

Учреждение образования
«Белорусский государственный университет информатики и
радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Дисциплина: Аппаратное обеспечение компьютерных сетей

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к курсовому проекту
на тему
«Локальная компьютерная сеть, Вариант 59»

БГУИР КП 1–40 02 01 01 228 ПЗ

Студент:

П.В. Сякачёв

Руководитель:

И.И. Глецевич

МИНСК 2022

Вариант	59
Объект	рекламное агентство
Форма здания, этажи, суммарная площадь помещений в квадратных метрах	прямоугольная, 2, 105
Количество стационарных пользователей (ПК), количество стационарных подключений, количество мобильных подключений	15, 15, ?
Сервисы (дополнительные подключения)	нет
Прочее оконечное оборудование (дополнительные подключения)	принтеры, проекторы
Подключение к Internet	Gigabit Ethernet: оптоволокно
Внешняя адресация IPv4, внутренняя адресация IPv4, адресация IPv6	статический внешний IP адрес, приватная подсеть, доступ в Internet, использовать подсеть из блока адресов для Беларуси
Безопасность	IPsec-VPN для удаленного подразделения
Надежность	резервирование соединений
Финансы	бюджетная сеть
Производитель сетевого оборудования	Dell
Дополнительное требование заказчика	экологичность

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ	3
ВВЕДЕНИЕ	5
1 ОБЗОР ЛИТЕРАТУРЫ	6
1.2 Оптоволоконный Gigabit Ethernet	6
1.2 Small Form-factor Pluggable	6
1.3 IPSec-VPN	7
1.4 Экологичность	7
1.4 Резервирование соединений	8
2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ	9
2.1 Маршрутизатор	9
2.2 Коммутаторы	9
2.3 Беспроводные точки доступа	9
2.4 Прочее оконечное оборудование (принтеры, проекторы)	10
3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ	11
3.1 Расположение устройств	11
3.2 Выбор сетевого оборудования	11
3.2.1 Выбор модели маршрутизатора	11
3.2.2 Выбор модели коммутатора	12
3.2.3 Выбор модели беспроводной точки доступа	13
3.3 Выбор оконечного оборудования	14
3.3.1 Выбор персонального компьютера	14
3.3.2 Выбор принтера и проектора	14
3.5 Адресация в локальной компьютерной сети	16
3.4 Настройка оборудования	18
3.4.1 Настройка роутера	18
3.4.2 Настройка коммутатора	21
3.4.3 Настройка беспроводной точки доступа	22
3.4.4 Настройка принтера и проектора	24
3.4.5 Настройка персональных компьютеров	25
4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ	26

ЗАКЛЮЧЕНИЕ	27
СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ	28
ПРИЛОЖЕНИЕ А	30
ПРИЛОЖЕНИЕ Б	31
ПРИЛОЖЕНИЕ В	32
ПРИЛОЖЕНИЕ Г	33
ПРИЛОЖЕНИЕ Д	34

ВВЕДЕНИЕ

В данной курсовой работе проектируется локальная компьютерная сеть для рекламного агентства. Инфраструктура данной сети приближена к реальности.

Локальная компьютерная сеть строится не только для удобства передачи информации в рамках данной организации, но и для удобства коммуникации и удобного получения данных извне, посредством сети Интернет. Для рекламного агентства это крайне важно, так как есть необходимость быстрого и удобного взаимодействия с заказчиками, качественной передачи большого объёма информации для создания и обработки рекламы.

Работа организации, в которой построена и грамотно настроена локальная компьютерная сеть, значительно отличается от работы таковой, в которой сеть будет отсутствовать, так как она позволяет экономить бюджет, пространство, помогает лучше устроить коммуникацию внутри и вне организации.

Локальная компьютерная сеть необходима для того, чтобы решать вопросы, которые касаются быстрого взаимодействия, качественной передачи информации и её защиты. Такая сеть позволит уменьшить количество периферийного оборудования, позволяя пользоваться общим, что, в свою очередь позволяет сэкономить бюджет. Также очень удобной является возможность подключить свои личные устройства (как при помощи стационарного, так и при помощи мобильного подключения), что позволяет работать с наиболее удобного для себя устройства.

Использование IPSec-VPN позволит агентству безопасно использовать внутренние ресурсы, которые закрыты от общего доступа через сеть Интернет.

Цель проекта: разработка проекта локальной компьютерной сети для рекламного агентства.

Задачи проекта: изучение материала по заданию на проект; изучение технологий по ходу выполнения проекта; разработка общей структуры сети, структурной схемы; выбор конкретных устройств, обоснование их выбора, описание настройки устройств, составление функциональной схемы; разработка структурной кабельной системы, составление её схемы.

1 ОБЗОР ЛИТЕРАТУРЫ

1.2 Оптоволоконный Gigabit Ethernet

В общем виде Gigabit Ethernet представляет собой различные технологии передачи Ethernet-кадров со скоростью 1 гигабит в секунду, определяемые рядом стандартов группы IEEE 802.3. Используется для построения проводных локальных сетей с 1999 года, постепенно вытесняя Fast Ethernet благодаря значительно более высокой скорости передачи данных.

На данный момент в стандарте используется исключительно полнодуплексный режим с соединением через коммутаторы.

Для работы с оптоволоком в 2004 году были добавлены стандарты IEEE 802.3ah: 1000BASE-LX10 и 1000BASE-BX10 – для передачи сигнала по одномодовому волокну; позже был добавлен 1000BASE-SX – для передачи по многомодовому волокну.

В совокупности с собственной пропускной способностью оптоволоконного кабеля, стандарты подразумевают кодирование, значительно повышающее скорость передачи линии.

Первоначально гигабитный Ethernet использовался только для опорных сетей с высокой пропускной способностью. Начиная с двухтысячного года, возможность гигабитного соединения начала появляться в персональных компьютерах.

Таким образом, Gigabit Ethernet является достаточно распространённым способом соединения в современных сетях и имеет достаточную, по современным меркам, пропускную способность [1].

1.2 Small Form-factor Pluggable

Small Form-factor Pluggable (SFP), то есть «подключаемый модуль малого форм-фактора» – это название достаточно точно описывает его внешний вид. Это компактный «блок» в стальном корпусе с разъемами на противоположных узких гранях. На «задней» стенке расположен коннектор для подключения к основному оборудованию – промышленному маршрутизатору или коммутатору, с другой – один или два разъема для сетевого кабеля, обычно прикрытые заглушкой. Один модуль может использоваться с разным оборудованием за счет стандартизации размеров и разъемов.

