

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
1. Проектирование кабельной структуры компьютерной сети предприятия.....	5
1.1....Разработка проекта кабельной структуры компьютерной сети предприятия.....	5
1.2. Выбор технологии, инструментальных средств и средств вычислительной техники для проектирования кабельной структуры компьютерной сети.....	9
2. Обеспечение защиты информации в сети с использованием программно-аппаратных средств.....	18
2.1 Анализ угроз безопасности и методов защиты информации в компьютерной сети.....	18
2.2 Разработка комплекса мероприятий по защите информации в компьютерной сети.....	19
3. Разработка мероприятий по приемо-сдаточным испытаниям компьютерной сети и сетевого оборудования.....	21
3.1 Разработка комплекса мероприятий по приемо-сдаточным испытаниям компьютерных сетей и сетевого оборудования.....	21
.....3.2 Выбор программно-аппаратных средств мониторинга и технического контроля.....	24
4. Оформление Проекта кабельной структуры компьютерной сети в соответствии с требованиями заказчика.....	32
4.1 Разработка проектной документации.....	32
4.2 Расчет технико-экономических показателей.....	44
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	48
ПРИЛОЖЕНИЕ А.....	49
ПРИЛОЖЕНИЕ Б.....	52

ВВЕДЕНИЕ

Актуальность данного проекта обусловлена стремительными темпами роста развития локально-вычислительных сетей. За последние два десятилетия произошли серьёзные преобразования, которые вызвали изменения в функциональности данной сферы. ИТ - процессы на сегодняшний день заняли прочное место в различных сферах предоставления услуг. Это, например, сервисные, юридические, бытовые услуги, а также ИТ процессы в сфере предоставления услуг. Здесь грамотная разработка и реализация позволяют обеспечить комплексную автоматизацию предприятия. сервер компьютер терминал сетевой. При правильной организации локально вычислительной сети позволит повысить производительность, эффективность и навыки работы данной компании.

Компьютерная сеть – это система, обеспечивающая обмен данными между вычислительными устройствами - компьютерами, серверами, маршрутизаторами и другим оборудованием или программным обеспечением. Для передачи информации могут быть использованы различные среды передачи данных. Помимо совокупности физических устройств и физических средств передачи данных, вычислительная сеть может быть оверлейной или виртуальной, то есть логически самостоятельной выделенной сетью, использующей ресурсы другой физической сети - вычислительной, телефонной сети и среды передачи данных.

Целью дипломного проекта является – построение компьютерной сети и организация развертывания системы мониторинга действий её сотрудников. в компании ООО «Авто-Форум».

В качестве информационной базы – будут использованы стандарты ГОСТ, связанные с компьютерными сетями, в них будет включаться ГОСТ Р 53246-2008 ИТ «Проектирование основных узлов системы», ГОСТ Р 56553-2015 «Кабельные системы. Планирование и монтаж», ГОСТ 29099-91 «Сети

вычислительные локальные, ГОСТ 21.110 – 2013 СПДС «Спецификация оборудования, изделий и материалов». Также будут использоваться стандарты компании «Cisco Systems» для совместимости сети с оборудованием компании «Cisco Systems». Помимо этого, также будет использоваться стандарт для осуществления контроля нормам СНиП 2.09.04-87.

Сведения о структуре дипломного проекта будут заключаться в 4 основных разделах с выходящими из них подпунктами, в которых будет подобно расписаны этапы по проектированию кабельной структуры компьютерной сети предприятия, обеспечению защиты информации в сети с использованием программно-аппаратных средств, разработке мероприятий по приемо-сдаточным испытаниям компьютерной сети и сетевого оборудования, а также оформление проекта кабельной структуры компьютерной сети в соответствии с требованиями заказчика.

1. Проектирование кабельной структуры компьютерной сети предприятия

1.1. Разработка проекта кабельной структуры компьютерной сети предприятия

Компания Организация с ограниченной ответственностью «АвтоФорум», арендует офисное помещение, расположенное по адресу 410020, Саратовская Область, г. Саратов, ул. Им Шехурдина А.п., д.2/4. Основным родом деятельности данной компании является продажа транспортных средств. Компания имеет свои печати и состоит на налоговом учете согласно законодательство Российской Федерации.

В офисном помещении необходимо произвести построение компьютерной сети с учетом метража помещений, и необходимого оборудования которое будет установлено в каждом отделе, все эти данные представлены ниже:

- 1) Руководитель филиала: 1 компьютер, 1 принтер, 1 IP-телефон. Размер: 42 м².
- 2) Зам. Руководителя филиала: 1 компьютер, 1 принтер, 1 IP-телефон. Размер: 36 м².
- 3) Отдел работы с онлайн заказами: 15 компьютеров, 2 принтера, 3 IP-телефонов. Размер: 49 м².
- 4) Отдел финансов: 3 компьютера, 1 принтер, 1 IP-телефон. Размер: 44 м².
- 5) Серверная. Размер: 20 м².
- 6) Отдел IT-специалистов: 1 компьютера, 1 IP-телефон. Размер: 44 м².
- 7) Отдел контроля качества обслуживания клиентов: 1 компьютер 1 IP-Телефон. Размер: 20 м².

После ознакомления с помещением необходимо произвести выбор сетевой топологии которая будет реализована для построения компьютерной

сети. Для сравнительного анализа будут выбрана две распространённые на данный момент сетевые топологии, подробные данные представлены в таблице 1.

