Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к курсовому проекту
на тему
ЛОКАЛЬНАЯ КОМПЬЮТЕРНАЯ СЕТЬ

БГУИР КП 1-40 02 01 01 009 ПЗ

Студент А. А. Донденко

Руководитель И. И. Глецевич

МИНСК 2023

Вариант	9
Объект	Компания по оказанию юридических услуг
Форма здания, этажи, суммарная площадь помещений в квадратных метрах	Прямоугольная, 1-3, 100
Количество стационарных пользователей (ПК), количество стационарных подключений, количество мобильных подключений	20, 20, заказчик не уверен
Сервисы (дополнительные подключения)	Файловый сервер NTFS/SMB для внутреннего использования
Прочее оконечное оборудование (дополнительные подключения)	Принтеры, заказчик не уверен
Подключение к Internet	Gigabit Ethernet: оптоволокно
Внешняя адресация IPv4, внутренняя адресация IPv4, адресация IPv6	Статический внешний IPv4 адрес, публичная подсеть, взаимодействие в рамках внутренней сети
Безопасность	Усиленная безопасность в отношении учетных записей пользователей
Надежность	Заказчик не уверен
Финансы	Бюджетная сеть
Производитель сетевого оборудования	Allied Telesis
Дополнительное требование заказчика	Нет

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4
1 ОБЗОР ЛИТЕРАТУРЫ 5
1.1 Файловый сервер NTFS/SMB 5
2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ 7
3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ 9
3.1 Обоснование выбора программного обеспечения для пользовательских станций 9
3.2 Обоснование выбора пользовательских станций 10
3.3 Обоснование выбора оконечного оборудования 11
3.4 Обоснование выбора файлового сервера 12
3.5 Обоснование выбора активного сетевого оборудования 12
3.5.1 Обоснование выбора маршрутизатора 12
3.5.2 Обоснование выбора коммутатора 13
3.5.3 Обоснование выбора точки доступа 13
3.6 Схема адресации IPv4 14
3.7 Схема адресации IPv6 15
3.8 Настройка оборудования Allied Telesis 16
3.8.1 Настройка коммутаторов 17
3.8.2 Настройка маршрутизатора 18
3.8.3 Настройка беспроводных точек доступа 21
3.9 Настройка прочего оборудования 22
3.9.1 Настройка файлового сервера SMB/NTFS 22
3.9.2 Настройка оконечного оборудования 23
4 ПРОЕКТИРОВАНИЕ СТРУКТУРНОЙ КАБЕЛЬНОЙ СИСТЕМЫ 24
4.1 План размещения оборудования 24
4.2 Обоснование выбора пассивного сетевого оборудования 24
4.2.1 Коннектор RJ45 24
4.2.2 Витая пара 25
4.2.3 Информационные розетки 25
4.2.4 Телекоммуникационный шкаф 25
4.2.5 Кабель-канал для витой пары 25
ЗАКЛЮЧЕНИЕ 26
СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 27
ПРИЛОЖЕНИЕ А 28
ПРИЛОЖЕНИЕ Б 29
ПРИЛОЖЕНИЕ В 30
ПРИЛОЖЕНИЕ Г 31
ПРИЛОЖЕНИЕ Д 32

ВВЕДЕНИЕ

Сегодня невозможно себе представить жизнь среднестатистического человека без постоянного обмена информацией в том числе с использованием компьютерных сетей. Более того, использование компьютерных сетей является неотъемлемым требованием для любой организации, претендующей на высокое удобство и эффективность труда.

В процессе выполнения курсового проектирования следует обратить особое внимание на характер услуг, предоставляемых заказчиком, а также бюджет, выделенный на разработку архитектуры локальной компьютерной сети. Немало важным является необходимость обеспечить достаточную безопасность локальной компьютерной сети с целью не допустить утечки информации юридического и коммерческого характера.

На самом первом этапе необходимо изучить требования заказчика к локальной компьютерной сети. Необходимо определить количество пользователей сети и особенности ее реализации.

Затем необходимо разработать концептуальную структуру локальной компьютерной сети. Это подразумевает определение подсетей, протоколов и прочих технологий, задействование которых будет необходимо для создания эффективной компьютерной сети.

После этого необходимо разработать физическую структуру сети. Для этого в первую очередь необходимо однозначно определиться с выбором оборудования и его расположения. Также в этот пункт входит проектирование структуры кабельных систем.

Заключительным этапом является конфигурирование и последующие тестирование всех устройств компьютерной сети. Если на этапе тестирования не было выявлено никаких проблем, стоит задуматься о способах оптимизации работы сети.

Целью данного курсового проектирования является разработка и реализация эффективной компьютерной сети для компании по оказанию юридических услуг с учетом требований заказчика.

Для достижения данной цели необходимо выполнить ряд задач:

- спроектировать логическую и физическую структуры;
- подобрать и сконфигурировать оборудование, необходимое для реализации структуры сети;
- разработать меры безопасности в отношении учетных записей пользователей;
- провести тестирование и оптимизацию итоговой компьютерной сети.

1 ОБЗОР ЛИТЕРАТУРЫ

Для корректного проектирования локальной компьютерной сети требуется изучить основы организации и построения компьютерных сетей, а также изучить возможные меры по усилению безопасности в отношении учетных записей пользователей.

Также необходимо изучить материалы, связанные с настройкой оборудования компании Allied Telesis. В частности, нужно научиться работать с операционной системой AlliedWare+, которая является стандартной для большей части оборудования компании.

Одним из дополнительных требований заказчика является создание файлового сервера NTFS/SMB. Соответственно необходимо изучить материалы, связанные созданием файлового сервера и этими протоколами.

1.1 Файловый сервер NTFS/SMB

По своей сути файловый сервер – это ресурс, доступ к которому имеют все абоненты сети. Он может использоваться не только для упрощения обмена файлов между абонентами сети, но и для увеличения общего уровня защиты информации. При этом файловым сервером может являться как аппаратное, так и программное обеспечение.

Server Message Block (SMB) – протокол прикладного уровня модели OSI, который в основном используется для доступа к сетевым ресурсам. Этот протокол использует технологию клиент-сервер и различные протоколы транспортного уровня модели OSI. На сегодняшний день данный протокол в первую очередь ассоциируется с операционными системами Windows и компанией Microsoft, которая и занимается разработкой новых версий протокола.

Принцип работы протокола разделен на несколько этапов.

На первом этапе клиенты соединяются с сервером посредством поддерживаемого SMB протокола транспортного уровня. На сегодняшний день чаще всего используется протокол NetBIOS через TCP\IP или TCP\IP напрямую, если возможно.

После успешной установки соединения появляется обмениваться SMB пакетами. Заголовок пакета SMB включает в себя: команду протокола, а также идентификаторы протокола, соединения с сетевым ресурсом, клиентского процесса, пользователя и группы пользователя.

Microsoft предоставляет следующую классификацию пакетов данных, отправляемых между клиентом и сервером в протоколе Microsoft SMB:

- пакеты управления сеансом, которые устанавливают и прекращают подключение к общим ресурсам сервера;

- пакеты доступа к файлам, посредством которых осуществляется доступ и управление файлов и каталогов на сервере;

- общие пакеты сообщений, которые представляют из себя пакеты с данными общего назначения.