Основное предназначение SFP-модуля – конвертация сигнала (в случае подключения по оптоволокну), его прием и передача. Соответственно устройства также называются приемопередатчиками или трансиверами. Они относятся к категории активного оборудования, то есть, требуют внешнего питания (3,3 В; подается напрямую от основного устройства), но при этом поддерживают «горячую замену» – отключать маршрутизатор для замены или подключения модуля не нужно[2].

1.3 IPSec-VPN

В общем виде VPN представляет собой совокупность технологий управления доступом и контролем, аутентификации, туннелирования, используемых для защиты и безопасной передачи данных через сеть Интернет.

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, имеются уязвимости. Во время разработки протокола IP на его уровне не были предусмотрены какие-либо функции безопасности, что 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 к сети организации на другом конце.

IPSec (IP Security) является набором протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPSec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. В основном применяется для организации VPN-соединений.

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.

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 приложений данных, использующих протоколы TCP и UDP [3].

1.4 Экологичность

Требованием заказчика к сети является экологичность. Её можно достичь, используя экологичные материалы при проектировании структурированной кабельной системы, используя устройства, работающие с технологиями Green Ethernet, Power over Ethernet и другими, направленными на экологичность или сбережение энергии.

Pover over Ethernet (PoE) — технология подачи электропитания на клиентское устройство через витую пару стандарта Ethernet (обычно используется кабель cat.5. с разъемами RJ45). Один и тот же кабель используется и для передачи данных и для питания устройства[4].

Первое поколение PoE (стандарт IEEE 802.3af) обеспечивает питание до 15,4 Вт постоянного тока для каждого подключенного устройства.

Второе поколение стандарт IEEE 802.3at, также называемое PoE+ может выдавать мощность до 30 Вт для каждого устройства. Данный стандарт используется для питания более «прожорливых» потребителей, например, камер видеонаблюдения Pan-Tilt-Zoom (PTZ) и беспроводных точек доступа 11n.

Технология PoE позволяет проектировать более безопасные сети, экономить электроэнергию, экономить провода и пространство.

Green Ethernet – технология энергосбережения для Ethernet[5]. Суть её заключается в более рациональном использовании электрической энергии. Коммутатор (любое сетевое устройство с поддержкой функции Green Ethernet) периодически опрашивает свои порты (разъемы), и в случае если подключенное устройство не работает, то есть выключено или вообще не подключено, – порт отключается от питания. Помимо этого, специальное программное обеспечение определяет длину кабелей и в зависимости от их длины регулирует мощность сигнала. По заявлениям производителя, Green Ethernet позволяет сократить энергопотребление на величину от 45% до 80%.

1.4 Резервирование соединений

Резервирование соединений является одним из методов обеспечения надежности подключения пользователя в сеть. Резервирование соединений может быть реализовано по-разному: добавление альтернативных путей или резервирование соединений для пользователей, которым необходим доступ к сети в любой момент.

Для резервирования соединений можно агрегировать каналы коммутатор-коммутатор и/или коммутатор-маршрутизатор.

В данной работе предполагается использовать резервирование коммутатор – маршрутизатор, так как в компании будет всего один коммутатор.

2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе описана структура локальной компьютерной сети. Схема структурная приведена в приложении А.

2.1 Маршрутизатор

Для корректной работы локальной сети с несколькими виртуальными локальными компьютерными сетями и доступом в сеть Интернет необходима реализация IP-маршрутизации, следовательно необходимо активное сетевое устройство, которое поддерживает сетевой уровень модели Open Systems Interconnection.

Для этого можно использовать маршрутизатор или коммутатор с поддержкой третьего уровня. Одним из требований заказчика является реализация IPSec-VPN, что возможно реализовать только на маршрутизаторах, следовательно для маршрутизации в сети будет использован именно он.

Дополнительными аргументами в пользу маршрутизатора может служить необходимость обеспечения безопасности сети, реализации QoS, NAT, что невозможно реализовать при помощи коммутаторов третьего уровня.

2.2 Коммутаторы

Общее число подключённых к сети устройств достаточно велико для того, чтобы подключить их непосредственно к маршрутизатору, потому рациональным решением будет использование коммутатора. Также смысл использования коммутатора заключается в том, чтобы снизить нагрузку на маршрутизатор, настроить виртуальные локальные сети.

Всего в сети будет задействован только один коммутатор, его будет достаточно для организации в небольшом здании бюджетной сети с пятнадцатью стационарными подключениями.

Коммутатор связан с маршрутизатором, который занимается IP-маршрутизацией этой локальной сети и обеспечивает доступ в Internet. К коммутатору подключены проводные оконечные устройства пользователей и беспроводные точки доступа.

2.3 Беспроводные точки доступа

Заказчик не уверен насчёт количества беспроводных подключений, но в наше время, учитывая распространённость портативных вычислительных устройств (ноутбуки, смартфоны) и их вычислительную мощность, достаточную для решений различных задач, для удобства работников следует предоставить им возможность беспроводного подключения. Так как общая

площадь этажа – 105 квадратных метров, будет достаточно установки двух беспроводных точек доступа. Также количество возможных подключений должно быть не менее 30.

Подключать беспроводные точки доступа напрямую к маршрутизатору нет необходимости, потому что они соединены с коммутатором.

2.4 Прочее оконечное оборудование (принтеры, проекторы)

Так как в агентстве будут использоваться не сетевые принтеры, то они, как и проекторы, будут подключены непосредственно к персональным компьютерам.

3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

Данный раздел посвящён выбору оборудования, описанию функционирования программной и аппаратной составляющей разрабатываемой локальной компьютерной сети. Схема функциональная приведена в приложении Б.

Значение используемых в схеме условно-графических изображений указано в левой части схемы.

3.1 Расположение устройств

Роутер, обеспечивающий доступ в Internet, расположен в отдельном техническом помещении, там же к нему подключён коммутатор, а к коммутатору – административная рабочая станция.

Рабочие станции обоих этажей подключены к коммутатору, также к нему подключены беспроводные точки доступа.

К компьютерам подключены принтеры (5 штук, по одному на кабинет) и 2 проектора.

3.2 Выбор сетевого оборудования

Требованием заказчика является выбор сетевого оборудования от компании Dell Technologies Inc. (далее - DELL). Эта компания является одной из крупнейших компаний в области производства компьютеров, серверов, сетевого оборудования и периферии. Всё поставляемое компанией оборудование представлено на официальном сайте [6].