Таблица 1 – Выбор сетевой топологии

Характеристика	Топология	
	«Звезда»	«Кольцо»
Стоимость расширения	Незначительная	Средняя
Присоединение абонентов	Пассивное	Активное
Защита от отказов	Высокая	Средняя
Стоимость подключение нового оборудования	Незначительная	Незначительная
Поведение системы при высоких нагрузках	Хорошее	Удовлетворительное
Обслуживание	Легкое	Среднее

Из таблицы следует, что топология «Звезда» обладает рядом преимуществ, а именно легкой расширяемостью, высокой отказоустойчивостью и легким подключением нового оборудования. Основной топологией будет выступать «Звезда». На рисунке 1 представлен пример данной топологии.

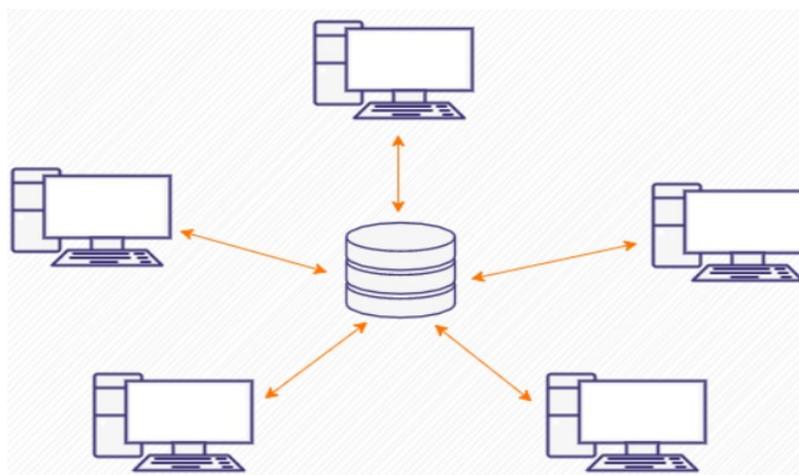


Рисунок 1– Топология «Звезда»

После выбора сетевой топологии, необходимо подойти к количеству сетевого активного сетевого оборудования, будет необходимо выбрать следующие сетевое оборудование: 3 коммутатора, 2 маршрутизатор, стоечный шкаф и 2 сервера.

Выбрав сетевую топологию которая будет использоваться перейдем к распределению подсетей, которые будут использоваться. Все внутренние отделы филиала будут использовать одну подсеть которая будет выдаваться при помощи DHCP протокола, установленного на сервере, для серверного оборудования и маршрутизатора будут использоваться выделенные IP-адреса. В таблице 2 представлена подсети которые будут использоваться в компьютерной сети.

Таблица 2 – Распределение компьютерных подсетей

Наименование отдела	Подсеть	Маска подсети
Руководитель филиала	192.168.1.0	24
Зам. Руководителя филиала	192.168.1.0	24
Отдел работы с онлайн заказами	192.168.1.0	24
Отдел финансов	192.168.1.0	24
Отдел IT-специалистов	192.168.1.0	24
Отдел контроля качества обслуживания клиентов	192.168.1.0	24
Серверная	10.153.78.0	29
IP-Телефония	192.168.2.0	24

В таблице также продемонстрирована IP-телефония которая будет использовать другую подсеть.

Установив количество сетевого оборудования, распределив подсети которые будут использоваться, необходимо перейти к выбору провайдера, который будет предоставлять сетевые услуги в филиал. Офисное здание уже

имеет сетевое подключение от компании «Дом.Ру». Для реализации будет использоваться офисный пакет сетевых услуг, представленных этой компанией со скоростью сети в размере от 300 Мбит/с. Данная скорость сетевого подключения обеспечит стабильную скорость передачи данных в глобальной сети «Internet».

После выбора провайдера и перечисления количества активного сетевого оборудования можно перейти к построению структурной схемы компьютерной сети. Данная схема представлена на рисунке 2.