В первую очередь после установки соединения происходит согласование диалектов протокола клиента и сервера.

Далее, используя SMB команды, клиент может выполнять с предоставленными сервером ресурсами весь перечень действий, которые можно выполнять с файловой системой.

Что касается безопасности, модель механизма защиты протокола SMB включает в себя два уровня: пользовательский уровень и уровень совместно используемого ресурса. Оба уровня используют шифрование для сокрытия персональных данных от потенциальных злоумышленников.

Уровень пользователя подразумевает необходимость аутентификации с использованием уникального имени пользователя и пароля для получения доступа к ресурсам сервера.

Для обеспечения дополнительного уровня контроля защиты сверх уровня пользователя используется уровень совместно используемого ресурса. Он подразумевает наличие у конкретных ресурсов сервера собственного пароля необходимого для доступа к этому ресурсу.

New Technology File Systems (NTFS) – это файловая система, которая используется в операционных системах семейства Windows. В ее основу легла High Performance File System (HPFS). В отличии от нее NTFS обладает рядом преимуществ, таких как: квотирование, журналирование, разграничение доступа, аудит, шифрование дисков и контроль доступа безопасности списка. Подобные улучшения имели и негативное последствие – значительное уменьшение скорости работы по сравнению с HPFS.

В контексте файловой системы для сервера NTFS имеет ряд полезных функций. Например, функция самовосстановления, которая позволяет находить поврежденные участки файловой системы без явного запроса на проверку от пользователя. Более того, благодаря различным оптимизациям кода ядра, вышеупомянутый процесс не сказывается на общей производительности системы.

Также стоит упомянуть, что зачастую контроля защиты протокола SMB не хватает для гибкой настройки прав доступа к файловым ресурсам сервера. В этом случае можно воспользоваться NTFS разрешения, которые работают как локально, так и по сети. SMB и NTFS разрешения не только не конфликтуют между собой, но и прекрасно дополняют друг друга. Благодаря NTFS разрешений можно изменять права чтения, записи, выполнения для конкретного пользователя или группы пользователей.

2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В соответствии с заданием необходимо разработать локальную компьютерную сеть для компании по оказанию юридических услуг.

Для формирования структуры будущей компьютерной сети необходимо проанализировать структуру офисного здания, в котором она будет размещена. Здание имеет три этажа прямоугольной формы, площадь каждого этажа – 100 метров квадратных.

Необходимо озаботиться о том, чтобы компьютерная сеть покрывала все три этажа здания. При этом необходимо, чтобы пользователи с каждого этажа имели доступ к файловому серверу и интернету.

Всего необходимо предусмотреть 20 пользовательских станций в компьютерной сети. Из них необходимо выделить отдельные станции для системного администратора и директора. Логично будет разместить эти станции на втором этаже.

Также на втором этаже необходимо разместить и файловый сервер в комнате системного администратора. Расположение всех ключевых узлов компьютерной сети на втором этаже обеспечит их равноудаленность от прочих абонентов сети что положительно скажется на общей эффективности сети.

Исходя из вышеперечисленных данных, 18 пользовательских станций для рядовых сотрудников следует разместить следующим образом: по семь на первом и третьем этажах и четыре на втором этаже здания.

В качестве дополнительного оборудования для компьютерной сети заказчик требует наличие принтеров. Также будет хорошей идеей поставить сканеры, потому что юридические компании зачастую работают в том числе и с бумажными документами клиентов, которые необходимо оцифровывать. Во избежание увеличения денежных затрат будет хорошей идеей использовать не по одному принтеру и сканеру на персональную станцию, а по две единицы на один этаж. При этом на втором этаже следует разместить только по одному принтеру и сканеру, так как количество пользователей меньше.

У этих пользовательский станций директора и администратора должны быть отдельные принтеры, потому что через эти станции может проходить документооборот, который прочим сотрудникам видеть нежелательно. Например, отчеты об использовании трафика сотрудниками или данные касательно заработной платы.

Чтобы обеспечить равномерное покрытие всей площади здания необходимо предусмотреть точки доступа беспроводной сети. Итоговое количество мобильных подключений будет равняться 5.

Для коммутации трафика со всех этажей будет использоваться три коммутатора. По одному на каждый этаж.

Для маршрутизации трафика между внешней и внутренней сетями будет использоваться один маршрутизатор. Он будет располагаться на втором этаже

компании.

Также на втором этаже будет располагаться условный выход в интернет посредством оптоволоконного кабеля.

Логическая топология реализована с помощью разделения сети здания на отдельные подсети. При этом все пользовательские станции для рядовых сотрудников на каждом из этажей будут относится к разным подсетям. Это сделано из расчета, что на каждом этаже будут находится работники с одинаковой зоной ответственности. Для станций директора, сервера и администратора будут созданы отдельные подсети.

Как следствие, согласно количеству подключений и требуемому для реализации локальной компьютерной сети оборудованию, можно выделить следующие структурные блоки:

– коммутатор;
– маршрутизатор;
– персональная станция;
– беспроводная точка доступа;
– принтер;
– сканер;
– персональная станция администратора;
– персональная станция директора;
– интернет;
– файловый сервер.

Блок интернета связан только с блоком маршрутизатора, который в свою очередь связан со всеми тремя коммутаторами на разных этажах и файловым сервером.

Блоки коммутаторов связаны со всем оборудованием на своих этажах, исключая принтеры, и маршрутизатором.

Блоки принтеров связаны с блоками беспроводных точек доступа на своих этажах. Также блоки персональных станций администратора и директора дополнительно связаны с отдельными принтерами.

Структурная схема локальной компьютерной сети представлена в приложении А.

3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе описывается функционирование программной и аппаратной составляющих разрабатываемой локальной компьютерной сети.

В рамках данного проекта сеть предприятия будет разделена на 7 виртуальные сетей:

1. Виртуальная сеть для директора компании.
2. Виртуальная сеть для администрирования.
3. Виртуальная сеть для доступа к файловому серверу.
4. Виртуальная сеть для устройств на первом этаже.
5. Виртуальная сеть для устройств на втором этаже.
6. Виртуальная сеть для устройств на третьем этаже.

Связь маршрутизатора, коммутаторов, принтеров, сканеров, файлового сервера, беспроводных точек доступа и компьютеров между собой будет произведена с помощью портов Gigabit Ethernet. Принтеры к компьютерам администратора и директора будут подключены при помощи портов USB.

Для соединения посредством Gigabit Ethernet будет использоваться стандарт 802.3ab 1000BASE-T, определяющий работу передачи данных по неэкранированной витой паре пятой категории.

Данный раздел сопровождает чертеж схемы СКС функциональной (приложение Б).

3.1 Обоснование выбора программного обеспечения для пользовательских станций.

При выборе операционной системы для персональных компьютеров следует в первую очередь обратить внимание на то, что все пользователи кроме системного администратора не обладают обширными знаниями об обращении с компьютерами. Из этого следует, что необходимо выбрать систему с максимально простым освоением. Также система должна ограничивать уровень прав пользователя с целью предотвращения вмешательства в системные файлы неграмотного пользователя.

