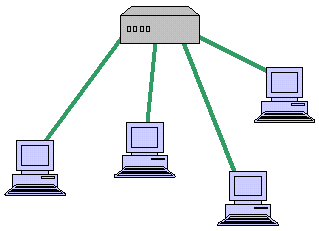


Рисунок 2.2 – Схема соединения «звезда»

Топология «шина» (см. рисунок 2.3) представляет собой сетевую топологию, в которой каждый компьютер или сетевое устройство подключены к одному кабелю или магистрали.

Преимущества топологии «шина»:

- хорошо применима для небольших сетей;

- самая простая сетевая топология для линейного подключения компью-теров или периферийных устройств;

- требует меньшей длины кабеля, чем топология «звезда».

Недостатки топологии «шина»

- трудно определить проблемы, если вся сеть выходит из строя;

- трудно устранить неполадки отдельных устройств;

- топология «шина» не подходит для больших сетей;

- дополнительные устройства замедляют работу сети;

- если основной кабель поврежден, сеть выходит из строя или

разбивается на две части.

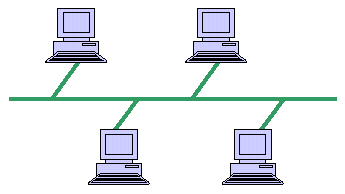


Рисунок 2.3 – Схема соединения «шина»

Топология «кольцо» (см. рисунок 2.4) является сетевой топологией, в которой все узлы связаны друг с другом таким образом, что они образуют замкнутый контур. Каждое сетевое устройство связано с двумя другими, как точки на окружности. В кольцевой сети пакеты данных перемещаются от одного устройства к другому, пока не достигают места назначения. Большинство кольцевых топологий позволяют пакетам перемещаться только в одном направлении, так называемая однонаправленная кольцевая сеть. Двунаправленная кольцевая сеть позволяют данным перемещаться в любом направлении. Основным недостатком кольцевой топологии является то, что, если какое-либо отдельное соединение в кольце разрывается, затрагивается вся сеть. Кольцевые топологии могут использоваться либо в локальных сетях либо в глобальных. В прошлом кольцевая топология чаще всего использовалась в школах, офисах и небольших зданиях, где сети были небольшими. Однако сегодня кольцевая топология используется редко.

Преимущества топологии «кольцо»:

- все данные передаются в одном направлении, что снижает вероятность коллизий пакетов;

- не нужен сетевой сервер для управления сетевым соединением между каждой рабочей станцией;

- данные могут передаваться между рабочими станциями на высоких скоростях;

- дополнительные рабочие станции могут быть добавлены без ущерба для производительности сети.

Недостатки топологии «кольцо»:

- все данные, передаваемые по сети, должны проходить через каждую рабочую станцию ​​в сети, что может сделать ее медленнее, чем звездная топология;

- на всю сеть будет оказано влияние, если одна рабочая станция выключится.

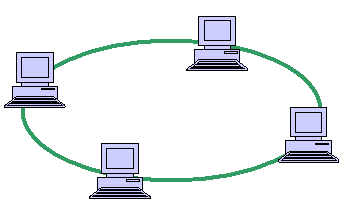


Рисунок 2.4 – Схема соединения «кольцо»

Анализируя основные топологии решено использовать в этом проекте топологию типа «звезда». Центральное устройство управляет движением пакетов в сети. Каждый компьютер через сетевую карту подключается к коммутатору отдельным кабелем.

**2.2 Выбор технологии локальной вычислительной сети**

Существует несколько разновидностей технологий локальной вычисли-тельной сети: Ethernet, Token Ring и FDDI.

Ethernet является самой популярной технологией LAN физического уровня, используемой сегодня. Технология Ethernet определяет максимальное количество узлов, максимальное расстояние между узлами, скорость передачи, которую можно ожидать и обеспечивает основу для передачи данных. Стандартная сеть Ethernet может передавать данные со скоростью до 10 мегабит в секунду (10 Мбит/с). Институт инженеров электротехники и электроники разработал стандарт Ethernet, известный как стандарт IEEE 802.3. Этот стандарт определяет правила настройки сети Ethernet, а также определяет, как элементы сети Ethernet взаимодействуют друг с другом. Придерживаясь стандарта IEEE, сетевое оборудование и сетевые протоколы могут эффективно взаимодействовать.

Стандарт Fast Ethernet (IEEE 802.3u) был установлен для сетей Ethernet, которым требуется более высокая скорость передачи данных. Этот стандарт повышает скорость Ethernet с 10 Мбит/с до 100 Мбит/с при минимальных изменениях существующей структуры кабеля. Существует три вида Fast Ethernet: 100BASE-ТХ для использования неэкранированной витой пары начиная с пятой категории; 100BASE-FX для использования оптоволоконного кабеля; 100BASE-Т4 использует два дополнительных проводника для использования неэкранированной витой пары начиная с третьей категории.

Token Ring – это еще одна форма конфигурации сети. Она отличается от Ethernet тем, что все сообщения всегда передаются в одном направлении по кольцу. Сети Token Ring последовательно передают «токен» каждому подключенному устройству. Когда токен поступает на конкретный компьютер (или устройство), получателю разрешается передавать данные в сеть. Поскольку только одно устройство может передавать в любой момент времени, то коллизий не происходит. Однако преимущества Token Ring имеют свою цену. Стоимость компонентов, как правило, выше, а сами сети считаются более сложными и сложными в реализации.

 Волоконно-оптический распределенный интерфейс передачи данных (Fibre Distributed Data Interface или FDDI) обычно реализуется как двойное кольцо передачи токенов в кольцевой топологии. Двойное кольцо состоит из первичного и вторичного колец. Основное кольцо предназначено для передачи данных. Вторичное кольцо передает данные в противоположном направлении, но чаще резервируется в качестве резервной кольца на случай, если первичное кольцо выходит из строя. Это обеспечивает степень отказоустойчивости, необходимую для сетевых магистралей. В случае сбоя в первичном кольце FDDI автоматически перенастраивается, чтобы использовать вторичное кольцо. Станции подключаются к одному (или обоим) кольцам с помощью разъема медиаинтерфейса (MIC).