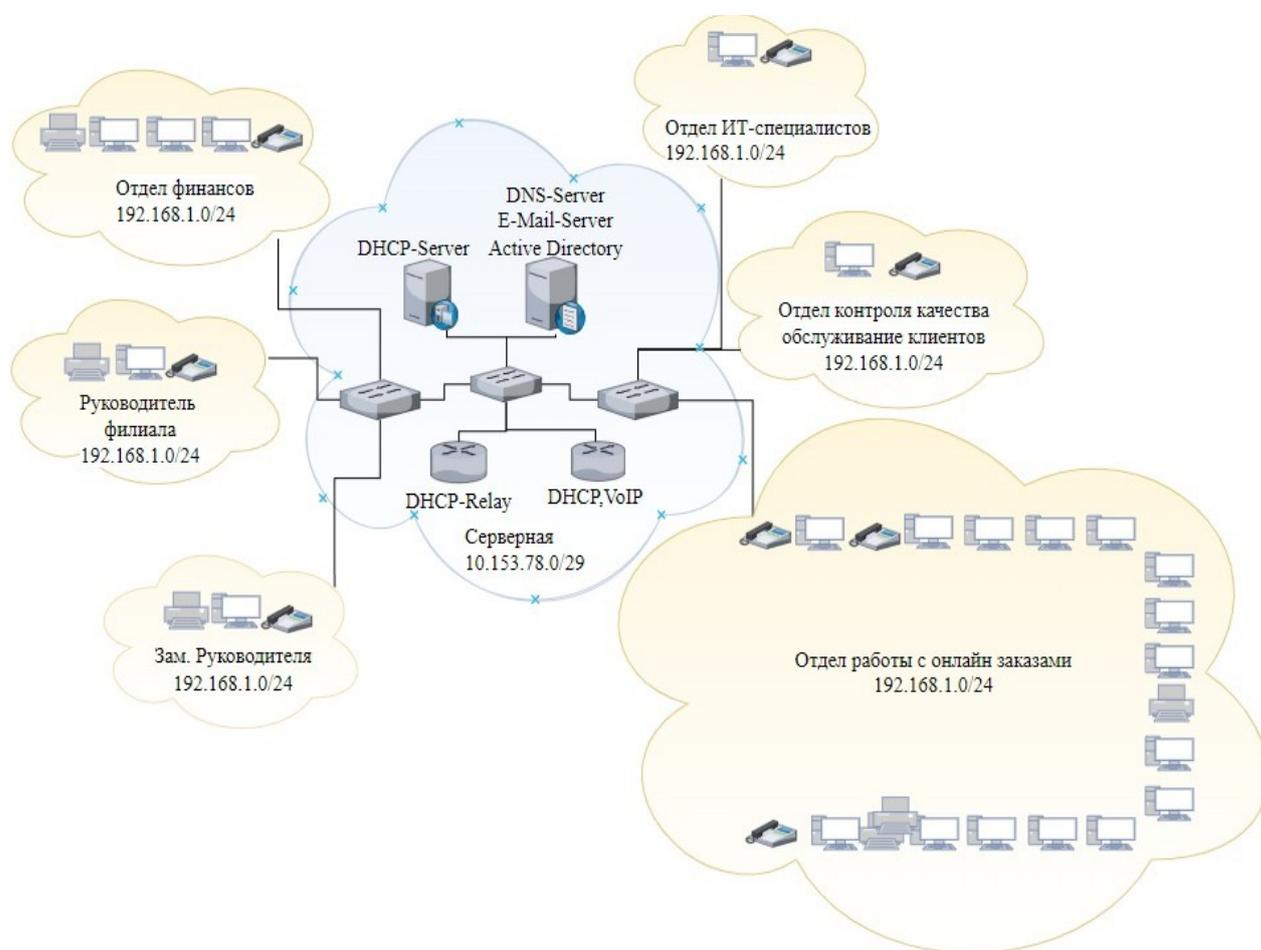


Рисунок 2 – Структурная схема компьютерной сети

1.2. Выбор технологии, инструментальных средств и средств вычислительной техники для проектирования кабельной структуры компьютерной сети

Для построения логической схемы компьютерной сети необходимо произвести выбор основного эмулятора в котором будет полный набор возможностей для реализации компьютерной сети, в таблице 3 будет производиться анализ самых распространённых эмуляторов.

Таблица 3 – Выбор эмулятора для построения логической схемы компьютерной сети

Наименование	Положительные стороны	Отрицательные стороны
GNS3	<ul style="list-style-type: none">- Поддерживает 42 маршрутизатора, 6 коммутаторов и 3 других устройства;- Симулирует сетевой трафик с помощью технологии виртуальных пакетов;	<ul style="list-style-type: none">- Отсутствие шифрования- Нет поддержки IP-телефонии.- Нет поддержки vrp.
Cisco Packet Tracer	<ul style="list-style-type: none">- Дружественность и логичность интерфейса;- Удобно проверять работу разных сетевых сервисов, вроде DHCP/DNS/HTTP/SMTP/POP3 и NTP;- Возможность перейти в режим simulation и увидеть перемещения пакетов с замедлением.	<ul style="list-style-type: none">- Практически всё, что выходит за рамки CCNA, на нем собрать не получится;- Так же иногда могут проявляться разнообразные глюки, которые лечатся только перезапуском программы.

Из таблицы следует, что эмулятор «Cisco Packet Tracer», подойдет для построения логической схемы, а также обладает основным преимуществом, а именно поддержка правил «VoIP», которые необходимы для реализации IP-телефонии. Теперь необходимо перечислить протоколы и правила которые необходимо развернуть на сетевом оборудовании. В таблице 4 проведен данный перечень.

Таблица 4 – Необходимые протоколы для реализации компьютерной сети

Наименование протокола	Задача
DHCP-Server	Автоматическая раздача сетевой конфигурации на рабочие станции
DHCP-Relay	Необходим для реализации протокола DHCP в другую подсеть
DNS	Служба доменных имен
DHCP-VoIP	Предназначен для распределения сетевых конфигураций для IP-телефонии
Vlan	Необходим для создания виртуальных локальных сетей.
VoIP	Служба необходимая для реализации IP-телефонии

После выбора эмулятора и перечисления необходимых сетевых протоколов перейдем к созданию логической схемы компьютерной сети. Первым этапом будет развертывание DHCP-Server на одном из серверов. Данный протокол понадобится для раздачи сетевой конфигурации рабочим станциям. Изначально зададим нашему серверу статический выделенный провайдером IP-адрес, Gateway, IP-адрес и DNS-сервера. На рисунке 3 продемонстрирована задача статической сетевой конфигурации для DHCP сервера.