Исходя из всего вышеперечисленного, очевидным выбором будет выбор операционной системы семейства Windows. Выбор конкретной версии также довольно очевиден. Windows 7 не подходит, так как Microsoft больше официально не поддерживает эту операционную систему. Windows 11 на данный момент только появилась на рынке и может иметь ряд скрытых недоработок. Соответственно выбор был сделан в пользу Windows 10.

Что касается версии Windows 10, выбор был сделан в пользу Windows 10 Pro. Главной причиной этому являются расширенные возможности в отношении обеспечения общей безопасности пользователей. В частности, одним из главных преимуществ является шифрование данных с помощью функции BitLocker. Использование данной функции значительно усложнит

потенциальным злоумышленникам попытки украсть конфиденциальные данные.

В результате проведенного анализа имеем операционную систему Windows 10 Pro.

3.2 Обоснование выбора пользовательских станций

Для того, чтобы выбрать пользовательские станции необходимо в первую очередь определить задачи, которые им необходимо будет решать.

В компании по оказанию юридических услуг большую часть времени сотрудники будут проводить в текстовом редакторе, например Microsoft Word. Узконаправленное программное обеспечение, например Консультант Плюс, также не требователен к ресурсам. Персональный компьютер должен также иметь достаточную производительность для воспроизведения видео различных форматов, работы в интернете и работы с изображением.

Следующим важным атрибутом для пользовательских станций является качество экрана. Работники компании будут проводить значительную часть времени, работая за компьютером. Для увеличения общего комфорта и снижения усталости глаз стоит задуматься о качественном мониторе.

Для подключения к компьютерной сети пользовательская станция должна обладать портом Gigabit Ethernet. А для подключения периферии необходимо минимум четыре порта USB. Менее важным, но все еще значительным является наличие звукового выхода.

Стоит упомянуть, что в связи в большим объемом передаваемых файлов, выбор накопителя для персональных компьютеров стоит сделать в пользу SSD накопителей, так как скорость чтения и записи у данного типа накопителей выше. При этом на объеме накопителя можно сэкономить, так как большая часть файлов будет храниться на файловом сервере.

Исходя из всего вышеперечисленного, был выбран формат моноблока для пользовательских станций. Дополнительными преимуществами такого выбора являются: экономия рабочего пространства и экономия денежных средств.

Проанализировав рынок моноблоков, выбор был сделан в пользу моноблока IRBY Pro 27-B-i3101-16-0-480-N-H510-012. Данная модель полностью удовлетворяет требованиям по интерфейсам, обладает качественной IPS матрицей, ее производительность не является избыточной, в качестве хранилища данных выступает SSD накопитель.

Приятными бонусами является идущая в комплекте периферия в виде беспроводной клавиатуры и мыши и наличие встроенной камеры с микрофоном. Также в стоимость включена операционная система Windows 10 Pro.

Стоимость одной единицы 2874 белорусских рублей. Всего необходимо 20 единиц техники.

3.3 Обоснование выбора оконечного оборудования

Единственным требованием заказчика к оконечному оборудованию является наличие принтера.

Так как компания по оказанию юридических услуг работает в основном с документами, переплачивать за цветную печать не имеет смысла. Также стоит учесть, что для подключения к беспроводной сети обязательно наличие у принтеров сетевого интерфейса. Это требование не касается двух принтеров, которые будут установлены для системного администратора и директора компании, так как они будут подключены к их пользовательским станциям при помощи порта USB.

Дополнительно было принято решение установить сканеры для сотрудников компании. Для них также обязательно наличие LAN интерфейса.

После анализа рынка стало очевидно, что гораздо выгоднее заменить пару принтер и сканер на одно МФУ. Данное решение позволит сэкономить деньги. Также подобный подход уменьшит количество абонентов сети, что увеличит количество свободных интерфейсов для будущего расширения компании.

Модель МФУ была выбрана Canon i-SENSYS MF453dw 5161C007. Всего необходимо пять единиц техники. Цена одной единицы – 927 белорусских рублей.

В качестве принтеров для системного администратора и директора была выбрана модель Canon i-SENSYS LBP6030B. Всего необходимо два таких принтера Цена одной единицы – 470 белорусских рублей.

.

3.4 Обоснование выбора файлового сервера

Одним из требований заказчика является наличие файлового сервера SMB\NTFS.

В качестве операционной системы для сервера была выбрана Windows Server 2022. Выбор операционной системы от Microsoft обусловлен тем, что именно эта компания занимается разработкой и дополнением протоколов SMB и NTFS. Выбор в пользу версии 2022 был сделан с целью обеспечения файлового сервера новейшими функциями в отношении серверов.

Что касается аппаратной части, необходим бюджетный сервер. От идеи построить сервер на базе персонального компьютера было решено отказаться, потому что на сервере будут храниться файлы чрезвычайной важности, то есть необходима максимальная отказоустойчивость. Более того, необходимо использование специального серверного процессора из-за большого количества абонентов сети.

Преимущественно на сервере будут храниться файлы небольшого объема: документы и фотографии. Из этого следует, что общий объем данных, который может хранить сервер, можно принять небольшим. Однако следует

рассмотреть варианты с возможностью дальнейшего увеличения данного объема.

Также важно учесть необходимость наличия минимум трех выходов Gigabit Ethernet для подключения к трем имеющимся коммутаторам.

После анализа рынка с учетом требований к серверу, выбор был сделан в пользу модели Supermicro IX-T100S-LN4-2224-S1.

Стоимость 5400 белорусских рублей.

3.5 Обоснование выбора активного сетевого оборудования

Сетевое оборудование — это оборудование необходимое для функционирования компьютерной сети. В свою очередь активное обозначает, что оборудование обрабатывает техническую информацию, перенаправляя и распределяя потоки в соответствии со встроенными алгоритмами. В данном случае необходимо осуществить выбор модели коммутатора и маршрутизатора. При этом производителем должна выступить компания Allied Telesis по требованию заказчика.

3.5.1 Обоснование выбора маршрутизатора

В первую очередь стоит упомянуть скудный выбор маршрутизаторов данного производителя на белорусском рынке электроники. Удалось найти лишь две модели – AT-AR2050V-51 и AT-AR4050S-51. При этом исходя из классификации компании первый относится к Secure VPN Routers, а второй к UTM Firewalls.

Таблица 3.1 – характеристики маршрутизаторов

	AR2050V	AR4050S
Поддержка 3G/4G	Есть	Есть
Поддержка IPv6	Есть	Есть
Количество и тип LAN портов	4 x 10/100/1000T RJ-45	8 x 10/100/1000T RJ-45
Количество и тип WAN портов	1 x 10/100/1000T RJ-45	2 x 10/100/1000T RJ-45
Количество и тип bypass портов	1 x 10/100/1000T RJ-45	2 x 10/100/1000T RJ-45
Удаленное управление	SSHv1/v2	SSHv1/v2
Максимальная потребляемая мощность, Вт	14	23/27

Что касается конкретных различий, все они идут в пользу модели AT-AR050S-51. Данная модель обладает вдвое большим количеством WAN и LAN портов, отдельным процессором для обеспечения комплексной защиты от

угроз, слотом для карты памяти для предотвращения утери важных данных и двумя слотами для дополнительных интерфейсов.