В FDDI используется технология передачи маркеров аналогичная в технологии сетей Token Ring. Станции FDDI генерируют маркер, который управляет последовательностью, в которой другие станции получат доступ к кольцу. Маркер проходит по кольцу, переходя от одного узла к другому. Когда станция хочет передать информацию, она захватывает маркер, передает столько кадров, сколько ей нужно, а затем высвобождает токен. В сети FDDI с двумя кольцами может быть до 500 станций. Максимальная окружность для кольца FDDI составляет 100 километров (или 200 километров для обоих объединенных колец), каждые 2 километра должен быть ретранслятор. Мосты или маршрутизаторы используются для подключения магистральной сети FDDI к локальным сетям Ethernet или Token Ring. По этим причинам FDDI не часто используется в качестве решения для глобальной сети (WAN).

В таблице 3.1 представлены сравнительные характеристики наиболее распространенных технологий локальной вычислительной сети.

Таблица 3.1 – Сравнительные характеристики технологий ЛВС.

|  |  |  |  |
| --- | --- | --- | --- |
| **Характеристики** | **Ethernet** | **Token Ring** | **FDDI** |
| Скорость передачи | 10 (100) Мбит/с | 16 Мбит/с | 100 Мбит/с |
| Топология | шина/звезда | кольцо/звезда | кольцо |
| Среда передачи | коаксиальный кабель, витая пара, оптоволокно | витая пара, оптоволокно | оптоволокно, витая пара |
| Максимальная протяженность сети | 2,5 км | 4 км | 100 км |
| Максимальное количество узлов | 1024 | 260 | 500 |
| Максимальное расстояние между узлами | 2500 м | 100 м | 2000 м |

Учитывая характеристики выше рассмотренных технологий для построения локальной вычислительной сети научно-медицинской организации выбрана технология Ethernet. Ethernet полностью удовлетворяет по скорости передачи данных 10 Мбит/сек. Данная технология в качестве среды передачи данных позволяет использовать витую пару. Соответственно не требуется больших денежных затрат. Для соединения далеко находящихся друг от друга сетевых узла без проблем можно использовать оптическое волокно.

Структурная схема представлена в приложении «А».

# 3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

**3.1 Обоснование выбора сетевой операционной системы**

Сетевая операционная система – это операционная система, предназначенная исключительно для поддержки рабочих станций, совместного использования базы данных, общего доступа к приложениям и совместного доступа к файлам и принтерам между несколькими компьютерами в сети. Операционная система, работающая в сети организации имеющей нескольких отделов и удаленных друг от друга зданий, должна обеспечивать для сотрудников доступ к файлам других отделов. В настоящее время наибольшее распространение получили две основные сетевые ОС – UNIX и Windows.

Так как научно-исследовательская организация содержит менее 50 устройств, то выбрана сетевая операционная система Windows Server 2016 Essentials. Так как Essentials это редакция Windows Server, специально предназначенная для использования в небольших организациях. Установка Windows Server 2016 Essentials будет происходить на физический сервер. На сервере должно быть не более двух физических процессоров и максимум 64 Гб оперативной памяти. Windows Server 2016 Essentials при необходимости можно интегрировать с облачными сервисами Microsoft, такими как Azure или Office 365. В рамках администрирования компьютерное сети организации можно оперативно посмотреть текущее состояние сервера – количество пользователей и устройств, общие папки, состояние резервного копирования. Есть возможность получить отчет о состоянии сервера. Можно управлять пользователями и группами (создавать, удалять) а также настраивать политику паролей (длина, сложность). При условиях роста научно-исследовательской организации, нужно помнить об ограничениях операционной системы Windows Server Essentials, изменить лимиты невозможно, но можно изменить саму редакцию операционной системы.

**3.2 Обоснование выбора серверного оборудования**

Согласно требованиям научно-исследовательской организации в качестве сервера был выбран сервер Cisco Business Edition 6000 (BE6000) (см. рис 3.1). Данный сервер предоставляет сотрудникам полный набор инструментов для работы: голосовая связь, видео, обмен сообщениями, конференц-связь, видеоконференции.

Cisco Business Edition 60000 разработан для организаций с числом сотрудников от 25 до 1000, что вполне подходит для нашей организации. При необходимости можно легко увеличить количество поддержки дополнительных пользователей.



Рисунок 3.1 – Сервер Cisco Business Edition 6000

*Источник: https://www.cisco.com/c/dam/global/ru\_ru/assets/images/ cmbe6000.jpg*

Cisco Business Edition 6000 использует технологии виртуализации и автоматизации типовых операций администрирования, поддерживает дружественный интерфейс пользователя (на русском языке). Многолетний опыт компании Cisco в области построения отказоустойчивых систем связи в распределенной среде, позволит организации заметно сократить стоимость владения системой за счет сокращения времени, необходимого для ее обслуживания и времени простоев, связанных с ошибками эксплуатации. Модель BE6000M: поддерживает четыре варианта приложения для совместной работы плюс один для предоставления на одной виртуализированной серверной платформе; максимальная количество пользователей – 1000, максимальная количество устройств – 1200 устройств. На официальном сайте компании Cisco можно найти руководство по настройке сервера Cisco Business Edition 6000 [11].

**3.3 Обоснование выбора клиентского оборудования**

В качестве ноутбуков выбран Lenovo ThinkPad T470 (см. рис. 3.2). Данный ноутбук специально создан для бизнеса и организаций. Благодаря мощному процессору и возможности функционирования без подзарядки до 18 часов удобно работать в любом месте. Диагональ ноутбука 14-дюймов. В ноутбуке используются самые современные технологии: твердотельный накопитель, сканер отпечатков пальцев. Все это необходимо для надежности ThinkPad. Благодаря высокому быстродействию и производительности процессоров Intel Core 7-го поколения ноутбук Lenovo ThinkPad T470 позволяет переключаться между любимыми приложениями в считанные секунды. Высокоскоростной твердотельный накопитель отличается повышенной производительностью, открытия и передачи файлов происходит со скоростью примерно 200 МБ/с. Накопитель характеризуется пониженным шумом, повышенной прочностью, надежностью и безопасностью. Благодаря сверхскоростной технологии подключения LTE-A (4G) ноутбук T470 позволяет быстро получить доступ ко всем данным и приложениям в облаке даже при отсутствии сетей wi-fi. Ноутбук T470 поставляется с установленной ОС Microsoft Windows 10 Pro Edition.



Рисунок 3.2 – Ноутбук Lenovo ThinkPad T470

*Источник: https://www.lenovo.com/medias/lenovo-laptop-thinkpad-t470-gallery-03.jpg*

На все ноутбуки и настольные компьютеры нужно установить пакет офисных приложений Microsoft Office 2013 RUS, из которого наиболее важными для работы научно-исследовательской организации являются программы Microsoft Word (работа с текстовыми документами) и Microsoft Outlook (работа с электронной почтой, планировщик заданий). Программное обеспечение необходимое для работы в сфере медицины устанавливает разработчик данного программного обеспечения.