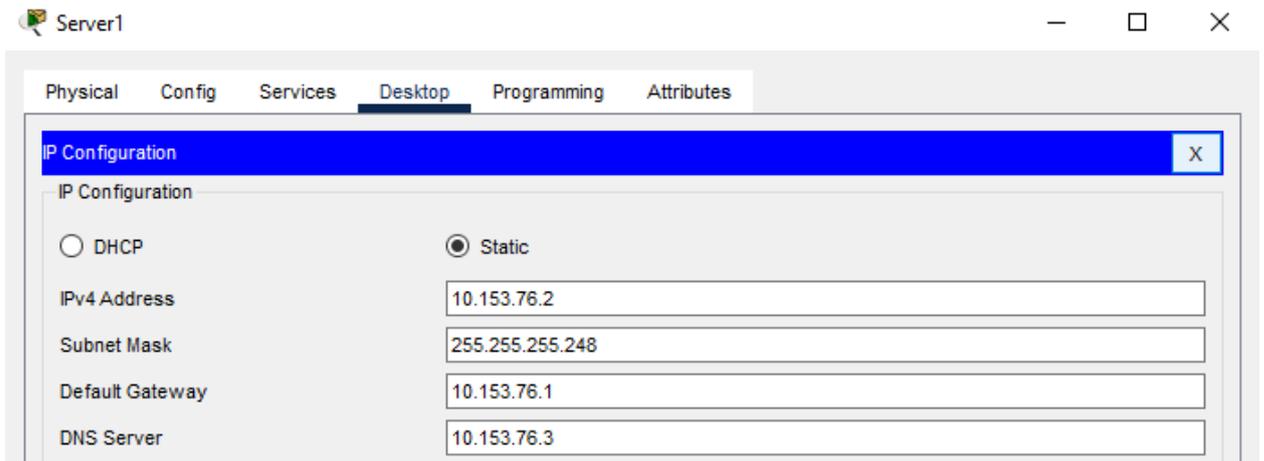


Рисунок 3 – Настройка статического IP-адреса для DHCP-Server

Как видно на рисунке 3 были заданы необходимые статическая сетевая конфигурация. После этого перейдем к развертыванию самого протокола DHCP. На рисунке 4 представлена конфигурации данного протокола, а именно задан, DNS, pool IP-адресов, Gateway, все эти данные будут задаваться на рабочие станции.

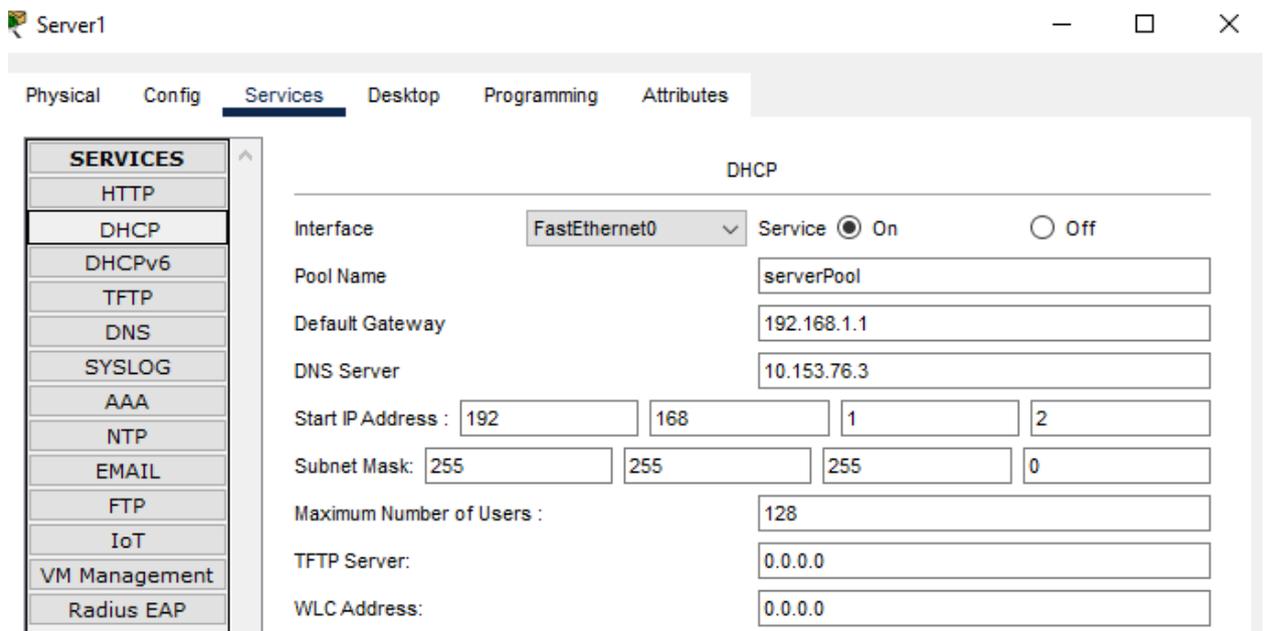


Рисунок 4 – Настройка DHCP-Server

После настройки данного протокола перейдем к настройка протокола DNS, на другом сервере, эму также зададим статическую сетевую

конфигурацию, также с выделенным IP-адресом. На рисунке 5 продемонстрирована задача статической сетевой конфигурации для DNS-Server.