При этом вторая модель, AT-AR-2050V-51, обладает всеми качествами, которые необходимы для создания сети небольшой организации. Данная модель дешевле конкурента почти в два раза.

Однако модель AT-AR4050S-51 имеет одно критическое преимущество – возможность подключение оптоволоконного кабеля посредством встроенного порта SFP. Окончательный выбор был сделан в пользу данной модели именно по этой причине.

Стоимость одной единицы техники 3750 белорусских рублей.

3.5.2 Обоснование выбора коммутатора

На каждом этаже к коммутатору будет подключаться минимум девять устройств. Соответственно первым требованием для коммутатора является наличие минимум десяти портов Gigabit Ethernet с целью наличия минимальной возможности к расширению сети. Также необходима поддержка VLAN и IPv6 адресации. В конечном итоге минимальные требования к коммутатору звучат так: управляемый коммутатор второго уровня от производителя Allied Telesis с минимум десятью интерфейсами Gigabit Ethernet, поддержкой VLAN и IPv6.

Из-за скудного выбора на рынке по данным требованиям соответствует только одна модель – Allied Telesis AT-GS950/16-50. Приятным бонусом данной модели является наличие технологии Green Ethernet, которая является комплексом мер по экономии энергии в локальных сетях Ethernet.

Стоимость одной штуки - 1940 белорусских рублей. Всего необходимо три единицы техники.

3.5.3 Обоснование выбора точки доступа

Для обеспечения беспроводного подключения для 5 устройств необходимо выбрать соответствующую точку доступа.

Модельный ряд беспроводных точек доступа Allied Telesis предоставляет выбор из шести моделей. Три из которых относятся ко второму поколению линейки TQ. Изначально подразумевается, что к мобильным точкам доступа будет подключено оборудование, не требующее большой скорости, такое как МФУ.

Общее количество подключений на отдельно взятую точку доступа в итоговой компьютерной сети не будет превышать двух. Также необходимо учесть возможность расширения в будущем.

Вышеописанные требования в полной мере реализуются любой из представленных на рынке моделей. Исходя из этого, для компьютерной сети была выбрана самая бюджетная модель – AT-TQ1402.

Всего необходимо три штуки, стоимость каждой – 670 белорусских рублей.

3.6 Схема адресации IPv4

Для компании по оказанию юридических услуг была выбрана публичная подсеть 203.148.132.0/26. Подсеть была взята из 898 варианта заданий.

Провайдером был предоставлен внешний статический IPv4 адрес 190.182.182.100/24.

Данную подсеть требуется разделить на несколько подсетей: 203.148.132.16/28, 203.148.132.32/28, 203.148.132.48/28, 203.148.132.40/30, 203.148.132.44/30, 203.148.132.32/30. Каждая из подсетей рассчитана на достаточное количество подключений, которые присутствуют в сети на данный момент. Также предусмотрен некий резерв адресов, чтобы обеспечить возможность расширения в будущем.

Подсеть 203.148.132.16/28 может включать в себя до 14 хостов и рассчитана подключения персональных станций рядовых сотрудников и МФУ на первом этаже.

Подсети 203.148.132.32/28 и 203.148.132.48/28 имеют аналогичное назначение, но для устройств на втором и третьем этажах соответственно.

Подсеть 203.148.132.40/40 рассчитана на два хоста и выделена специально для директора компании.

Подсеть 203.148.132.44/40 рассчитана на два хоста и выделена специально для системного администратора.

Подсеть 203.148.132.32/40 рассчитана на два хоста и выделена специально для файлового сервера NTFS/SMB.

На каждую подсеть приходится отдельный VLAN. Схема адресации, на которой продемонстрировано отношение выделенных подсетей к соответствующим VLAN представлена в таблице 3.2. Также для передачи нетегированного трафика требуется создать Native VLAN 200.

Таблица 3.2 – Схема адресации подсетей IPv4.

Назначение	VLAN	Адрес подсети	Маска подсети
Подсеть рядовых подключений на первом этаже	41	203.148.132.16	255.255.255.240
Подсеть рядовых подключений на первом этаже	42	203.148.132.32	255.255.255.240
Подсеть рядовых подключений на первом этаже	43	203.148.132.48	255.255.255.240
Подсеть для директора	10	203.148.132.40	255.255.255.252
Подсеть для администратора	20	203.148.132.44	255.255.255.252
Подсеть для сервера	30	203.148.132.32	255.255.255.252

3.7 Схема адресации IPv6

Для реализации взаимодействия посредством IPv6 во внутренней подсети необходимо назначить устройствам адреса формата Unique Local Unicast. Global ID часть была выбрана случайным образом, а Subnet ID соответствует VID.

Таблица 3.3 – Схема адресации подсетей IPv6.

Назначение	VLAN	Адрес подсети
Подсеть рядовых подключений на первом этаже	41	fd80:2023:1401:41::/124
Подсеть рядовых подключений на первом этаже	42	fd80:2023:1401:42::/124
Подсеть рядовых подключений на первом этаже	43	fd80:2023:1401:43::/124
Подсеть для директора	10	fd80:2023:1401:10::/126
Подсеть для администратора	20	fd80:2023:1401:20::/126
Подсеть для сервера	30	fd80:2023:1401:30::/126

3.8 Настройка оборудования Allied Telesis

Выбранное оборудование компании Allied Telesis можно настраивать при помощи web-интерфейса. Для этого можно использовать протокол HTTP. Процесс подключения и настройки подробно описан в руководстве пользователя.

Для того, чтобы приступить к настройке, необходимо подключиться к LAN порту оборудования и в браузере по выбору ввести http:// и IPv4 адрес настраиваемой единицы техники. Далее необходимо ввести имя пользователя и пароль. Значениями по умолчанию являются manager для имени пользователя и friend для пароля. После ввода данных необходимо кликнуть на кнопку войти.