Так как в настоящее время DELL делает упор на производство компьютеров, с производства сняты беспроводные точки доступа и маршрутизаторы от этого производителя, из-за чего в проектировании данной сети будет использоваться только коммутатор от данной компании.

Для выбора подходящих маршрутизаторов и беспроводных точек доступа было принято решение обратиться к ассортименту компании Mikrotik, так как он имеет достаточно бюджетные варианты, подходящие по всем требованиям заказчика, а также при производстве сетевых устройств следует экологическим стандартам. Основное направление производства этой компании – проводное и беспроводное сетевое оборудование. Все устройства, поставляемые компанией, представлены на официальном сайте [7].

3.2.1 Выбор модели маршрутизатора

Основными критериями для выбора маршрутизации послужили наличие SFP, поддержка IPSec-VPN и IPv6-маршрутизации, а также наличие технологии PoE.

Согласно вышеперечисленным критериям, была выбрана модель Mikrotik hEX S (RB760iGS) [8], обладающая следующими техническими характеристиками:

1. IPSec VPN;
2. Слоты SFP: 1;
3. POE (1 пассивный и 1 активный порт);
4. 5 LAN Gigabit Ethernet портов;
5. 5 WAN Gigabit Ethernet портов (комбинированные с LAN);
6. Приоритизация трафика: Quality of Service;
7. IPv4 и IPv6 маршрутизация;
8. Операционная система RouterOS Level 4.



Рисунок 3.1 – Mikrotik hEX S (RB760iGS)

3.2.2 Выбор модели коммутатора

Так как внутренней маршрутизацией в сети занимается IP-маршрутизатор, то при выборе коммутатора нет смысла рассматривать L3-коммутаторы. Коммутатор должен иметь достаточное количество RJ-45 портов для подключения всех оконечных станций и беспроводных точек доступа и поддерживать технологию PoE. Количество портов должно быть примерно в два раза больше, чем необходимо, так как в будущем в компании могут появиться сетевые принтеры, камеры видеонаблюдения или какое-либо другое оконечное сетевое оборудование.

Согласно этим критериям, из бюджетной серии коммутаторов была выбрана модель DELL PowerSwitch N1148P-ON [9], которая имеет следующие технические характеристики:

1. 48 портов RJ-45 Gigabit Ethernet;
2. Скорость коммутации 176 Гб/с;
3. 4 слота SFP+ 10 Гб/с;
4. Поддерживает технологию PoE/PoE+ (24 портов);

5. Поддерживает технологию Green Ethernet;
6. Работает на операционной системе Dell EMC Networking OS 6;
7. Активное охлаждение.



Рисунок 3.2 – DELL PowerSwitch N1148P-ON

3.2.3 Выбор модели беспроводной точки доступа

Основными критериями для выбора беспроводной точки доступа послужили наличие PoE, более современные стандарты Wi-Fi, наличие Gigabit Ethernet портов.

Согласно этим критериям, была выбрана модель Mikrotik cAP ac (RBCAPGI-5ACD2ND) [10], которая имеет следующие характеристики:

1. Рабочая частота 2.4 и 5 ГГц;
2. Стандарты Wi-Fi 802.11ac (Wi-Fi 5) и старше;
3. POE (1 пассивный и 1 активный порт);
4. 2 Gigabit Ethernet портов;
5. Операционная система RouterOS Level 4.



Рисунок 3.3 – Mikrotik cAP ac (2 варианта)

3.3 Выбор окончного оборудования

Так как требованием заказчика является проектировка бюджетной сети, то при выборе окончного оборудования основным критерием, помимо наличия у устройств необходимых портов и достаточных характеристик, была стоимость оборудования.

3.3.1 Выбор персонального компьютера

Персональные компьютеры необходимы для работы и доступа к интернету. При выборе модели учитывались такие характеристики, как наличие Gigabit Ethernet портов, количество оперативной и встроенной памяти, её скорость, а также характеристики видеокарты и процессора. Таким образом был выбран доступный офисный персональный компьютер модели TGPC KING Office S I-X 74943 [11], который имеет следующие характеристики:

1. Двухъядерный процессор Intel Pentium Gold G6405 с тактовой частотой 4100 МГц;
2. 8 Гб оперативной памяти DDR4 с частотой 2666 МГц;
3. Встроенный накопитель SSD 240 Гб;
4. Сетевой разъем 1 Gigabit Ethernet;
5. Наличие HDMI и USB разъемов.

3.3.2 Выбор принтера и проектора

При выборе прочего окончного оборудования основными критериями были соответствие требованиям, доступность и более низкое энергопотребление, что напрямую связано с экологичностью.

В результате был выбран принтер Pantum P2200[12], который имеет следующие характеристики:

1. Чёрно-белая лазерная печать;
2. Скорость печати – 20 страниц в минуту;
3. USB разъем.

Также был выбран проектор CACTUS CS-PRE.09B.WVGA[13] со следующими характеристиками:

1. Матрица WVGA (800x480);
2. Расстояние 1-3 м;
3. Экран 32-120»;
4. HDMI разъем.

3.4 Расчёт качества связи беспроводной сети

При расчете количества точек доступа необходимо учесть:

- количество пользователей;
- фактор перекрытия;
- затухание радиосигнала.

Всего должен быть покрыт один этаж. Поскольку планировка этажей входит в курсовую работу, возьмем приблизительное значение высоты этажа, равное 3 метрам, где 0,5 метра – это высота потолка. Заранее примерное расположение беспроводных точек доступа будет в коридоре, они будут находиться на равном расстоянии от центра площади компании и от крайних стен. Тогда расстояние до дальних углов от приблизительного расположения точек доступа будет равняться 5,88 м.

Максимальная поддерживаемая скорость на частоте 2,4 ГГц - 300 Гб/с, на частоте 5 ГГц – 867 Гб/с. Однако реальные скорости будут ниже. Лучше всего, чтобы одна точка обслуживала менее 10 пользователей. Исходя из этого показателя, предположим, что нам необходимо две точки доступа.

Затухание радиоволн в беспрепятственной воздушной среде рассчитывается по формуле 3.1 и измеряется в децибелах.

$$L = 32,44 + 20 \lg(F) + 20 \lg(D), \quad (3.1)$$

где F – частота в ГГц, D – расстояние в метрах.