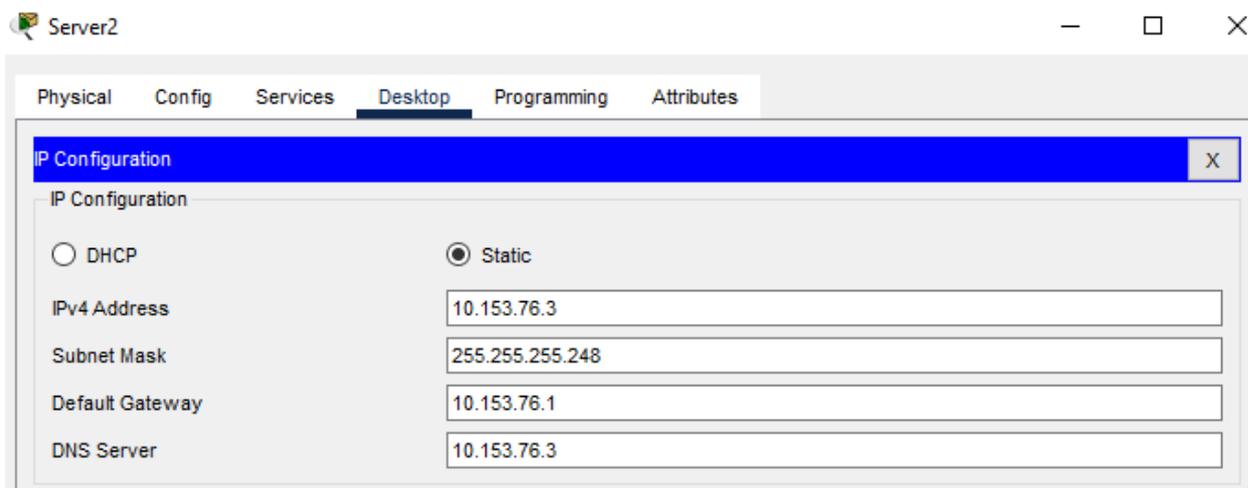


Рисунок 5 – Настройка статической конфигурации для DNS-Server

После задачи данной сетевой конфигурации, перейдем к настройке самого протокола DNS. Рисунок 6 демонстрирует, что необходимо задать доменное имя и указать IP-адрес сервера.

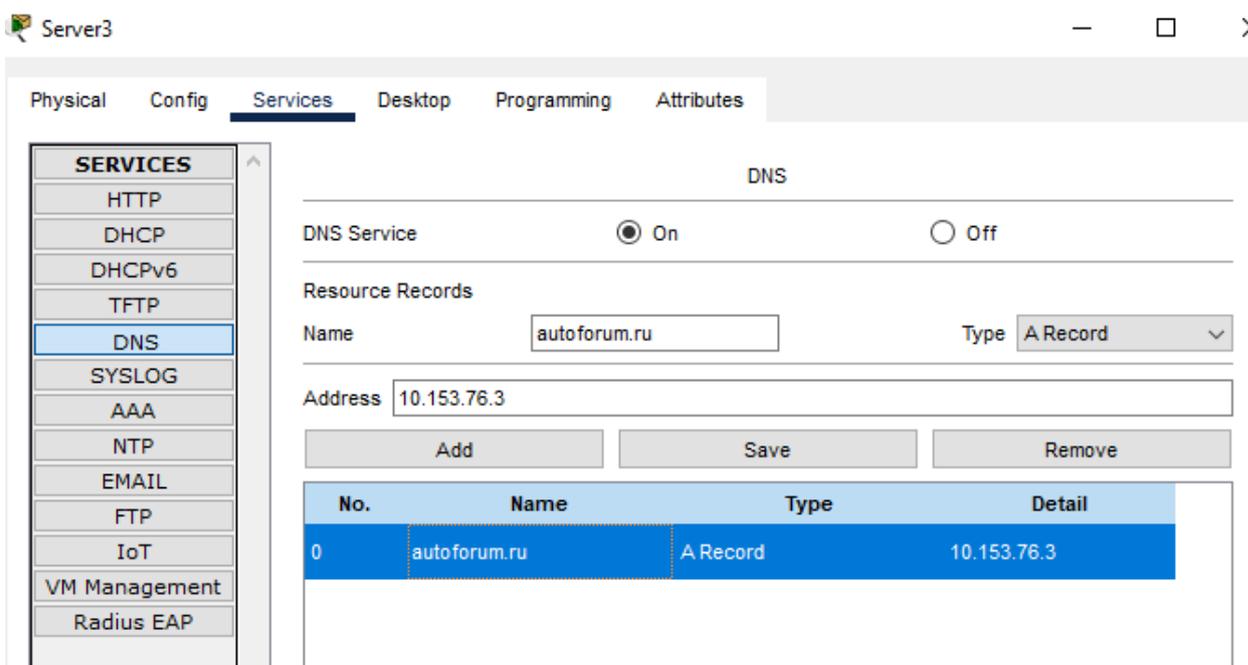


Рисунок 6 – Настройка DNS

После настройки DNS, развернем также локальную электронную почту, она необходима для передачи документации среди отделов. Для этого создадим пользователей электронной почты, и зададим доменное имя DNS-Сервера. Рисунок 7 демонстрирует пример настройки пользователей в системе локальной электронной почты.