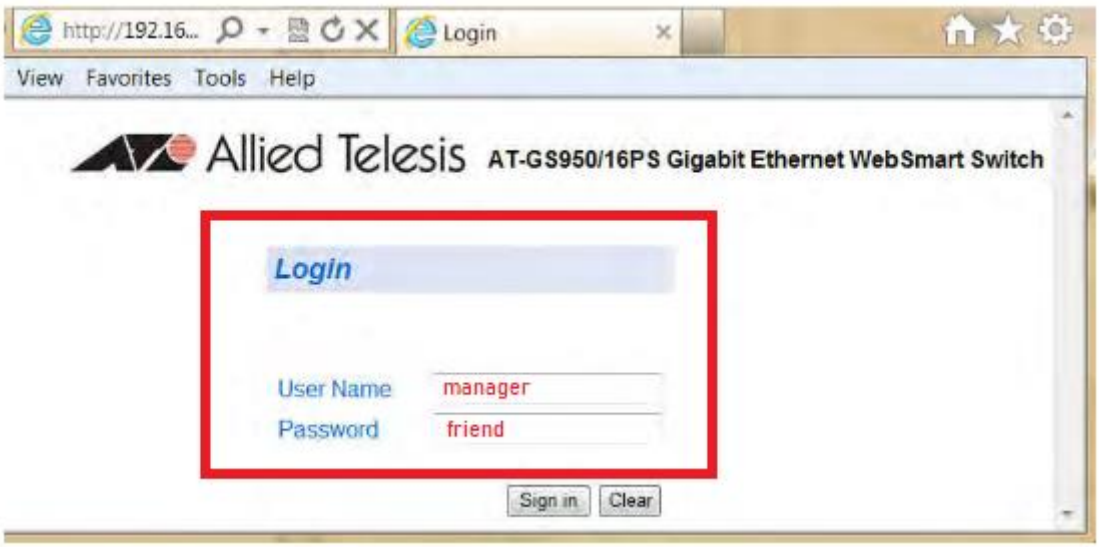

Рисунок 3.1 – Окно входа для оборудования компании Allied Telesis.

3.8.1 Настройка коммутаторов

Настройка для коммутаторов будет продемонстрирована на примере коммутатора, который находится на втором этаже.

Для начала нужно перейти во вкладку `Management`. В этой вкладке необходимо указать имя Switch2 и местоположение Second Floor для коммутатора.

Рисунок 3.2 – Вкладка Management коммутатора.

Далее нужно кликнуть на кнопку `Apply` и перейти во вкладку `Administration`. Здесь необходимо кликнуть на кнопку `Modify` рядом с профилем manager. После этого нужно изменить стандартный пароль на TJuCj2Ql.

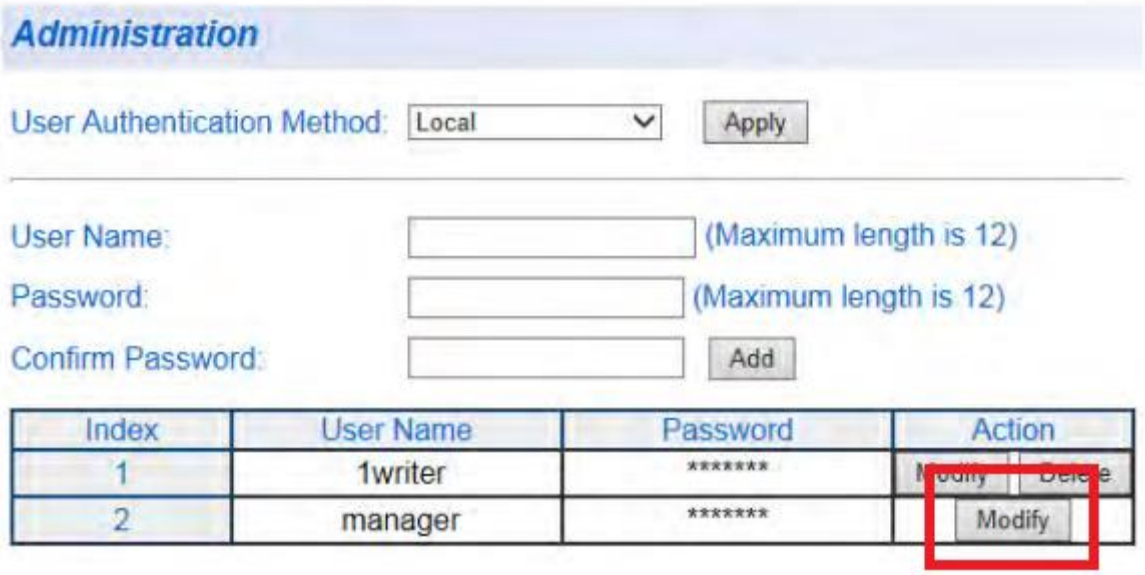

Рисунок 3.3 – Окно настройки доступа к администрированию.

Теперь необходимо перейти во вкладку `IPv4 Setup` и переключить `System IP Mode` в режим `DHCP`. Далее переходим в вкладку `IPv6 System Settings` и переключаем `IPv6 State` и `DHCPv6 Client` в состояние `enabled`.

Следующим теперь необходимо создать VLANs. Для этого нужно перейти во вкладку `Tagged VLAN` и задать VLAN ID, VLAN Name, Management VLAN, и принадлежность портов к создаваемому VLAN. После этого необходимо кликнуть на кнопку `Apply`.

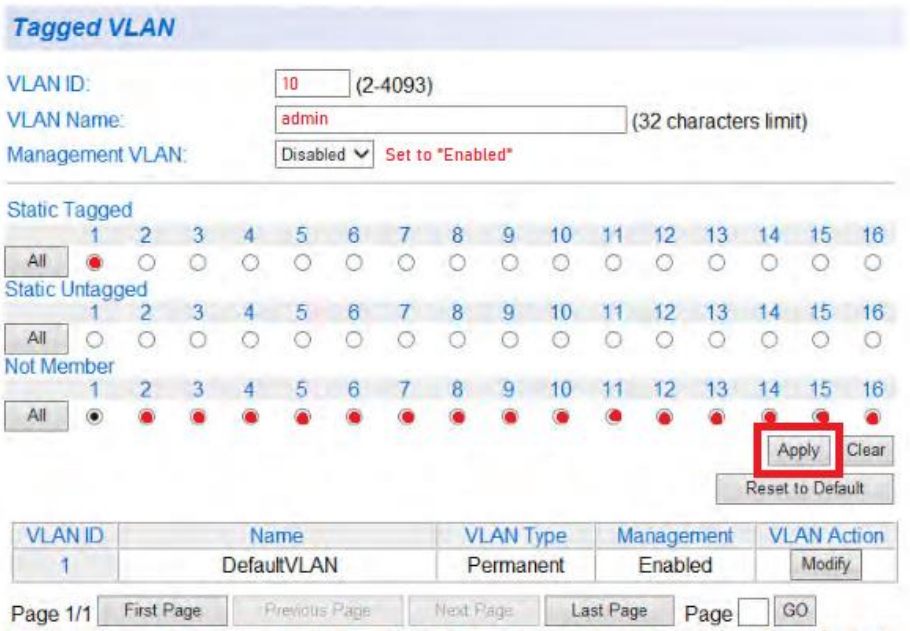

Рисунок 3.4 – Окно добавление VLAN.

Для функционирования сети необходимо создать следующие VLAN: admin, head и user2. Значения полей для этих VLAN описано в таблице 3.3.

Неиспользуемые порты необходимо административно отключить во вкладке Physical Interfaces.

Таблица 3.4 – Конфигурирование VLANs

VLAN Name	VLAN ID	Management VLAN	Static Tagged	Not Member
admin	10	Enabled	1, 8	2-7, 9-16
head	20	Disabled	2, 8	1, 3-7, 9-16
user2	42	Disabled	3-8	1-2, 9-16

Теперь необходимо позаботься об обеспечении усиленной безопасности сети. Для этого в первую очередь нужно включить использование SSL во вкладке SSL Settings. Благодаря этому доступ к настройкам коммутатора будет происходить только по защищенному протоколу HTTPS, который отличается наличием шифрования.