Для работы необходимы планшетные компьютеры. В качестве планшетных компьютеров выбраны Huawei MediaPad M3 lite10. В планшете Huawei MediaPad M3 lite10 обеспечивает надежную защиту информации с помощью отпечатков пальцев с поддержкой жестов управления. Режим защиты зрения позволяет комфортно читать с планшета в ночное время. Благодаря своей энергоэффективности, планшет потребляет меньше энергии, за счет чего снижается негативное воздействие на окружающую среду.

Для связи сотрудников (вышестоящих по должности) выбран мобильный телефон Huawei P20. Данным мобильный телефон имеет мощную батарею 3400 мА/ч, поддерживает функцию безопасной быстрой зарядки Huawei SuperCharge. Технология быстрой зарядки помогает зарядить устройство, даже когда у сотрудника совсем мало времени. Технология Huawei Share 2.0 обеспечивает мгновенную передачу фото и файлов между смартфонами Huawei и компьютерами (Windows или MAC) без подключения кабеля, блокировки устройств и других дополнительных действий.

**3.4 Обоснование выбора активного сетевого оборудования**

В качестве маршрутизатора выбран Cisco серии 4000, ISR 4331 (см. рис 3.3). Универсальное решение для построения корпоративной сети.



# Рисунок 3.3 – Маршрутизатор Cisco 4331 Integrated Services Router

*Источник: https://www.cisco.com/c/dam/en/us/support/docs/SWTG/*

*ProductImages/Routers-4331-ISR\_frnt\_rt-1000.jpg*

В данном маршрутизаторе есть технология как IWAN. С помощью данной технологии осуществляется динамическая маршрутизация трафика приложений с выбором оптимального канала связи. Это позволяет гарантировать требуемые производительность приложений и конфиденциальность передаваемых данных. В условиях стремительного развития организации, роста трафика данных и перехода большинства бизнес-процессов в онлайн, оборудование предоставляет необходимые скорость, масштабируемость и сервисы. Маршрутизатор подходит для подключения офисов с требованиями к пропускной способности от 50 до 300 Мбит/с. В данном маршрутизаторе можно при необходимости задействовать на одной платформе такие актуальные технологии, как VPN, межсетевой экран, контроль приложений, выбор маршрута, оптимизация WAN, передача голоса, видеонаблюдение. Кроме того, оборудование обеспечивает интеллектуальное распознавание и управление трафиком сетевых приложений в корпоративной сети благодаря технологии Application Visibility and Control. Конфигурация маршрутизаторов приведена в приложении «Д».

В качестве коммутатора выбран Cisco Catalyst 2960-24TT (см. рис. 3.4). Это коммутатор второго уровня с фиксированной конфигурацией, которое позволяет подключать рабочие станции к сетям Fast Ethernet и Gigabit Ethernet на скорости среды передачи, удовлетворяя растущие потребности в пропускной способности на периферии сети. Данный коммутатор ориентирован в первую очередь на предприятия малого и среднего бизнеса, а также филиалы крупных компаний для решения задачи реализации уровня доступа к сети. Коммутатор обеспечивает широкий набор функций обеспечения безопасности и качества обслуживания, а также управление полосой пропускания. Для упрощения задачи конфигурирования в коммутаторах серии Catalyst 2960 предусмотрена



# Рисунок 3.4 – Каммутатор Cisco Catalyst 2960-24TT

*Источник: https://www.cisco.com/c/dam/en/us/support/docs/SWTG/*

*ProductImages/switches-catalyst-2960-24tt-l-switch.jpg*

функция Smartports, позволяющая выполнить основные настройки порта коммутаторов, основываясь на его назначении. Cisco Catalyst 2960 обеспечивают потребность в передаче данных со скоростью 100 Мбит/сек и 1 Гбит/сек, позволяют использовать LAN сервисы, например, для сетей передачи данных, построенных в филиалах корпораций.

Настроим port security на интерфейсе коммутара, к которому подключен сервер. Включая port security на интерфейсе, мы предотвратим неавторизованный доступ к серверу, если злоумышленник подключит свое устройство к этому интерфейсу.

По умолчанию, switchport security отключен на всех интерфейсах. Включить port security можно только на интерфейсе, настроенном как access интерфейс. Затем необходимо включить защиту портов с помощью команды «switchport port-security». Далее следует указать, сколько MAC-адресов коммутатор может иметь на одном интерфейсе одновременно. Команда для настройки этого следующая «switchport-security maximum N» (где N может быть от 1 до 6272). Далее вводом команду «switchport port-security violation protect». В данном случае при нарушениях, от неизвестного MAC адреса пакеты отбрасываются, но при этом никаких сообщений об ошибках не генерируется. Пример конфигурации port security на интерфейсе идущему к серверу:

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security maximum 1

Switch(config-if)# switchport port-security mac-address 00-d0-ba-11-21-31

Switch(config-if)# switchport port-security violation protect

Switch(config-if)#end

В качестве ADSL2+ модема выбран Linksys by Cisco ADSL2+ Modem Router AG300-9С. Этот модем обеспечивает компьютеры высокоскоростным подключением к интернету, а также доступом к локальным ресурсам, включая файлы и принтеры. Модем позволяет устройствам в сети взаимодействовать друг с другом. Чтобы защитить данные, модем оснащен расширенным брандмауэром для защиты от интернет-злоумышленников. Исходящие пакеты данных могут быть защищены мощным шифрованием. Вы можете получить доступ к одному принтеру с разных компьютеров и получить доступ к данным, расположенным на жестком диске другого компьютера. Linksys рекомендует использовать установочный компакт-диск для первоначальной установки модема.

Настройку Linksys by Cisco ADSL2+ можно произвести следующим образом. Для начала получим доступ к веб-утилите. Чтобы получить доступ к веб-утилите, нужно запустить Internet Explorer и ввести шлюз по умолчанию IP-адрес 192.168.1.1, в поле Address. Затем нажать Enter. Появится экран входа в систему. Ввести admin (имя пользователя по умолчанию) в поле User Name и admin (пароль по умолчанию) в поле Password. Затем нажать кнопку OK. Появится экран-вкладка с основными настройками. На этой вкладке можно изменить общие параметры модема. С дальнейшими настройками модема можно ознакомится в руководстве пользователя [13].