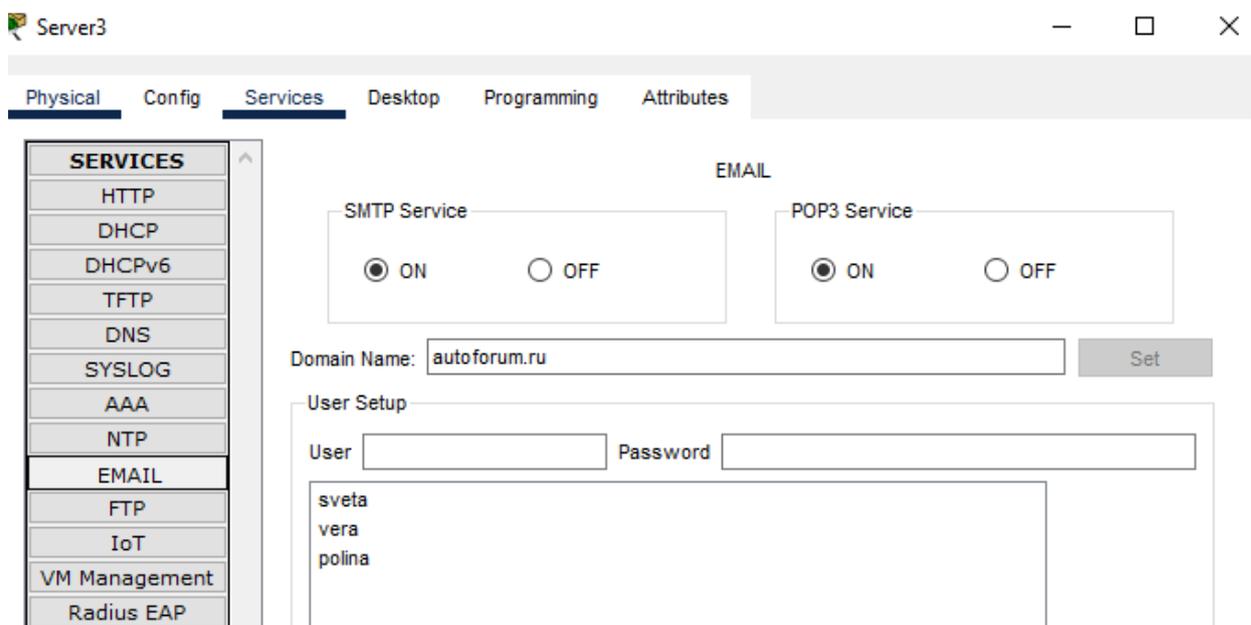


Рисунок 7 – Настройка электронной почты

Следуя из рисунка 7 для примера были созданы три профиля пользователей электронной почты, им были присвоены имена и задан пароль, данные параметры необходимы для дальнейшей авторизации на рабочих станциях.

После настройки серверного оборудования необходимо произвести настройку маршрутизатора, на котором будет реализован DHCP-Relay, так как рабочие станции будут находиться в другой маске подсети. На рисунке 8 представлена полная конфигурация маршрутизатора.

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int
Router(config)#interface fa 0/0
Router(config-if)#ip add
Router(config-if)#ip address 10.153.76.1 255.255.255.248
Router(config-if)#no sh
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#ip ad
Router(config)#int
Router(config)#interface fa 0/1
Router(config-if)#ip add
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shu
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#ip dh
Router(config-if)#ip help
Router(config-if)#ip helper-address 10.153.76.2
Router(config-if)#exit
Router(config)#

```

Рисунок 8 – Настройка маршрутизатора DHCP-Relay

После настройки первого маршрутизатора на котором был развернут DHCP-Relay, перейдем к настройке другого на котором будет развернут DHCP и VoIP протокол для реализации IP-телефонии. На рисунке 9 продемонстрирована конфигурация для настройки маршрутизатора под VoIP.

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#inte
Router(config)#interface fa 0/0
Router(config-if)#ip add
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shu
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#ip dhc
Router(config)#ip dhcp p
Router(config)#ip dhcp pool Telephon
Router(dhcp-config)#ne
Router(dhcp-config)#network 192.168.2.1 255.255.255.0
Router(dhcp-config)#de
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#opti
Router(dhcp-config)#option 150 ip 192.168.2.1
Router(dhcp-config)#exit
Router(config)#ip dhc
Router(config)#ip dhcp exc|
Router(config)#ip dhcp excluded-address 192.168.2.1

```

Рисунок 9 – Настройка DHCP на маршрутизаторе под IP-телефонию

После настройки самого протокола DHCP, необходимо произвести конфигурацию VoIP, на рисунке 10 представлена данная конфигурация.

```
Router(config)#telephony-service
Router(config-telephony)#max-eph
Router(config-telephony)#max-ephones 20
Router(config-telephony)#max-dn
Router(config-telephony)#max-dn 20
Router(config-telephony)#ip s
Router(config-telephony)#ip source-address 192.168.2.1 port 2000
Router(config-telephony)#aut
Router(config-telephony)#auto ass
Router(config-telephony)#auto assign 1 to 20
Router(config-telephony)#exit
Router(config)#ephone-dn 1
Router(config-ephone-dn)%%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up

Router(config-ephone-dn)#number 101
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 2
Router(config-ephone-dn)%%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up

Router(config-ephone-dn)#number 102
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 3
Router(config-ephone-dn)%%LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state to up

Router(config-ephone-dn)#number 103
Router(config-ephone-dn)#
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 4
Router(config-ephone-dn)%%LINK-3-UPDOWN: Interface ephone_dsp DN 4.1, changed state to up

Router(config-ephone-dn)#number 104
Router(config-ephone-dn)#exit
Router(config)#
```

Рисунок 10 – Конфигурация VoIP на маршрутизаторе

После настройки маршрутизатора произведем настройку коммутационного оборудования, изначально настроим магистральные порты в режим полной передачи VLAN, магистральные порты — это те порты которые соединяют два коммутационных оборудования. На рисунке 11 представлен пример настройки такого порта.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#inte
Switch(config)#interface gi 0/1
Switch(config-if)#sw
Switch(config-if)#switchport mode
Switch(config-if)#switchport mode tra
Switch(config-if)#switchport mode tru
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk all
Switch(config-if)#switchport trunk allowed vlan 1?
WORD
Switch(config-if)#switchport trunk allowed vlan 1,2
Switch(config-if)#
```

Рисунок 11 – Настройка магистрального порта

После настройки магистральных портов необходимо произвести настройку портов, к которым будет подключена IP-телефония. Для её создания мы создадим на всем коммутационном оборудовании «VLAN 2», данный VLAN будет использоваться исключительно для реализации IP-телефонии, а портам зададим специальным режим «Voice». На рисунке 12 представлен пример конфигурация сетевых портов на коммутаторе под IP-телефонию.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#inter
Switch(config)#interface range fa 0/17 - fa 0/20
Switch(config-if-range)#sw
Switch(config-if-range)#switchport vo
Switch(config-if-range)#switchport voice vlan 2
Switch(config-if-range)#exit
Switch(config)#
```