Также необходимо ограничить адреса, с которых может происходить конфигурирование. Для этого нужно перейти во вкладку IP Access List и переключить IP Restriction Status в enabled. После этого необходимо добавить IPv4 м IPv6 Адреса административной станции. Необходимые адреса 203.148.132.41 для IPv4 и fd80:2023:1401:10::1 для IPv6 соответственно. После ввода адресов необходимо кликнуть на кнопку Add. И только после этого необходимо кликнуть на кнопку Apply.

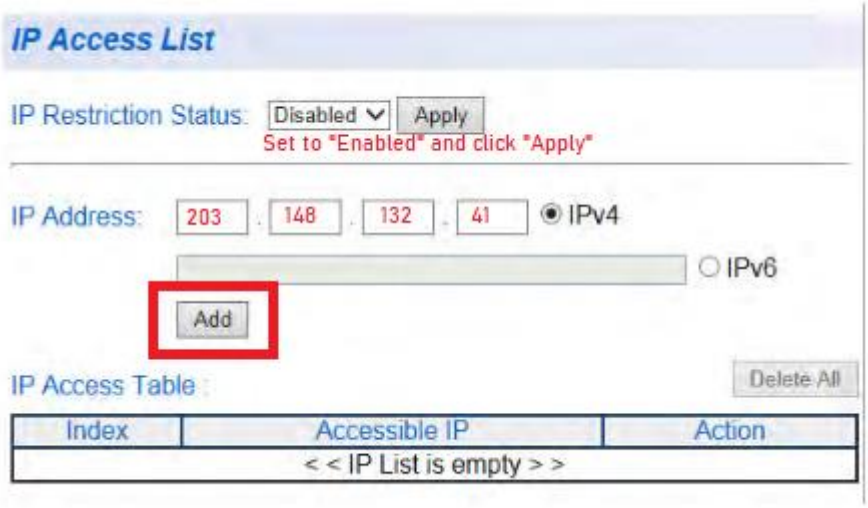

Рисунок 3.5 – Окно добавление IP Access адресов.

3.8.2 Настройка маршрутизатора

После подключения к маршрутизатору вышеописанным образом необходимо запустить мастер настройки. Для этого нужно перейти во вкладку Wizard и кликнуть на Setup. После этого начнется конфигурирование интернет-соединения по шагам.

На первом шаге необходимо выбрать тип соединения `IPv4 Fixed`. После этого необходимо задать IP Address – 192.182.182.100. и переключить `DHCP Server` в состояние `On`.

В связи с тем, что компания Allied Telesis не предоставляет инструкцию по полной настройке маршрутизатора через GUI, настройка частично будет осуществлена через CLI посредством PuTTY.

Сразу необходимо задать IPv4 и IPv6 адреса на маршрутизаторе:

```
awplus(config)#interface vlan10
awplus(config-if)#ip address 203.148.132.42/30
awplus(config-if)#ipv6 address fd80:2023:1401:10::2/126
awplus(config-if)#exit
awplus(config)#interface vlan20
awplus(config-if)#ip address 203.148.132.46/30
awplus(config-if)#ipv6 address fd80:2023:1401:20::2/126
awplus(config-if)#exit
awplus(config)#interface vlan30
awplus(config-if)#ip address 203.148.132.34/30
awplus(config-if)#ipv6 address fd80:2023:1401:30::2/126
awplus(config-if)#exit
awplus(config)#interface vlan41
awplus(config-if)#ip address 203.148.132.17/28
awplus(config-if)#ipv6 address fd80:2023:1401:41::1/124
awplus(config-if)#exit
awplus(config)#interface vlan42
awplus(config-if)#ip address 203.148.132.33/28
awplus(config-if)#ipv6 address fd80:2023:1401:42::1/124
awplus(config-if)#exit
awplus(config)#interface vlan43
awplus(config-if)#ip address 203.148.132.49/28
awplus(config-if)#ipv6 address fd80:2023:1401:43::1/124
awplus(config-if)#exit
awplus(config)interface eth1
awplus(config-if)#switchport enable
awplus(config-if)#switchport mode trunk
awplus(config-if)#swithcport trunk allowed vlan 10,20,30,41-
43
awplus(config)interface eth2
awplus(config-if)#switchport enable
awplus(config-if)#switchport mode trunk
awplus(config-if)#swithcport trunk allowed vlan 10,20,30,41-
43
awplus(config-if)#exit
awplus(config)interface eth3
awplus(config-if)#switchport enable
awplus(config-if)#switchport mode trunk
awplus(config-if)#swithcport trunk allowed vlan 10,20,30,41-
43
awplus(config-if)#exit
awplus(config)interface eth4
```

```
awplus(config-if)#switchport enable
awplus(config-if)#switchport mode access
awplus(config-if)#swithcport access vlan 30
awplus(config-if)#exit
```

Теперь необходимо настроить работу DHCP для каждого этажа. Нужно создать три набора адресов, которые будут выдаваться устройствам в VLAN 41 – 43. Для настройки также будет использоваться CLI.

```
awplus(config)ip dhcp pool floor1
awplus(config-dhcp)#network 203.148.132.16/28
awplus(config-dhcp)#range 203.148.132.19
awplus(config-dhcp)#host 203.148.132.18 a1a1.b1b1.c1c1
awplus(config-dhcp)#exit
awplus(config)ip dhcp pool floor2
awplus(config-dhcp)#network 203.148.132.32/28
awplus(config-dhcp)#range 203.148.132.35
awplus(config-dhcp)#host 203.148.132.34 a2a2.b2b2.c2c2
awplus(config-dhcp)#exit
awplus(config)ip dhcp pool floor3
awplus(config-dhcp)#network 203.148.132.48/28
awplus(config-dhcp)#range 203.148.132.51
awplus(config-dhcp)#host 203.148.132.50 a3a3.b3b3.c3c3
awplus(config-dhcp)#exit
awplus(config)ipv6 dhcp local pool floor1_v6
fd80:2023:1401:41/124
awplus(config)#interface vlan41
awplus(config-if)#ipv6 dhcp server floor1_v6
awplus(config-if)#exit
awplus(config)ipv6 dhcp local pool floor2_v6
fd80:2023:1401:42/124
awplus(config)#interface vlan42
awplus(config-if)#ipv6 dhcp server floor2_v6
awplus(config-if)#exit
awplus(config)ipv6 dhcp local pool floor3_v6
fd80:2023:1401:43/124
awplus(config)#interface vlan43
awplus(config-if)#ipv6 dhcp server floor3_v6
awplus(config-if)#exit
```

Следующим этапом будет настройка межсетевого экрана. Для этого воспользуемся GUI. В первую очередь необходимо разделить компьютерную сеть на зоны. Переходим во вкладку `Security` подраздел `Entities`. После необходимо кликнуть на кнопку `New Zone` и последовательно добавить следующие зоны: head, server, admin, floor1, floor2, floor3, internet. Затем нужно добавить в эти зоны подсети в соответствии с ранее созданной адресацией. После заполнения вышеуказанной информации необходимо кликнуть на кнопку `Save`.