**3.5 Выбор аппаратных средств для реализации беспроводного**

**решения**

В небольших организациях для доступа к сети wi-fi очень хорошо могут применяться решения, рассчитанные на небольшое количество точек доступа, редко данный уровень решения имеет более 20 точек доступа, но с централизованной архитектурой.

Модель точки доступа Cisco AIR-AP1252 – точка доступа корпоратив-ного класса, поддерживающая стандарт IEEE 802.11n. Предлагает комбинированные скорости передачи данных до 600 Мбит/с, чтобы предоставить пользователям мобильный доступ к приложениям для передачи данных, голоса и видео с высокой пропускной способностью независимо от их местоположения. Надежная точка доступа Cisco AIR-AP1252 представляет собой модульную платформу, которая может быть легко модернизирована для поддержки различных беспроводных возможностей. Эта модульность позволяет предприятиям с уверенностью внедрять существующие беспроводные технологии уже сейчас, инвестиции в сетевые технологии будут расширяться для поддержки новых и будущих беспроводных технологий. Точка доступа была специально разработана для поддержки требований по мощности, пропускной способности и другим характеристикам высокоскоростных технологий WLAN, включая 802.11n. В настоящее время точки доступа поддерживает модули 2,4 ГГц и 5 ГГц, совместимые со стандартом IEEE 802.11n. По мере развития технологий точка доступа гибка для поддержки будущих радиомодулей, предназначенных для предоставления интеллектуальных радиочастотных услуг, что дополнительно повышает производительность и надежность беспроводной сети. Cisco AIR-AP1252 – это



# Рисунок 3.5 – Точка доступа Cisco AIR-AP1252

*Источник: https://images-na.ssl-imagesamazon.com/images/I/41uNmR3dVhL.jpg*

надежная точка доступа, предназначенная как для офисных помещений, так и для фабрик, складов, больниц и крупных торговых предприятий, которым требуется универсальность точек доступа. С интерфейсом Gigabit Ethernet (10/100/1000) Cisco AIR-AP1252 обеспечивает пропускную способность линии для высокоскоростных технологий WLAN, таких как 802.11n. Точка доступа обеспечивает гибкость как встроенных, так и локальных вариантов питания.

Cisco AIR-AP1252 поддерживает стандартные отраслевые протоколы беспроводной безопасности, в том числе 802.11i, защищенный доступ wi-fi (WPA), WPA2 и 802.1X, а также многочисленные типы протоколов расширяемой аутентификации (EAP). Точка доступа обеспечивает аппаратно-ускоренное шифрование Advanced Encryption Standard (AES), разработанное для удовлетворения самых строгих требований к шифрованию на уровне предприятия и правительства без ущерба для производительности. Как часть решения Cisco Secure Wireless, точки доступа Cisco AIR-AP1252, работающие с LWAPP, обеспечивают комплексное предотвращение и обнаружение вторжений проводных и беспроводных сетей. Каждая точка доступа может сканировать радиочастотную среду и сообщать о подозрительной или несанкционированной беспроводной активности, что позволяет предприятиям создавать комплексную защиту от угроз в стандартах 802.11a/b/g и 802.11n. Это позволяет сети полностью устранить угрозу от атак. Если точка доступа обнаружит злонамеренную атаку, будет сгенерирован сигнал тревоги, о котором администратор сети сообщит.

Далее опишем основные этапы конфигурации точки доступа. Для получения подробной информации нужно обратится к руководству пользователя [13].

На 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 несанкцио-нированного 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

Шаг 1. Открыть интернет-браузер. Необходимо использовать Microsoft Explorer (версия 5.x или более поздней версии).

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

Шаг 3. Ввести имя пользователя в поле User Name.

Шаг 4. Ввести пароль в поле Password и нажать Enter.

Шаг 5. Нажать System Software. Откроется страница System Software.

Шаг 6. Нажать System Configuration. Откроется страница System Configuration.

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

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

**3.5.1 Расчет характеристик проектируемой беспроводной сети**

По заданию в научно-медицинской организации должно быть беспроводное подключение устройств к сети, для это рассчитаем количества точек доступа необходимого для внедрения в проектируемую сеть организации.

Для поддержки передачи данных необходимо рассчитать требуемую производительность в расчете на одного клиента. Зная максимально достижимую теоретически рассчитанную пропускную способность стандарта 802.11n до 300 Мбит/с, но в реальных условиях пропускная способность и площадь зоны покрытия сети зависят от многих факторов: от помех, наличия препятствий, степени загрузки сети wi-fi. Поэтому реальная производительность точки доступа гораздо ниже и будет составлять не более 50 Мбит/с. Для передачи данных, использования различных приложений нужно выделить каждому пользователю беспроводной сети канал с пропускной способностью не менее 2 Мбит/с.

Зная, как рассчитывается пропускная способность канала для одно соединение

*,* (3.1)

где – скорость передачи данных;

– количество поддерживаемых подключений.

Из формулы 3.1 рассчитаем количество подключений к одной точке доступа,

*,* (3.2)

Следовательно, из формулы 3.2 мы получим количество пользователей беспроводной сети, которых сможет одновременно поддерживать одна точка доступа. При этом учтем что в нашем случае пропускная способность точки доступа равна , а среднее количество пользователей в первом здании научно-исследовательской организация равно 9 и 10 во втором здании. По формуле (3.2), имеем:

Для того чтобы рассчитать необходимое количество точек доступа для каждого здания нашей организации, воспользуемся формулой

, (3.3)

где – общее количество подключений ()

– количество подключений, поддерживаемых одной точкой доступа.

Для расчета количества точек доступа нам нужно преждевременно знать общее количество пользователей.

В проектируемой сети научно-медицинской организации количество пользовательского оборудования состоит только клиентских станций

(3.4)

где – количество пользователей сети (согласно заданию, для первого здания и для второго здания);

Возвратившись к формуле 3.3 можем рассчитать количество точек доступа, необходимых для каждого здания:

,

.

Согласно проведенным расчетам, для обеспечения беспроводного подключения пользователей к сети нам потребуется 1 точка доступа для обеспечения работы 9 пользователей в первом здании и 1 точка доступа для обеспечения работы 10 пользователей во втором здании с минимальной скоростью 2 Мбит/с.