Рисунок 12 – Настройка коммутатора под IP-телефонию

После настройки всего активного сетевого оборудования перейдем к настройке рабочих станций, а именно нам необходимо включить режим получения сетевой конфигурации при помощи протокола DHCP. Рисунок 13 демонстрирует параметр DHCP на рабочей станции

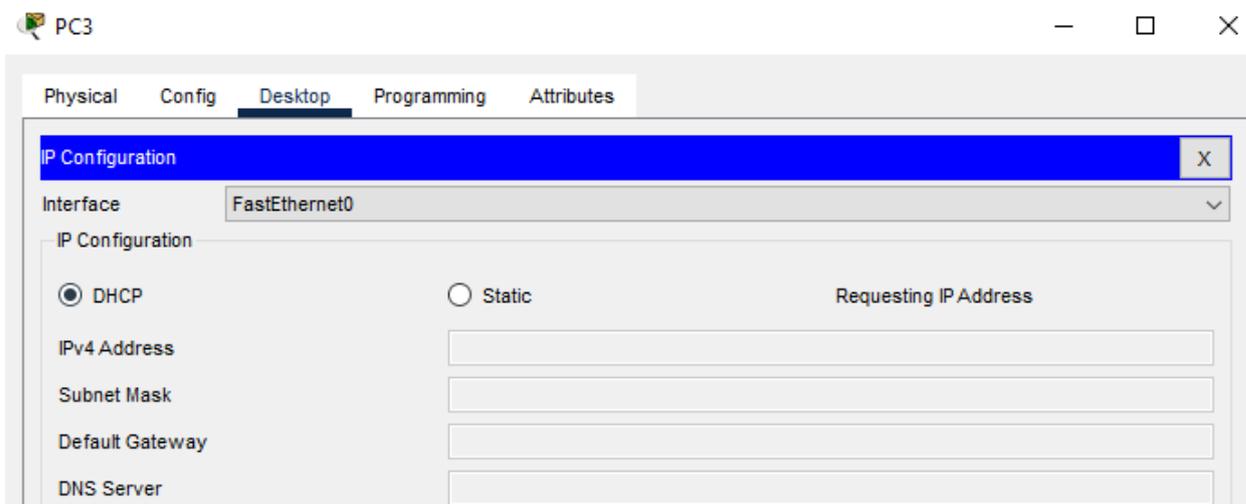


Рисунок 13 – Настройка сетевой конфигурации компьютерной сети

После того как установили, что сетевая конфигурация будет получаться при помощи протокола DHCP, произведем авторизацию пользователей в системы электронной почты. На рисунке 14 представлен пример авторизации пользователя в локальной электронной почте

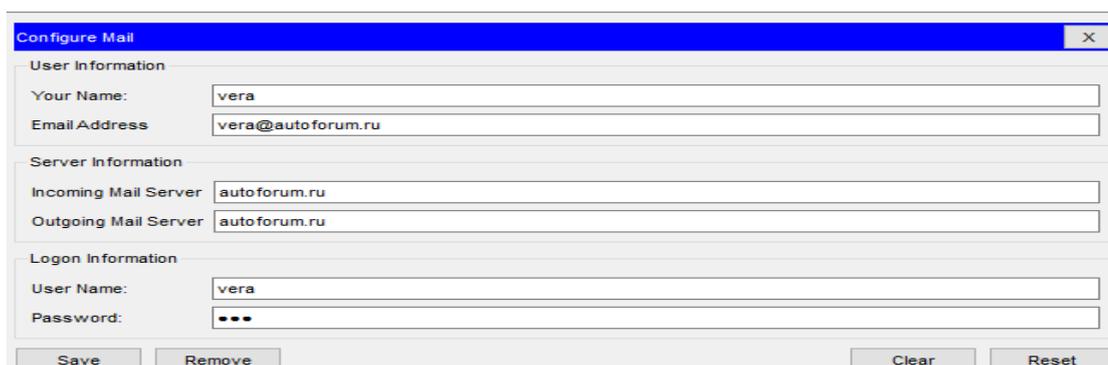


Рисунок 14 – Авторизация в системе электронной почты

Как видно из рисунка 14, необходимо заполнить поля с учетом пользователей которые были созданы на сервере.

После проведения всех данных сетевых настроек можно перейти к созданию полной и рабочей логической схемы компьютерной сети которая будет использоваться в филиале ООО «АвтоФорум». Данная схема продемонстрирована на рисунке 15.

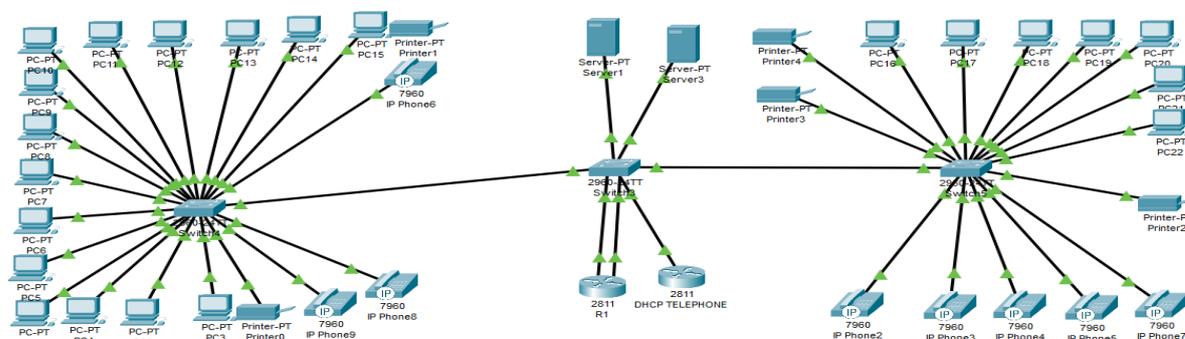


Рисунок 15 – Логическая схема компьютерной сети

2. Обеспечение защиты информации в сети с использованием программно-аппаратных средств