Для настройки межсетевого экрана необходимо перейти во вкладку

Firewall. Здесь необходимо кликнуть на кнопку `Add new firewall rule`. В появившемся окне необходимо заполнить следующие поля: Action – действие, Application – сервис или приложение, From – источник, To – получатель. Источник и получатель могут быть как целыми зонами, так и конкретными хостами. Необходимо последовательно определить ряд правил. Запретить зоне internet доступ к любой другой зоне, кроме floor1, floor2, floor3. Запретить зонам floor1, floor2, floor3 доступ к зонам admin и head. Явно разрешить зоне admin доступ к любой другой зоне.

Последним этапом станет настройка доступа к администрированию маршрутизатора. Для этого необходимо перейти во вкладку `Administration`, где необходимо изменить стандартный пароль на OwZkFS88. Далее необходимо произвести настройку доверительных адресов во вкладке `IP Access List` аналогично коммутатору.

3.8.3 Настройка беспроводных точек доступа

После подключения к точке доступа вышеописанным образом необходимо кликнуть на `Easy Setup`.

Рисунок 3.6 – Окно начальной настройки.

В появившемся окне необходимо в поле Connection Type выбрать `DHCP`.

Рисунок 3.7 – Выбор типа подключения.

После этого необходимо перейти во вкладку VLAN Configuration и в поле Management VLAN Tag выбрать `Enabled`, а в поле Management VLAN ID написать `10`.

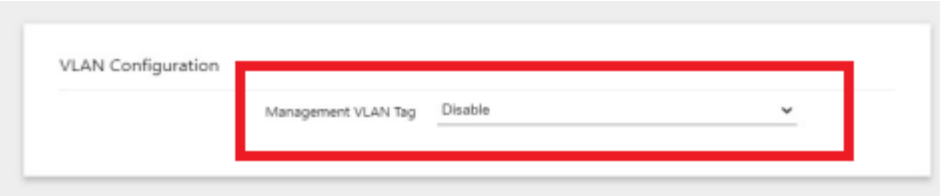

Рисунок 3.8 – Окно настройки VLAN.

Затем необходимо зайти во вкладку Radio Setting и задать SSID Floor1, Floor2 или Floor3 в соответствии с номером этажа и пароль – v5KbK3e.

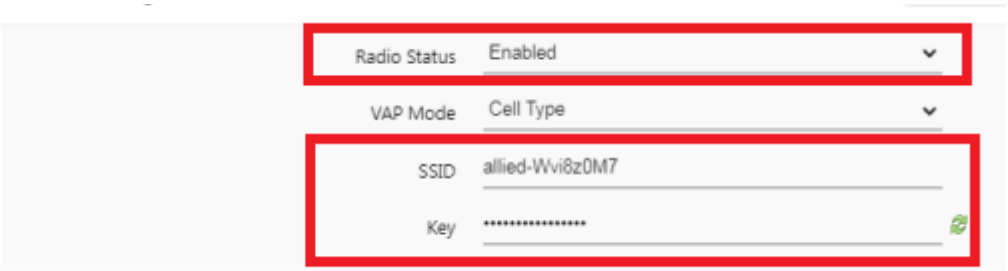

Рисунок 3.9 – Окно настройки BSS.

Последним этапом станет настройка доступа к администрированию точки доступа. Для этого необходимо перейти во вкладку `Administration`, где необходимо изменить стандартный пароль на BxpRW2q4.

Для сохранения настроек необходимо кликнуть на кнопку `Save and Apply`.

3.9 Настройка прочего оборудования

3.9.1 Настройка файлового сервера SMB\NTFS

В первую очередь необходимо в поиске операционной системы найти `Включение или отключение компонентов Windows`. Далее необходимо включить SMB Direct, Поддержка общего доступа к файлам SMB 1.0/CIFS и все подпункты и кликнуть `OK`.

Далее необходимо зайти в `Панель Управления` и выбрать пункт `Система и Безопасность` и подпункт `Межсетевой экран Windows`. После этого необходимо выбрать `Входящие правила`. Теперь необходимо включить правило Общий доступ к Файлам и Принтерам и зайти в его свойства используя правую кнопку мыши. Заходим в пункт `Охват` и разрешить доступ только для следующих подсетей: административной, директора и рядовых пользователей.

Самому серверу необходимо назначить статические IPv4 и IPv6 адреса на проводном интерфейсе. Адреса следующие: 203.148.132.33/30 и fd80:2023:1401:30::1/126. Также необходимо назначать шлюзы по умолчанию: 203.148.132.34/30 и fd80:2023:1401:30::2/126. Подробнее данный процесс

описан в следующем пункте.

Заключительным этапом будет создание общих папок и настройка пользователей с определенными правами доступа. Для этого необходимо зайти в Учетные записи и кликнуть на Добавить нового пользователя без учетной записи Майкрософт. Затем нужно задать имя пользователя и пароль и кликнуть ОК. Аналогичные действия нужно выполнить для каждого отдельного пользователя или группы пользователей.

После этого нужно создать новую папку используя правую кнопку мыши в предпочитаемом месте на сервере. Затем нужно зайти в свойства созданной папки и пункт Безопасность. Далее нужно присвоить пользователям права доступа к этой папке. Также можно изменить права на чтение, запись и исполнение применительно каждого пользователя или группы пользователей.

3.9.2 Настройка оконечного оборудования

Настройка пользовательских станций начинается с включения Windows Hello – индивидуально настраиваемого и безопасного способа получить доступ к устройствам Windows 10. Для этого необходимо перейти в пункт Параметры Входа Windows Hello. Так как в выбранной ранее модели моноблока присутствует веб-камера, имеет смысл настроить вход с использованием распознавания лица с помощью соответствующего пункта меню. Это исключит возможность получения доступа к станции потенциального злоумышленника.

Далее необходимо на каждом устройстве сконфигурировать сетевые интерфейсы. Для этого необходимо перейти в свойства данного интерфейса и выбрать в пункте Присвоение IP вариант Автоматически (DHCP).

Для администратора и директора необходимо выбрать вариант Вручную и задать следующую информацию. Для директора: адрес – 203.148.132.41, маска подсети – 255.255.255.252, шлюз – 203.148.132.42, адрес IPv6 – fd80:2023:1401:10::1, длина префикса – 126, шлюз IPv6 fd80:2023:1401:10::2. Для администратора: адрес – 203.148.132.45, маска подсети – 255.255.255.252, шлюз – 203.148.132.46, адрес IPv6 – fd80:2023:1401:20::1, длина префикса – 126, шлюз IPv6 fd80:2023:1401:20::2.

Принтеры, которые подключены к персональным компьютерам директора и администратора при помощи USB портов в дополнительной настройке не нуждаются.