**3.6 Информационная безопасность локальной компьютерной сети**

Для информационной безопасности на компьютеры будет установлено программное обеспечение от компании Symantec. Необходимость защиты данных и систем требует нового подхода. Традиционного антивируса недостаточно для защиты систем. Symantec является единственным поставщиком, объединяющим безопасность настольных компьютеров, ноутбуков, серверов и электронной почты. Программное обеспечение компании Symanteс обеспечит многоуровневую защиту конечных устройств, почтовых систем и интернет-шлюзов. Защитит конфиденциальные данные на конечных устройствах, почтовом сервере и шлюзе обмена сообщениями с помощью передовых технологий фильтрации содержимого и предотвращения потери данных. Заблокирует 99% спама и защитит организацию от спама и фишинговых угроз с помощью передовой в отрасли технологии защиты от спама.

# 3.7 Схема адресации сети организации

Главным вопросом при объединение в единую сеть организации является какую схему IP-адресации лучше всего реализовать в данной ситуации.  
В зависимости от типа установленного соединения (Интернет, VPN) ответ на этот вопрос может отличаться. Схема IP-адресации, которую используют сегодня организации, основана на IPv4. Компании используют общедоступные IP-адреса, которые назначаются Интернет-провайдером, для доступа в Интернет. Как правило, эти общедоступные IP-адреса используются за пределами организации. Путем преобразования (брандмауэрами, NAT, прокси) организации используют большое количество частных IP-адресов.

Внутренние IP-адреса или частные адреса были реализованы IETF (Internet Engineering Task Force). В определяется три блока адресов:

* 10.0.0.0/8;
* 172.16.0.0/12;
* 192.168.0.0/16.

Эти адреса могут быть использованы любой организацией. Их единственным ограничением является то, что они не маршрутизируются через Интернет. Однако эти адреса можно использовать в одной сети или разделить на несколько подсетей. Эти подсети могут использоваться для подключения различных организационных единиц, безопасности и упрощения администрирования.

Организации, которые продолжают полагаться исключительно на IPv4 и не планируют внедрять IPv6 в ближайшем будущем, рискуют столкнуться с множеством бизнес-задач, от увеличения затрат и ограниченной функциональности до ограничения критических возможностей роста на развивающихся рынках. Единственным долгосрочным решением этой проблемы и последующих сбоев в бизнесе является принятие IPv6, обеспечивающего практически неограниченное количество адресов. Многие организации начинают внедрять IPv6, часто начиная с внедрения IPv6 на своих почтовых и веб-серверах. Это, по крайней мере, позволяет общаться с внешним миром по обоим протоколам. Некоторые также включают IPv6 во внутренних сетях, включая корпоративные глобальные сети и центры обработки данных. В этих случаях предприятия используют конструкции с двумя стеками.

Схема адресации сети IPv4 и IPv6 приведена в таблице 3.2 и таблице 3.3 соответственно.

Таблица 3.2 – Схема адресации сети IPv4

|  |  |  |  |
| --- | --- | --- | --- |
| Устройство | Сеть | Используемый/-e адрес/-а | Комментарий |
| FTP Server | 192.168.1.0/25 | 192.169.1.10 |  |
| LaboratoryA PC1-PC4, Director Laptop, Director | 192.168.1.0/25 | 192.169.1.1-192.169.1.254 | DHCP, исключая адреса 192.169.1.1, |
| Smartphone, Tablet 1-2, Printer, Phone 1-2, Laptop 1-2 |  |  | 192.169.1.10 |
| Router 0 (внутренний интерфейс) | 192.168.1.0/25 | 192.169.1.1 |  |
| Router 0 (внешний интерфейс) | 210.210.1.0/25 | 192.169.1.2 |  |
| Router 1 (внутренний интерфейс) | 192.168.2.0/25 | 192.169.2.1 |  |
| Router 2 (внешний интерфейс) | 210.210.2.0/25 | 192.169.2.1 |  |
| LaboratoryB PC1-PC8, Laptop 4-9, Printer, Phone 4-7 | 192.168.2.0/25 | 192.169.1.1-192.169.1.254 | DHCP, исключая адрес 192.169.2.1 |

Таблица 3.3 – Схема адресации сети IPv6

|  |  |  |  |
| --- | --- | --- | --- |
| Устройство | Сеть | Используемый/-e адрес/-а | Комментарий |
| FTP Server | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:a::/64 | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:a::10 |  |
| LaboratoryA PC1-PC4, Director Laptop, Director | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:A::/64 | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:a: 0000:0000:0000:0000 - | DHCP, исключая |

# *Продолжение таблицы 3.3*

|  |  |  |  |
| --- | --- | --- | --- |
| Устройство | Сеть | Используемый/-e адрес/-а | Комментарий |
| Smartphone, Tablet 1-2, Printer, Phone 1-2, Laptop 1-2 |  | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:a:  ffff:ffff:ffff:ffff | адреса [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:a::10, [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:a::1 |
| Router 0 (внутренний интерфейс) | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:a::/64 | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:a::1 |  |
| Router 0 (внешний интерфейс) | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:b::/64 | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:b::1 |  |
| Router 1 (внутренний интерфейс) | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:d::/64 | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:d::1 |  |
| Router 2 (внешний интерфейс) | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:c::/64 | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:c::1 |  |
| LaboratoryB PC1-PC8, Laptop 4-9, Printer, Phone 4-7 | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:d::/64 | [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:d: 0000:0000:0000:0000 - [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:d: ffff:ffff:ffff:ffff | DHCP, исключая адрес [2a0d:2d00](https://apps.db.ripe.net/db-web-ui/#/lookup?source=ripe&key=2a0d:2d00::/32&type=inet6num): 2268:d::1 |

бельные системы по-прежнему жизненно важны для [IT-инфраструктуры](https://tcitechs.com/it-infrastructure/) каждой организации.

# 4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ

# СИСТЕМЫ

В последние годы многие бизнес-технологии стали беспроводными, но структурированные кабельные системы по-прежнему жизненно важны для [IT-инфраструктуры](https://tcitechs.com/it-infrastructure/) каждой организации.

Структурированная кабельная система – это [система кабелей, проводов и другого оборудования,](http://www.network24.co.uk/structuredcabling101.html) которая соединяет инфраструктуру систем связи организации. Это могут быть [телефоны](http://blog.tcitechs.com/blog/what-are-the-benefits-of-using-voip-for-business), видеокамеры, компьютеры и центры обработки данных.

Структурированная кабельная система имеет много преимуществ.