Рассчитаем затухание до дальнего угла от приблизительного места расположения точек доступа по формуле 3.1:

$$L_{2,4} = 32,44 + 20 \lg(2,4) + 20 \lg(5,88) \approx 55,43 \text{ дБ.}$$

$$L_5 = 32,44 + 20 \lg(5) + 20 \lg(5,88) \approx 61,81 \text{ дБ.}$$

Для обеспечения хорошего сигнала точкой доступа необходимо расположить её в центре площади, которую необходимо покрыть сигналом.

Таблица 3.1 – Типы препятствий для радиочастотных сигналов

Тип препятствия	Дополнительные потери (дБ)	Эффективное расстояние
Открытое пространство	0	100%
Окно без тонировки (отсутствует металлизированное покрытие)	3	70%
Окно с тонировкой (металлизированное покрытие)	5-8	50%
Деревянная стена	10	30%
Межкомнатная стена (15,2 см)	15-20	15%

Продолжение таблицы 3.1

Несущая стена (30,5 см)	20-25	10-15%
Бетонный пол/потолок	15-25	10-15%
Монолитное железобетонное перекрытие	20-25	10%

Учитывая, что комнаты разделяют обычные межкомнатные стены, то около 15-20 дБ (см. таблицу 3.1) будет теряться, тогда $L_{стен} = 20$ дБ.

Также стоит учесть возможное затухание за счёт взаимного размещения оборудования $L_{обор} = 5$ дБ.

С учетом мощности передатчика ГГц $P_{2,4} = 22$ дБм и $P_5 = 18$ дБм для точки доступа Mikrotik cAP рассчитаем уровень сигнала для частот 2,4 ГГц и 5 ГГц в на наибольшем расстоянии:

$$S_{2,4} = P_{2,4} - L_{2,4} - L_{стен} - L_{обор} = 22 - 55,43 - 20 - 5 = -58,43 \text{ дБм.}$$

$$S_5 = P_5 - L_5 - L_{стен} - L_{обор} = 18 - 61,81 - 20 - 5 = -62,43 \text{ дБм.}$$

Качество обслуживания беспроводных клиентов напрямую зависит от мощности сигнала в точке обслуживания и может быть оценена по следующей шкале:

до -30 дБм – идеальный сигнал;

от -30 до -50 дБм – отличный сигнал;

от -50 до -60 дБм – комфортный сигнал для большинства задач;

-67 дБм – минимальный уровень сигнала для HD-видео и голосовой связи;

до -70 дБм – слабый сигнал, достаточный для email и легкого интернет-серфинга;

от -70 до -80 дБм – сигнал нестабильный, возможна передача коротких текстовых сообщений;

до -90 дБм – сигнала почти нет, пользоваться сетью почти невозможно

По результатам расчетов получается, что минимальная мощность Wi-Fi сигнала в здании при размещении единственной точки доступа в середине здания будет находиться в пределах, обеспечивающих комфортный сигнал.

В результате было решено использовать две точки доступа, которые будут расположены в коридоре в центрах двух условных половин площади компании.

3.5 Адресация в локальной компьютерной сети

Для разделения разных сетевых частей компании было решено выделить три виртуальных подсети: административную, пользовательскую, беспроводную.

В состав административной виртуальной подсети входит административный персональный компьютер (PC1), роутер и коммутатор.

В состав пользовательской виртуальной подсети входят 15 стационарных подключений (15 персональных компьютеров).

В состав беспроводной виртуальной подсети входят две беспроводных точки доступа и беспроводные устройства, подключённые к ним. Для таких устройств выделено 30 адресов.

Согласно условию, для адресации (как внутренней, так и внешней) нужно использовать подходящие подсети из своего варианта (если возможно).

Вариант №832 лабораторных работ предлагает к использованию следующие подсети:

Таблица 3.2 – Предлагаемые к использованию подсети

№	IPv4-адрес	Количество адресов
1	22.0.0.0/8	16777214+2
2	53.198.0.0/15	131070+2
3	74.118.0.0/15	131070+2
4	113.226.0.0/18	16382+2
5	129.15.0.0/16	65534+2
6	154.209.184.0/22	1022+2
7	165.234.12.128/28	14+2
8	190.178.128.0/18	16382+2
9	196.125.254.96/28	14+2
10	202.234.213.224/27	30+2

Согласно варианту, для внешней IPv4 адресации используется выделенный интернет-провайдером статический IPv4-адрес. В качестве такого адреса выберем адрес 22.0.0.0/24. Так как внутренняя адресация IPv4 – приватная подсеть, а в варианте нет подходящих адресов, то выберем подсеть, которую можно использовать в приватной подсети – 192.168.0.0/16. Также разобьём эту подсеть на более мелкие. Итоги разбиения - в таблице 3.2 и 3.3.

Для внешней IPv6 адресации выбрана подсеть из блока адресов для Беларуси, порция адреса именуемая «Subnet ID» будет составлена из дополненного нулями номера, соответствующего VLAN. Схема IPv6 адресации представлена в таблице 3.3

Таблица 3.3 – Схема IPv4 адресации сетей

Название подсети	VLAN	Адрес подсети	Маска подсети
Административная	11	192.168.11.0	255.255.255.248

Продолжение таблицы 3.3

Пользовательская	2	192.168.2.0	255.255.255.224
Беспроводная	3	192.168.3.0	255.255.255.192

Таблица 3.4 – Адресация для каждого устройства

Устройство	VLAN	Адрес подсети	Маска подсети
Маршрутизатор	11	192.168.11.1	255.255.255.248
ПК		192.168.11.2	255.255.255.248
Коммутатор		192.168.11.3	255.255.255.248
Маршрутизатор	2	192.168.2.1	255.255.255.224
ПК		От 192.168.2.2 До 192.168.2.3	255.255.255.224
Маршрутизатор	3	192.168.3.1	255.255.255.192
Беспроводные точки доступа		От 192.168.3.2 До 192.168.3.3	255.255.255.192
Беспроводные подключения		От 192.168.3.4 До 192.168.3.33	255.255.255.192

Таблица 3.5 – Схема IPv6 адресации

Название подсети	VLAN	Адрес подсети
Административная	11	2a02:0bf0:010d:11:::/64
Пользовательская	2	2a02:0bf0:010d:2:::/64
Гостевая	3	2a02:0bf0:010d:3:::/64

3.4 Настройка оборудования

3.4.1 Настройка роутера

Для обеспечения резервирования каналов объединим два интерфейса в один агрегацией каналов:

```
/interface bonding
add mode=802.3ad slaves=ether1,ether2 primary=ether1
name=bond1
```