4 ПРОЕКТИРОВАНИЕ СТРУКТУРНОЙ КАБЕЛЬНОЙ СИСТЕМЫ

4.1 План размещения оборудования

Компания по оказанию юридических услуг расположена в одном здании на трех этажах. Общая площадь всех помещений составляет 300 квадратных метров. Площадь каждого этажа составляет 100 квадратных метров. Форма этажа – прямоугольная с соотношением сторон два к одному. Соответственно ширина каждого этажа составляет семь метров, а длина – 14 метров.

Каждый из этажей представляет собой офис прямоугольной формы.

На первом и третьем этажах оборудовано по семь кабинетов для рядовых сотрудников, одному туалету и одной комнате с офисным оборудованием. Соответственно данные этажи имеют одинаковую планировку.

На втором этаже оборудован туалет, кабинет директора, кабинет системного администратора и четыре места для рядовых сотрудников. При этом

Самый верхний этаж предназначен для руководителя компании. На данном этаже находится одно рабочее место для руководителя, на котором располагается персональный компьютер руководителя и принтер. Так же в данной комнате располагается стол для переговоров. Первый и второй этажи имеют одинаковую планировку. Здание является шестиугольником, это дает множество вариантов расположения сотрудников, но самым оптимальным, является расположение по одному рабочему месту у каждой второй стены, напротив окна. Данное решение имеет большой плюс – очень большое количество света на рабочем месте сотрудника, что повышает работоспособность сотрудника. Так же, как и у руководителя компании, у каждого сотрудника на рабочем месте присутствует свой принтер.

4.2 Обоснование выбора пассивного сетевого оборудования

Сетевое оборудование, которое предназначено не для анализа передаваемой информации, а для обеспечение требующихся технических характеристик, к примеру, подключение между собой коммутаторов, называются пассивными. Для реализации компьютерной сети понадобиться следующее пассивное сетевое оборудование: коннекторы RJ45, витая пара и информационные розетки.

4.2.1 Коннекторы RJ45

Для покрытия всех нужд и уменьшения итоговой стоимости за один коннектор было принято решение закупить коннекторы оптом. Размер партии – 100 штук. Модель – Cablexpert PLUG3UP6/5.

Стоимость партии 25 белорусских рублей.

4.2.2 Витая пара

В качестве витой пары необходима модель шестой категории с внешним экранированием. После анализа рынка оптимальной по цене и соответствующей по требованиям оказалась модель – F/UTP Cat 6 PVC 4x2x0,57. Общее экранирование фольгой позволит увеличить общую помехоустойчивость сети. Цена за один метр – 2,5 белорусских рубля.

4.2.3 Информационные розетки

Для данной компьютерной сети выбраны информационные розетки Glossa GSL000181K RJ45. Основными причинами такого выбора стали доступная цена и разнообразие цветовых решений, что позволит лаконично вписать данную модель в любой интерьер. Цена за одну штуку 22 белорусских рубля. Всего необходимо закупить 20 штук.

4.2.4 Телекоммуникационный шкаф

В рамках разработанной компьютерный сети необходимо наличие телекоммуникационного шкафа. При этом для активного сетевого оборудования нужен небольшой шкаф, а для сервера нужен шкаф большего размера. Исходя из соображений экономии бюджеты, были выбраны самые дешевые варианты из имеющихся на рынке.

Были выбраны модель Silver 9U ценой 300 белорусских рублей для активного сетевого оборудования и модель ЦМО ШТК-М-22.6.8-4ААА 22U ценой 1500 белорусских рублей для сервера. При этом нужно закупить три единицы первой модели и одну единицу второй.

4.2.5 Кабель-канал для витой пары

Как было сказано ранее кабели будут прокладываться в кабель-каналах. Сечение кабеля вида витая пара категории 6 составляет примерно 31.5 мм^2. Кабель-каналы необходимо подбирать таким образом, чтобы его заполнение составляло примерно 60%. Максимальное количество кабелей, вместе требующих проводки будет составлять 10 штук, что в среднем составит суммарную площадь сечения 315 мм^2. Для покрытия такого сечения требуется короб с сечением минимальной площадью сечения 525 мм^2.

Для соответствия данному требованию был выбран кабель-канал Bylectrica КДК 25 на 25 миллиметров. Цена за один метр – два белорусских рубля.

ЗАКЛЮЧЕНИЕ

В результате выполнения данного курсового проекта была успешно разработана локальная компьютерная сеть компании по оказанию юридических услуг.

Были получены теоретические и практические навыки по проектированию локальных компьютерных сетей. Была изучена документация и рекомендации по выбору и настройке сетевого оборудования компании Allied Telesis. Также был изучен материал для настройки файлового сервера на базе операционной системы Windows Server.

В итоге работы была спроектирована компьютерная сеть в несколько этапов. Последовательно были разработаны логическая и физическая топологии.

Также было подобрано оборудование необходимое для реализации ранее разработанной топологии.

После этого был спроектирован план этажа с учетом подобранного оборудования.

Дополнительно была настроены следующие функции Windows Group Policy, IP Access List и Windows Hello для обеспечения дополнительной безопасности в отношении учетных записей пользователей.

В процессе проектирования все требования заказчика были реализованы в полном объеме. Была усилена безопасность в отношении учетных записей пользователей и настроен файловый сервер SMB\NTFS.

Дополнительно была обеспечена отказоустойчивость файлового сервера благодаря аппаратной поддержки технологии RAID.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

[1]. Вычислительные машины, системы и сети: дипломное проектирование (методическое пособие) [Электронный ресурс]: Минск БГУИР 2019. – Электронные данные. – Режим доступа: https://www.bsuir.by/m/12_100229_1_136308.pdf. – Дата доступа: 28.09.2022

[2] Олифер, В. Компьютерные сети. Принципы, технологии, протоколы / В. Олифер, Н. Олифер – Спб: Питер, 2019. – 992 с.

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

[4] Обзор файловой системы NTFS [Электронный доступ]. – Режим доступа: https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/ntfs-overview – Дата доступа: 21.10.2023.

[5] Общие сведения о совместном использовании файлов с помощью протокола SMB3 в Windows Server [Электронный доступ] – Режим доступа: https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/file-server-smb-overview – Дата доступа: 21.10.2023.

[6] Getting Started with the Device GUI on UTM Firewalls [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.alliedtelesis.com/sites/default/files/documents/getting-started-guides/getting_started_utm_firewall_gui.pdf – Дата доступа: 21.10.2023.

[7] VLANs Feature Overview and Configuration Guide [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/vlan_feature_overview_guide.pdf – Дата доступа: 21.10.2023.

[8] User Guide: AT-GS950/16PS [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/gs950_16pswebs112v200a.pdf – Дата доступа: 21.10.2023.

[8] User Guide: AT-TQ1402 Series [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/ati-tq1402series-ug.pdf – Дата доступа: 21.10.2023.

ПРИЛОЖЕНИЕ А
(обязательное)

Схема СКС структурная

ПРИЛОЖЕНИЕ Б
(обязательное)

Схема СКС функциональная

ПРИЛОЖЕНИЕ В
(обязательное)

Схема СКС принципиальная (план здания)

ПРИЛОЖЕНИЕ Г
(обязательное)

Перечень оборудования

ПРИЛОЖЕНИЕ Д
(обязательное)

Ведомость документов