Во-первых, легко масштабируется. Поскольку структурированные кабельные системы аккуратно размещают провода таким образом, что ими легко управлять, никогда не возникает проблем при добавлении новых машин или технологий в IT-среду. Если организация растет, и возникает необходимость добавить новые компьютеры, это можно сделать, не прерывая ежедневных рутин.

Во-вторых, время простоя сети меньше. Неструктурированные кабельные системы с запутанными проводами [часто вызывают проблемы с подключением](http://www.cablinginstall.com/articles/2016/06/5-damaging-problems.html), которые могут привести к простою сети и снижению производительности. Тщательно спланированная кабельная система обеспечит правильную работу сети.

В-третьих, для решения возникших проблем в сети потребуется меньше времени. Независимо от того, насколько хорошо организована кабельная система, проблемы все равно могут возникать. Природа аппаратного оборудова-ния [время от времени дает сбой](http://searchservervirtualization.techtarget.com/tip/Plan-for-hardware-failure-because-you-cant-avoid-it). Однако структурированная кабельная система делает менее трудоемким [поиск проблемы и ее решение](http://blog.tcitechs.com/blog/what-does-an-it-support-company-even-do).

В-четвертых, эстетически приятнее. Придя в офис на встречу потенциальный клиент видит кучу запутанных проводов в офисе. Это выглядит не очень красиво. Заранее спланированные кабельные системы часто скрыты от глаз. Если они видны, то они аккуратно связаны и подключены к соответствующим машинам.

В-пятых, безопасность. С неструктурированными кабельными системами, есть более [высокий шанс](https://www.globalquestinc.com/what-you-may-not-know-about-structured-cabling) пожара, поражение электрическим током.

В-шестых, лучшая окупаемость инвестиций. Благодаря оптимальной конструкции сетевой структурированной кабельной системы, требуется меньше обслуживания и замены. Организация может сэкономить на проводке и кабелях.

В-седьмых, работает с интернетом вещей. В общем [Интернет вещей](http://blog.tcitechs.com/blog/what-is-the-internet-of-things-and-why-is-it-a-security-threat) (IoT) это подключение любого устройства, будь то смартфон или умный автомобиль, к Интернету. IoT-устройства становятся все более распространенными на рабочем месте. Структурированные кабельные системы могут быть объединены с IoT для [достижения следующих преимуществ](http://www.rahisystems.com/data-center-power/why-structured-cabling-is-critical-to-the-iot/) как автоматизации ключевых бизнес-операций, кибер-безопасности.

Структурированная кабельная система с каждым днем преобладает над традиционным двухточечным подходом. Старые промышленные системы, многие из которых часто основаны на двухточечном подключении, уступили место повсеместной технологии Ethernet. Внедрение новых технологий спровоцировало увеличение цифровых устройств на производственных площадках, увеличился спрос на более высокую производительность, пропускную способность и надежность, обеспечиваемые высоко структуриро-ванной, основанной на стандартах сетевой инфраструктурой. Промышленные скорости передачи данных выросли с килобит в секунду до мегабит в секунду и даже гигабит в секунд. Для эффективной работы с такими скоростями – обеспечения бесперебойной работы и снижения затрат – современные сети нуждаются в хорошо спроектированной и структурированной кабельной системе.

Структурированные кабельные системы также способны развиваться в будущем. Промышленные скорости передачи данных в конечном итоге могут превзойти 10-гигабит в секунду. Между тем, промышленные процессы и машины становятся все более интеллектуальными, используя передовые контрольно-измерительные приборы, датчики и беспроводные технологии. По всем этим и многим другим причинам структурированные кабельные системы заменяют зачастую специальный подход «точка-точка». При структурированно кабельной системе удовлетворяются все текущие и будущие потребности в промышленной связи, включая передачу голоса, данных и видео. Чтобы получить все преимущества структурированной кабельной системы, необходим не менее систематический подход к спецификации, установке, тестированию и обслуживанию сетей на предприятии.

Структурированные кабельные системы включают в себя пять подсистем на объекте: точка демаркации – граница между сферой ответственности Интернет-провайдера и потребителя; телекоммуникационное помещение, в котором находится сетевое оборудование и точки консолидации; вертикальная разводка, которая соединяет оборудование в различных помещениях, как правило, между различными этажами; горизонтальная проводка, соединяет оборудование помещения с отдельными рабочими зонами, обычно на одном этаже; рабочая зона – это место где пользовательское оборудование подключается через розетки к горизонтальной кабельной системе.

Высокоэффективный способ развертывания решений Ethernet по всей архитектуре заключается в физическом распределении кабельных трасс с использованием зональной кабельной архитектуры для всего предприятия. Зональная разводка позволяет объединять системы объекта с кабельными трассами Ethernet по мере их проектирования. Эти системы объединяются в рамках общей трассы, а затем заканчиваются внутри зонных шкафов, распределенных по всему предприятию.

**4.1 Выбор категории кабеля «витая пара» для реализации сети**

Для начала рассмотрим два вида витой пары UTP и STP. UTP – неэкранированная витая пара, является наиболее распространенным видом. В данном виде витой пары провода находятся внутри резиновой втулки без какой-либо защиты. STP означает экранированную витую пару. При этом виде витой пары используется слой фольги который защищает сигналы от электрических помех. STP дороже, но сигнал не ухудшается так сильно при большом расстоянии передачи. Теоретически все кабели UTP должны поддерживать длину до 100 метров между коммутаторами или хостами. Если нужно сделать более длинное соединение, то для этого понадобится коммутатор с питанием для удлинения при необходимости. Так же работоспособность зависит от качества: качественные кабели могут работать дольше, а плохо изготовленные – значительно короче.

Витая пара состоит из восьми проводников, скрученных и разделенных на 4 пары. Каждый проводник обозначен сплошным цветом с соответствующим им полосатым белым. Теперь рассмотрим основные категории кабеля «витая пара»: Cat 5, Cat 5e, Cat 6.

Cat 5e («e» обозначает «расширенный») – эта категория «витой пары», предназначена для уменьшения перекрестных помех, и обеспечивающая скорость до 1000 Мбит/с или широко известный «Gigabit Ethernet». Cat 5e – самый распространенный вид кабеля, который можно найти сегодня в продаже, и он вполне подходит для домашнего использования. Для гигабитных скоростей используются все четыре пары кабеля. Cat 6 теоретически может обеспечить скорость до 10000 Мбит/с – при максимальной длине около 37 метров, и этого достаточно для использования в небольших офисах. Данная категория витой пары прекрасно подойдет также для объединения в единую сеть офиса находящего на нескольких этажах. Cat 6 полностью совместим с существующими категориями Cat 5e и Cat 5.  Пары проводников витой пары категории Cat 6 свиты с более частым шагом и имеют пластиковый стержень разделитель, проходящий через центр, уменьшая перекрестные помехи и обеспечивая более высокие скорости. Cat 6a – это новый стандарт, разработанный для поддержки 10 Гбит/с на длине 100 метров.