Для настройки внешнего IPv4:

```
/ip address
add address=22.0.0.1/24 interface=SFP
```

Для настройки внешнего IPv6:

```
/ipv6 address
```

```
add          address=2a02:0bf0:010d:::1/64interface=SFP
advertise=no
```

**Настройка виртуальных подсетей будет произведена через консоль.
Агрегированный интерфейс является тегированным (далее trunk):**

```
/interface bridge
add name=bridge1
/interface bridge port
add bridge=bridge1 interface=bond1 hw=yes
/interface vlan
add interface=bridge1 vlan-id=10 name=ADMIN
add interface=bridge1 vlan-id=2 name=USER
add interface=bridge1 vlan-id=3 name=WIRELESS
```

**Далее, необходимо назначить сетевые адреса, чтобы VLAN интерфейсы
могли работать как шлюзы:**

```
/ip address
add address=192.168.11.1/29 interface=ADMIN
add address=192.168.2.1/27 interface=USER
add address=192.168.3.1/26 interface=WIRELESS
```

Назначим сетевые адреса IPv6 для каждого VLAN-а:

```
/ipv6 address
add address=2a02:0bf0:010d:11:::1/64interface=ADMIN
advertise=no
add address=2a02:0bf0:010d:02:::1/64interface=USER
advertise=no
add address=2a02:0bf0:010d:03:::1/64interface=WIRELESS
advertise=no
```

Необходимо установить адресные пулы беспроводного VLAN:

```
/ip pool
add name=WIRELESS ranges=192.168.3.3-192.168.3.31
```

Далее, настраиваем DHCP:

```
add address=192.168.3.0/26 comment=WRL gateway=192.168.3.1
```

**Далее добавляем ранее настроенные пулы интерфейсу беспроводного
VLAN:**

```
/ip dhcp-server
add address-pool=WIRELESS disabled=no interface=WIRELESS
name=WRL
```

Добавляем FireWall:

```
/ip firewall filter
add action=accept chain=input comment="default
configuration" connection-state=established,related
add action=accept chain=input src-address-
list=allowed_to_router
add action=accept chain=input protocol=icmp
add action=drop chain=input
/ip firewall address-list
add address=192.168.11.1-192.168.11.4 list=allowed_to_router
add address=192.168.2.1-192.168.2.17 list=allowed_to_router
add address=192.168.3.1-192.168.3.61 list=allowed_to_router
```

По заданию необходимо сделать IPSec-VPN сервер, для этого создадим сертификат и профиль для подключения:

```
/certificate
add common-name=ca name=ca
sign ca ca-crl-host=2.2.2.2
add common-name=2.2.2.2 subject-alt-name=IP:2.2.2.2 key-
usage=tls-server name=server1
sign server1 ca=ca
/ip ipsec profile
add name=ike2
/ip ipsec proposal
add name=ike2 pfs-group=none
```

Создадим пул адресов:

```
/ip pool
add name=ike2-pool ranges=192.168.20.2-192.168.20.61
/ip ipsec mode-config
add address-pool=ike2-pool address-prefix-
length=32 name=ike2-conf
```

Опишем политику и создадим новый пир:

```
/ip ipsec policy group
add name=ike2-policies
/ip ipsec policy
add dst-address=192.168.20.0/24 group=ike2-
policies proposal=ike2 src-address=22.0.0.0/8 template=yes
/ip ipsec peer
add exchange-mode=ike2 name=ike2 passive=yes profile=ike2
```

Добавим метод идентификации:

```
/ip ipsec identity
```

```
add auth-method=digital-  
signature certificate=server1 generate-policy=port-  
strict mode-config=ike2-conf peer=ike2 policy-template-  
group=ike2-policies
```

Сгенерируем клиентские сертификаты:

```
/certificate  
add common-name=rw-client1 name=rw-client1 key-usage=tls-  
client  
sign rw-client1 ca=ca  
export-certificate  
rw-client1 export-passphrase=1234567890 type=pkcs12
```

3.4.2 Настройка коммутатора

Для обеспечения резервирования каналов, объединим два интерфейса, направленные к роутеру, в один путём агрегации каналов:

```
console(conf)#interface range GigabitEthernet 0/0-1  
console(conf-if)#channel-group 1 mode auto
```

Для начала, чтобы работать с VLAN, нужно добавить их в базу коммутатора:

```
console(config)# vlan database  
console(config-vlan)# vlan 2  
console(config-vlan)# vlan 3  
console(config-vlan)# vlan 11  
console(config-vlan)# end  
console(config)# interface vlan 2  
console(config-if)# name USER  
console(config-if)# end  
console(config)# interface vlan 3  
console(config-if)# name WIRELESS  
console(config-if)# end  
console(config)# interface vlan 11  
console(config-if)# name ADMIN  
console(config-if)# end
```

После этого сконфигурируем все интерфейсы:

```
console(config)# interface port-channel 1  
console(config-if)# switchport mode trunk  
console(config-if)# switchport trunk allowed vlan 1-3, 11  
console(config-if)# end  
console(config)# interface gigabitEthernet 0/2  
console(config-if)# switchport mode access  
console(config-if)# switchport access vlan 11  
console(config-if)# end
```

```

console(config)# interface range gigabitEthernet 0/3-4
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 3
console(config-if)# end
console(config)# interface range gigabitEthernet 0/5-18
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 2
console(config-if)# end

```

Удалённое управление при помощи secure shell:

```

console(config)# username admin password <password>
privilege 15
console(config)# interface managementethernet 1/1
console(conf-if-ma)# ip add 192.168.11.3/29
console(conf-if-ma)# no shutdown
console(conf-if-ma)# exit
console(config)# ip ssh server enable
console(config)# ip ssh server version
console(config)# crypto key generate rsa
console(config)# ip ssh password-authentication enable
console(config)# ip ssh rsa-authentication enable

```

3.4.3 Настройка беспроводной точки доступа

Для того, чтобы в дальнейшем подключаться к точке доступа по IP, настроим DHCP-клиент:

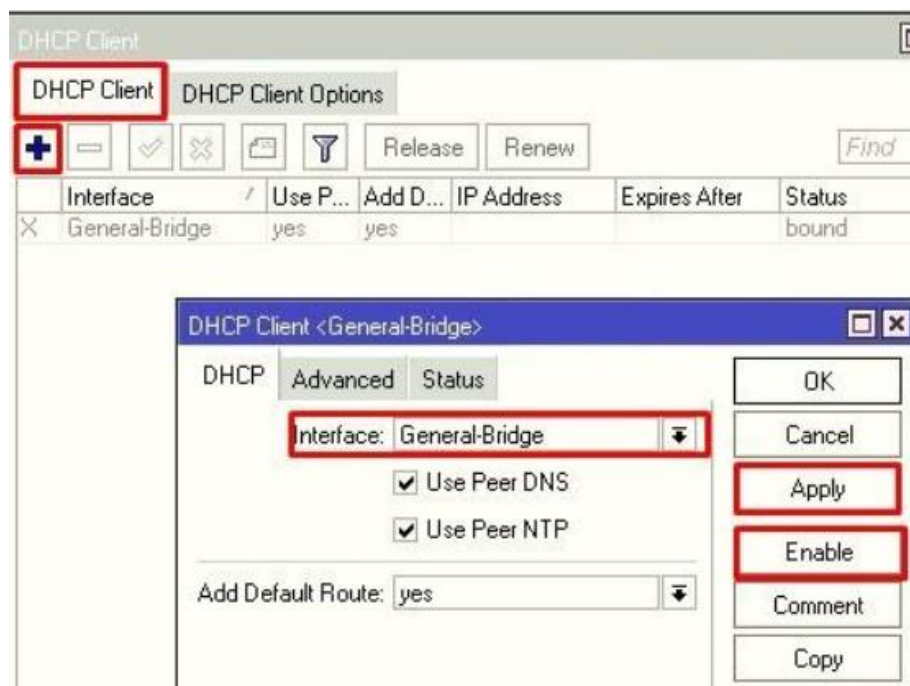


Рисунок 3.4 – Настройка DHCP

Для защиты точки доступа перейдём во вкладку Wireless/Security Profiles и добавим новый профиль:

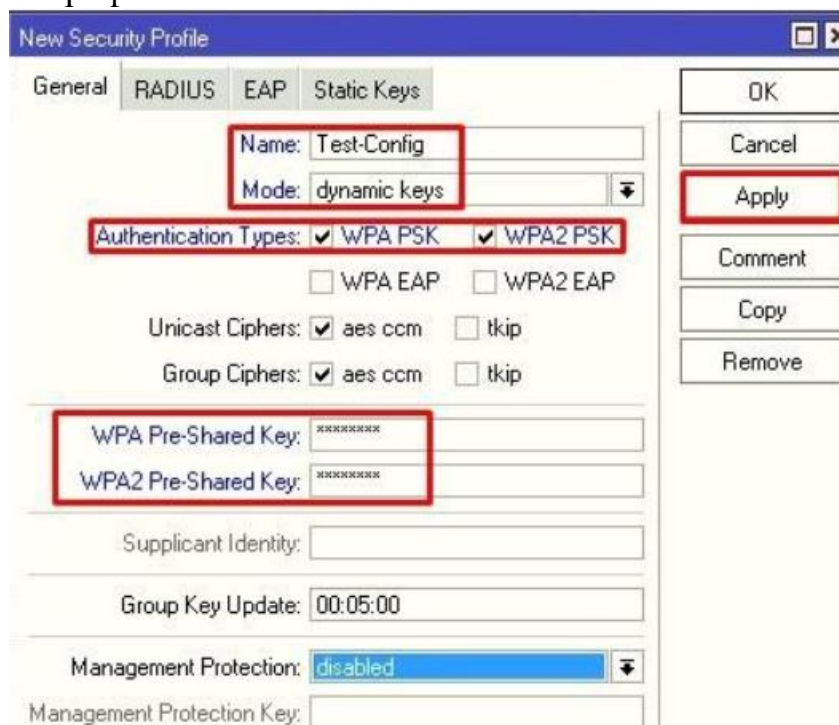


Рисунок 3.4 – Настройка Security Profiles

Настроим точку доступа для работы в частоте 2.4 ГГц (рисунок 3.5) и 5 ГГц (рисунок 3.6), перейдя в Wi-Fi/Interfaces/vlan1 и Wi-Fi/Interfaces/vlan2 соответственно:

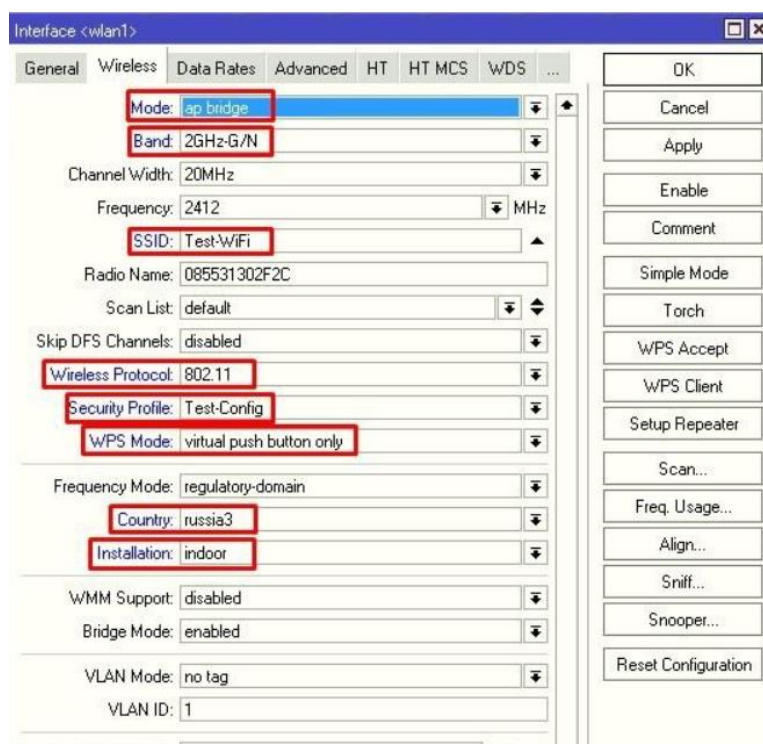


Рисунок 3.5 – Настройка 2.4 ГГц

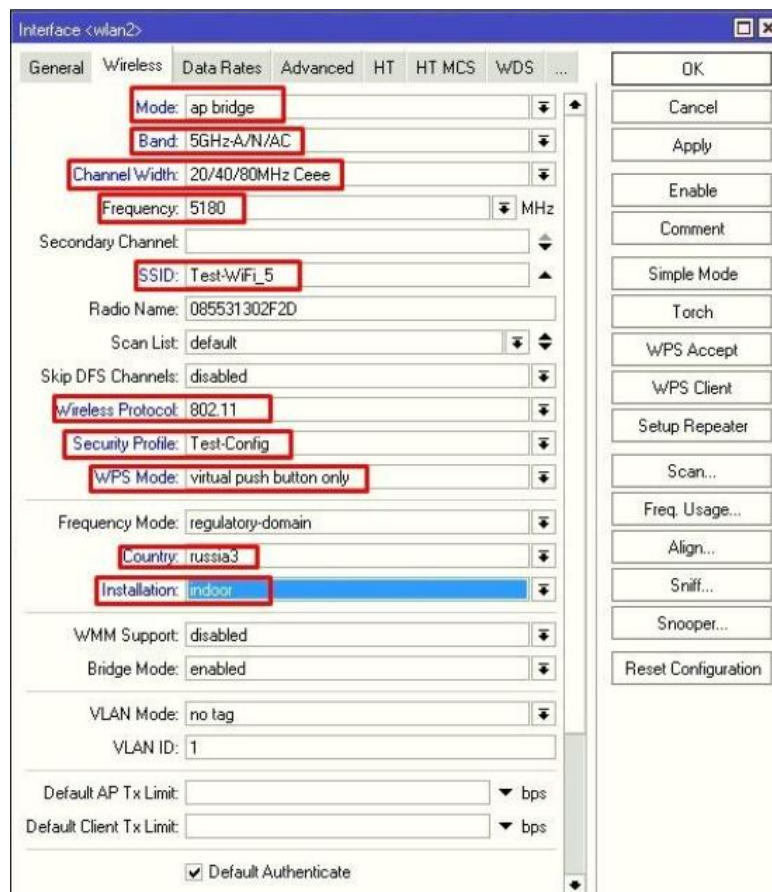


Рисунок 3.6 – Настройка 5 ГГц

После всего изменим стандартный пароль для конфигурации на другой через System/Password:

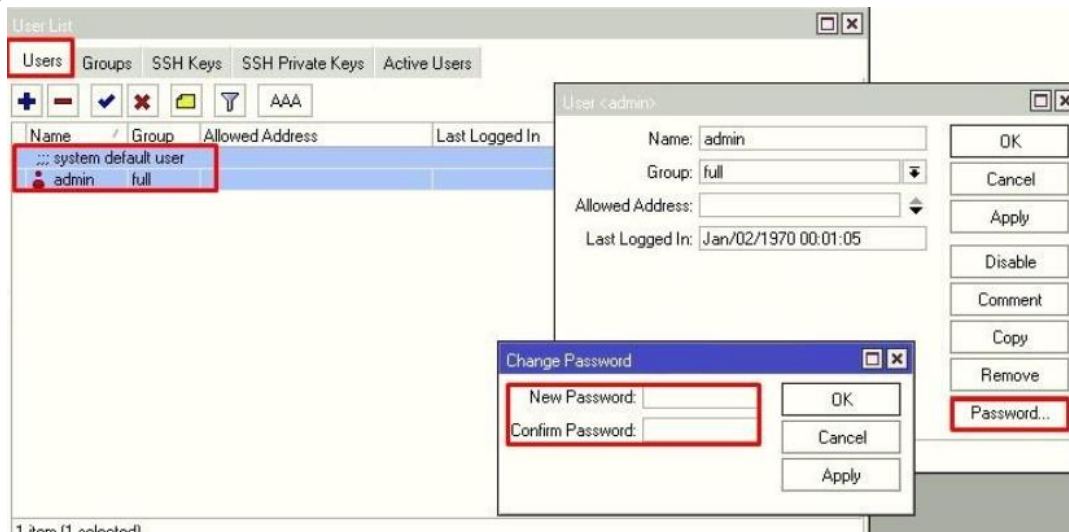


Рисунок 3.7 – Изменение пароля

3.4.4 Настройка принтера и проектора

Для подключения принтера и проектора к персональному компьютеру необходимо подключиться к ним при помощи USB-кабеля и HDMI-кабеля

соответственно и запустить установку драйверов В окне с предложением выбрать тип подключения.

3.4.5 Настройка персональных компьютеров

Персональные компьютеры подключаются посредством Ethernet. Для настройки ПК необходимо зайти в панель управления, выбрать раздел «Сеть и Интернет», в разделе «Сетевые подключения» нажать кнопку «Изменение настроек адаптера». В открывшемся окне перейти к настройкам Ethernet, нажать на «IP версии 4», на кнопку свойства и задать в открывшемся окне свойств «Использовать следующий IP-адрес». После чего ввести адрес компьютера, маску подсети и шлюз по умолчанию.

Чтобы настроить IPv6 адрес, необходимо аналогичным образом необходимо в панель настроек IPv6 адреса, далее следует выбрать «Получить адрес автоматически».

Процедуру настройки адресов необходимо повторить на всех персональных компьютерах. Пример настройки представлен на рисунке 3.2.

4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

План этажа с изображённой кабельной системой представлен в приложении В.

Общая площадь помещений, занимаемых компанией составляет 105 м², она находится на втором этаже, разделена на 5 кабинетов, коридор и санузел.

В отдельном кабинете администратора расположены коммутатор и маршрутизатор, для удобства помещённые в телекоммуникационный шкаф, закреплённый в углу непосредственно под потолком. Для этой цели был выбран шкаф TWD-1566 GP [14] – доступный настенный шкаф 600х600х770 с замком. Подключение маршрутизатора производится с помощью технологии PoE.

Беспроводные точки доступа находятся в коридоре, закреплены на потолке. Подключение точки доступа производится с помощью технологии PoE.

В проектируемой локальной компьютерной сети кабельная система реализована с помощью прокладки витой пары над фальшпотолком, максимально далеко от ламп. К сетевым розеткам кабель спускается в кабель-канале. Из коридора в кабинеты кабель проходит в кабель-канале через отверстия в стене.

В качестве кабеля был выбран U/UTP cat.6 LSZH/LS0H [15] – кабель, способный поддерживать скорость до 10 Гб/с, поддерживает технологию PoE, оболочка выполнена из огнестойких материалов, не содержащих галогенов, с ограниченным выделением дыма и агрессивных газов.

В качестве коробов выбраны – Bylectrica КДК25х25 [16] и КДК40х25 [17], выполненные из экологичного поливинил хлорида.