Для реализации сети научно-медицинской организации решено использовать экранированную витую пару категории Cat 5e.

План этажа первого здания представлен в приложении «В».

План этажа второго здания представлен в приложении «Г».

**ЗАКЛЮЧЕНИЕ**

В области информационных технологий одной из самых важных и интересных задач на сегодняшний день является разработка и внедрение корпоративных информационных сетей. С быстрыми темпами развития сетевых технологий возникает необходимость в их использовании и внедрении. Использование современных информационных технологий организациями дает большое конкурентное преимущество, которое можно наблюдать на мировом рынке, и является сильным аргументов для привлечения новых клиентов.

В ходе курсовой работы реализована локальная компьютерная сеть научно-медицинской организации. Были поставлены и решены задачи такие как, выбор сетевой архитектуры, конфигурация сетевого оборудования, рассчитаны параметры беспородной сети, а также вопросы безопасности сети. Согласно заданию на курсовую работу спроектирована локальная вычислительная сеть организации, располагающаяся в двух зданиях, удаленных друг от друга. Все сетевое и коммутационное оборудование должно находятся в коммутационных шкафах. С помощью подключения источников бесперебойного питания, оборудование защищено от пропадания сетевого напряжения. При использовании в организации беспроводной сети создаются существенные преимущества, такие как мобильность при выходе в интернет возможность подключения ноутбуков, персональных компьютеров, смартфонов через wi-fi, и что не мало важно, возможность видоизменять сеть, без каких-либо трат. Для каждой организации компьютерная локальная сеть является необходимым и немаловажном сегодня атрибутом. В конечном счете, каждая организация выбирает свою форму сети, для того или иного случая, которая будет наиболее подходить для данной организации.

ПРИЛОЖЕНИЕ А

*(обязательное)*

Локальная компьютерная сеть.

Схема СКС структурная

ПРИЛОЖЕНИЕ Б

*(обязательное)*

Локальная компьютерная сеть.

Схема СКС функциональная

ПРИЛОЖЕНИЕ В

*(обязательное)*

Здание первое.

План этажа

ПРИЛОЖЕНИЕ Г

*(обязательное)*

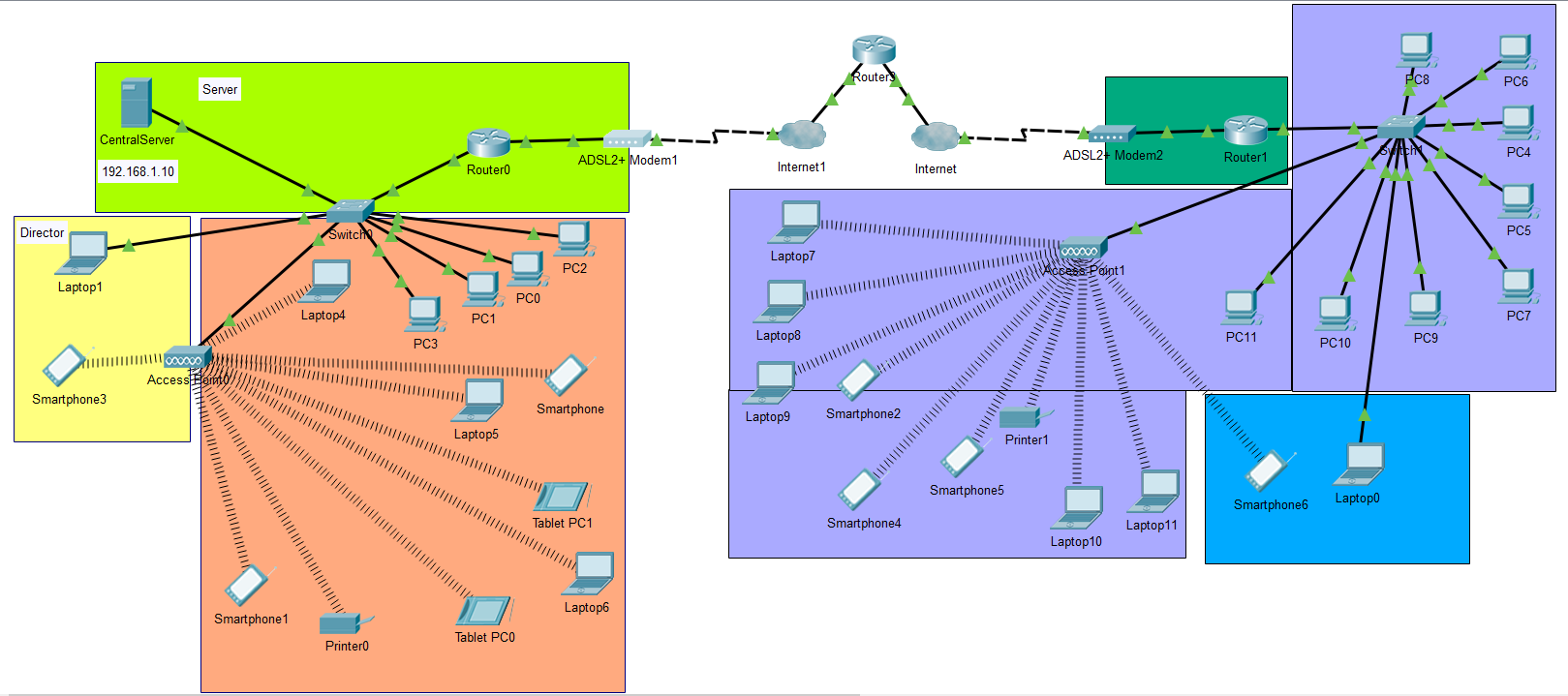
Здание второе.