Для подключения к устройствам был выбран коннектор RJ-45 Cabeus 8P8C-S6 [18].

В схеме используются одинарная и двойные накладные розетки, были выбраны модели TDM Electric SQ1809-0003 [19] (одинарная) и SQ1809-0003[20] (двойная).

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы была разработана локальная компьютерная сеть для рекламного агентства. Были получены практические и теоретические знания, и навыки проектирования локальной вычислительной сети.

За время выполнения данной курсовой работы, был исследован рынок сетевого оборудования, в результате чего было выбрано оборудование, которое удовлетворяет всем стандартам качества, надежности. Также, пришлось ознакомиться с настройкой оборудования ранее неизвестной фирмы. Изучались различные способы настройки данного оборудования.

Результатами проектирования являются структурная, функциональная схемы, план здания, перечень оборудования и материалов, необходимых для построения и реализации сети.

Сеть в данной работе была разбита на логические структурные единицы. Коммутаторы, маршрутизаторы и беспроводные точки доступа были настроены в соответствии с потребностями вышеупомянутых логических структур.

Курсовая работа показала, что сети используются в абсолютно разных, иногда даже малосвязанных между собой, сферах жизни. Написание курсовой работы побудило к изучению совершенно нового материала и новых методов работы с компьютерными сетями, восполнению пробелов в знаниях, касающихся компьютерных сетей.

Полученная компьютерная сеть проста в обслуживании, при необходимости ее можно будет легко усовершенствовать.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

[1] Xnets | Gigabit Ethernet по оптоволокну [Электронный ресурс]. – Режим доступа: <http://www.xnets.ru/plugins/content/content.php?content.172>. – Дата доступа: 09.12.2022.

[2] Habr | Как SFP, SFP+ и XFP делают нашу жизнь проще [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/company/zyxel/blog/498066/>. – Дата доступа: 09.12.2022.

[3] Habr | Анатомия IPsec [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/company/haker/blog/256659/>. – Дата доступа: 09.12.2022.

[4] Habr | Технология PoE в вопросах и ответах [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/company/zyxel/blog/485842/>. – Дата доступа: 09.12.2022.

[5] Wikipedia | Green Ethernet [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Green_Ethernet. – Дата доступа: 09.12.2022.

[6] Официальный сайт Dell [Электронный ресурс]. – Режим доступа: <https://www.dell.com/>. – Дата доступа: 09.12.2022.

[7] Официальный сайт Mikrotik [Электронный ресурс]. – Режим доступа: <https://mikrotik.com>. – Дата доступа: 09.12.2022.

[8] Mikrotik | Mikrotic XEx S [Электронный ресурс]. – Режим доступа: https://mikrotik.com/product/hex_s. – Дата доступа: 09.12.2022.

[9] Dell | Dell Networking N1100 Series Switches [Электронный ресурс]. – Режим доступа: <https://www.dell.com/ae/business/p/networking-n1100-series/pd>. – Дата доступа: 09.12.2022.

[10] Mikrotik | Mikrotik cAP ac [Электронный ресурс]. – Режим доступа: https://mikrotik.com/product/cap_ac. – Дата доступа: 09.12.2022.

[11] Onliner | Компьютер TGPC KING Office S I-X 74943 [Электронный ресурс]. – Режим доступа: <https://catalog.onliner.by/desktoppc/tgpc/tgpc74943>. – Дата доступа: 09.12.2022.

[12] Onliner | Принтер Pantum P2200 [Электронный ресурс]. – Режим доступа: <https://catalog.onliner.by/printers/pantum/p2200>. – Дата доступа: 09.12.2022.

[13] Onliner | Проектор CACTUS CS-PRE.09B.WVGA [Электронный ресурс]. – Режим доступа: <https://catalog.onliner.by/projectors/cactus/cspre09bwvga>. – Дата доступа: 09.12.2022.

[14] TeleStream | Шкаф настенный TWD-1566 GP [Электронный ресурс]. – Режим доступа: https://www.telestream.by/catalog/telekommunikatsionnye_shkafy/nastennye/64832/. – Дата доступа: 09.12.2022.

[15] Deal.by | Кабель U/UTP cat.6 LSZH/LS0H [Электронный ресурс]. – Режим доступа: <https://cabeltorg.by/catalog/kabeli-i-provoda/kabel-u-utp-cat-6-lszh-4x2x23awg-305m/>. – Дата доступа: 09.12.2022.

[16] 21vek.by | Кабель-канал Bylectrica КДК25х25 [Электронный ресурс]. – Режим доступа: https://www.21vek.by/cable_trays/2525_bylectrica_01.html. – Дата доступа: 09.12.2022.

[17] 21vek.by | Кабель-канал Bylectrica КДК40х25 [Электронный ресурс]. – Режим доступа: https://www.21vek.by/cable_trays/4025_bylectrica.html. – Дата доступа: 09.12.2022.

[18] CABEUS-shop | Cabeus Коннектор RJ-45 [Электронный ресурс]. – Режим доступа: http://www.cabeus-shop.ru/goods/cabeus_8p8c-c6.htm?yclid=7552357275268076555. – Дата доступа: 09.12.2022.

[19] Onliner | Розетка компьютерная TDM Electric SQ1809-0003 [Электронный ресурс]. – Режим доступа: https://catalog.onliner.by/wall_socket/tdmelectric/tdmesq18090003. – Дата доступа: 09.12.2022.

[20] Onliner | Розетка компьютерная TDM Electric SQ1809-0004 [Электронный ресурс]. – Режим доступа: https://catalog.onliner.by/wall_socket/tdmelectric/tdmesq18090004. – Дата доступа: 09.12.2022.

[21] Mikrotik | RouterOS – Mikrotik documentation [Электронный ресурс]. – Режим доступа: <https://help.mikrotik.com>. – Дата доступа: 09.12.2022.

ПРИЛОЖЕНИЕ А
(обязательное)

Локальная компьютерная сеть. Схема структурная

ПРИЛОЖЕНИЕ Б
(обязательное)

Локальная компьютерная сеть. Схема функциональная

ПРИЛОЖЕНИЕ В
(обязательное)

Локальная компьютерная сеть. План этажа

ПРИЛОЖЕНИЕ Г
(обязательное)

Локальная компьютерная сеть.
Перечень оборудования, изделий и материалов

ПРИЛОЖЕНИЕ Д
(обязательное)

Локальная компьютерная сеть.
Ведомость документов