План этажа

ПРИЛОЖЕНИЕ Д

*(рекомендуемое)*

Реализация проектируемой сети в Cisco Packet Tracer



ПРИЛОЖЕНИЕ Е

*(рекомендуемое)*

Конфигурация сетевого оборудования

**Router 0**

Current configuration : 1595 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname R0

!

ip dhcp excluded-address 192.168.1.1

ip dhcp excluded-address 192.168.1.10

!

ip dhcp pool office

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

dns-server 192.168.1.10

!

ip cef

ipv6 unicast-routing

!

ipv6 cef

!

crypto isakmp policy 1

encr 3des

hash md5

authentication pre-share

group 2

!

crypto isakmp key cisco address 210.210.2.2

!

crypto ipsec transform-set TS esp-3des esp-md5-hmac

!

crypto map CMAP 10 ipsec-isakmp

set peer 210.210.2.2

set transform-set TS

match address FOR-VPN

!

spanning-tree mode pvst

!

interface FastEthernet0/0

ip address 210.210.1.2 255.255.255.0

ip nat outside

duplex auto

speed auto

ipv6 address 2001:DB8:AAAA:B::1/64

ipv6 enable

crypto map CMAP

!

interface FastEthernet0/1

ip address 192.168.1.1 255.255.255.0

ip nat inside

duplex auto

speed auto

ipv6 address 2001:DB8:AAAA:A::1/64

ipv6 address autoconfig

ipv6 enable

!

interface Vlan1

no ip address

shutdown

!

router rip

!

ip nat inside source list FOR-NAT interface FastEthernet0/0 overload

ip classless

ip route 0.0.0.0 0.0.0.0 210.210.1.1

!

ip flow-export version 9

!

ipv6 route ::/0 2001:DB8:AAAA:B::2

!

ip access-list extended FOR-VPN

permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

ip access-list extended FOR-NAT

deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

permit ip 192.168.1.0 0.0.0.255 any

!

line con 0

!

line aux 0

line vty 0 4

login

end

**Router1**

Current configuration : 1526 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname Router

!

ip dhcp excluded-address 192.168.2.1

!

ip dhcp pool office

network 192.168.2.0 255.255.255.0

default-router 192.168.2.1

dns-server 192.168.1.10

!

ip cef

ipv6 unicast-routing

!

no ipv6 cef

!

crypto isakmp policy 1

encr 3des

hash md5

authentication pre-share

group 2

!

crypto isakmp key cisco address 210.210.1.2

!

crypto ipsec transform-set TS esp-3des esp-md5-hmac

!

crypto map CMAP 10 ipsec-isakmp

set peer 210.210.1.2

set transform-set TS

match address FOR-VPN

!

spanning-tree mode pvst

!

interface FastEthernet0/0

ip address 210.210.2.2 255.255.255.0

ip nat outside

duplex auto

speed auto

ipv6 address 2001:DB8:AAAA:C::1/64

ipv6 enable

crypto map CMAP

!

interface FastEthernet0/1

ip address 192.168.2.1 255.255.255.0

ip nat inside

duplex auto

speed auto

ipv6 address 2001:DB8:AAAA:D::1/64

ipv6 enable

!

interface Vlan1

no ip address

shutdown

!

ip nat inside source list FOR-NAT interface FastEthernet0/0 overload

ip classless

ip route 0.0.0.0 0.0.0.0 210.210.2.1

!

ip flow-export version 9

!

ipv6 route ::/0 2001:DB8:AAAA:C::2

!

ip access-list extended FOR-VPN

permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

ip access-list extended FOR-NAT

deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

permit ip 192.168.2.0 0.0.0.255 any

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

End

ПРИЛОЖЕНИЕ Ж

*(обязательное)*

Локальная компьютерная сеть.

Перечень оборудования, изделий и материалов

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Колисниченко, Д. Беспроводная сеть дома и в офисе / Д. Колисни-ченко. – Санкт-Петербург : БХВ-Петербург, 2009. – 456 с.

[2] Куроуз, Д. [Компьютерные сети: нисходящий подход : [перевод с английского] / Джеймс Куроуз, Кит Росс. – 6-е изд. – Москва : Э, 2016. – 907 с.](http://e-catalog.nlb.by/Record/BY-NLB-br0000145233)

[3] Новиков, Ю. В. Основы локальных сетей: курс лекций: учебное пособие для высших учебных заведений / Ю. В. Новиков, С. В. Кондратенко. – Москва: Интернет-университет информационных технологий, 2005. – 355 с.

[4] Одом, У. [Официальное руководство по подготовке к сертификационным экзаменам Cisco CCNА ICND2 200-101. Маршрутизация и коммутация: академическое издание / Уэнделл Одом. – Москва [и др.] : Вильямс, 2015. – 734с.](http://e-catalog.nlb.by/Record/BY-NLB-br0000439295)

[5] Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: учебное пособие для студентов высших учебных заведений, обучающихся по направлению 552800 "Информатика и вычислительная техника" и по специальностям 220100 "Вычислительные машины, комплексы, системы и сети" / В. Олифер, Н. Олифер. – 5-е изд. – Санкт-Петербург [и др.] : Питер, Питер Пресс, 2016. – 991 с.

[6] Семенов, A. Б. Волоконная оптика в локальных и корпоративных сетях. / А. Б. Семенов. – Москва : АйТи-Пресс, 2005. – 304 с.

[7] Сергеев, А. Основы локальных компьютерных сетей / А. Сергеев. – Санкт-Петербург : Лань, 2016. – 184 с.

[8] Технологии современных беспроводных сетей Wi-Fi: учебное пособие для студентов (адъюнктов), обучающихся по основным образовательным программам высшего образования по направлениям подготовки бакалавриата / магистратуры укрупненной группы специальностей и направлений подготовки 09.00.00 "Информатика и вычислительная техника" / Е. В. Смирнова [и др.]. – Москва : Издательство МГТУ, 2017. – 446 с.

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

[10] Cisco Networking Academy [Электронный ресурс]. – Cisco Networking Academy, 2018. – Режим доступа: https://www.netacad.com/.

[11] Cisco Business Edition 6000 Version 12.0 [Электронный ресурс] – Cisco, 2018. – Режим доступа: https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000-version-12-0/model.html#ConfigurationGuides.

[12] Linksys AG300 ADSL Gateway User [Электронный ресурс] – Linkys,

2018. – Режим доступа: http://downloads.linksys.com/downloads/userguide/

ag300-eu-ug-web,0.pdf

[13] Configuration Examples and TechNotes Cisco Aironet 1250 Series Access Point [Электронный ресурс] – Cisco, 2018. – Режим доступа: https://www.cisco.com/c/en/us/support/wireless/aironet-1250-series/products-configuration-examples-list.html