2.1 Анализ угроз безопасности и методов защиты информации в компьютерной сети

Под угрозой понимается событие (воздействие), которое в случае своей реализации становится причиной нарушения целостности информации, ее потери или замены.

Можно выделить три типа угроз:

- несанкционированное получение информации злоумышленником (утечка информации);
- постоянное или временное блокирование некоторого сервиса, в результате чего система перестает выполнять свои функции по назначению;
- умышленное или случайное изменение информации, например, удаление файлов или записей в БД.

Также нужно производить мониторинг сети с помощью протоколов Syslog, SNMP, Netflow:

1) Сообщения syslog и их анализ. Журналы событий фиксируют процесс работы сетевого устройства и отражают его состояние. Любое выполненное системой действие отражается в соответствующем системном сообщении — записи в журнале (логе). Системные сообщения могут иметь различные уровни детализации, и в зависимости от этого в журнале событий выделяются различные уровни протоколирования (логирования).

2) Сбор данных по протоколу SNMP. Простой протокол управления сетью (Simple Network Management Protocol, SNMP) является стандартом для обмена управляющей информацией между сетевыми устройствами и системой управления сетью (Network Management System, NMS). С точки зрения мониторинга сети протокол SNMP служит незаменимым средством сбора телеметрической информации с сетевых устройств.

3) Сбор данных по протоколу NetFlow. Протокол NetFlow разработан компанией Cisco Systems. В контексте задачи управления сетью он является незаменимым инструментом для мониторинга загрузки каналов передачи данных.

Остановимся на протоколе SNMP. Например, с помощью данных, полученных по SNMP, мы можем локализовать «паразитный трафик», загружающий сетевое оборудование. Средствами SNMP можно опрашивать OID устройств, отвечающих за загрузку сетевых интерфейсов. Если «перегруженным» устройством является коммутатор, велика вероятность, что на паре его интерфейсов мы сможем увидеть аномально высокий уровень загрузки.

2.2. Разработка комплекса мероприятий по защите информации в компьютерной сети

Существует несколько комплексов мероприятий по защите информации в компьютерной сети, которые указаны ниже:

1) Антивирусное ПО. Антивирусное ПО помогает в защите компьютерной сети от вирусов и различных программ, которые могут украсть данные компьютера. Антивирусы очень важны для компьютера, потому что благодаря им повышается защита компьютера от различных видов угроз. Например, для налоговой инспекции будет использован антивирус под названием «Kaspersky Internet Security», т. к. имеет более высокую степень защиты, может удалять большинство различных угроз и обеспечивает наиболее высокую степень защиты от несанкционированного доступа.

2) Установка ключа безопасности. Благодаря ключу безопасности повышается степень защиты компьютеров и компьютерной сети в целом, а именно вместо обычного входа с паролем в компьютер будет установлен ключ безопасности, который записан на флешку, данную флешку получают только проверенные сотрудники которым можно положиться. Данный ключ

безопасности очень подходит для налоговой инспекции, т. к. только проверенные сотрудники имеют доступ к секретной информации.

3) Установка системы мониторинга действий её пользователей, данная прикладное средство обеспечит возможность записать информацию о действиях сотрудников компании, которые они совершают на рабочих станциях, это позволит избежать следующих действий:

- внутренний шпионаж;
- передача конфиденциальной информации сторонним лицам;
- посещение в рабочее время не связанных с работой интернет ресурсов и приложений.

3. Разработка мероприятий по приемо-сдаточным испытаниям компьютерной сети и сетевого оборудования

3.1 Разработка комплекса мероприятий по приемо-сдаточным испытаниям компьютерных сетей и сетевого оборудования

Изначальным этапом проверки работоспособности компьютерной сети необходимо произвести проверку протокола DHCP, для этого воспользуемся командой «Ipconfig», данная команда выведет информацию о сетевой конфигурации порта на рабочей станции. Рисунок 16 демонстрирует какую сетевую конфигурацию получил компьютер.

```
FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::210:11FF:FEEA:3809
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                               192.168.1.1
```

Рисунок 16 – Проверка DHCP-Server и DHCP-Relay

Из рисунка 16 следует, что рабочая станция получила необходимую сетевую конфигурацию, теперь необходимо воспользоваться командой «Ping», данной командой произведем запрос с одной подсети в другую. На рисунке 17 представлена проверка соединения двух станций, находящихся в разных подсетях.

```
C:\>ping 10.153.76.3

Pinging 10.153.76.3 with 32 bytes of data:

Reply from 10.153.76.3: bytes=32 time<lms TTL=127

Ping statistics for 10.153.76.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 17 – Проверка соединения в другой подсети.

Исходя из результатов, показанных на рисунке 17 видно, что соединение есть, это говорит о правильности сетевых настроек маршрутизатора DHCP-Relay, коммутационного оборудования, DHCP-Server. Теперь произведем проверку доступа к Web-сайту филиала. Рисунок 18 демонстрирует результат запроса на сайт компании.

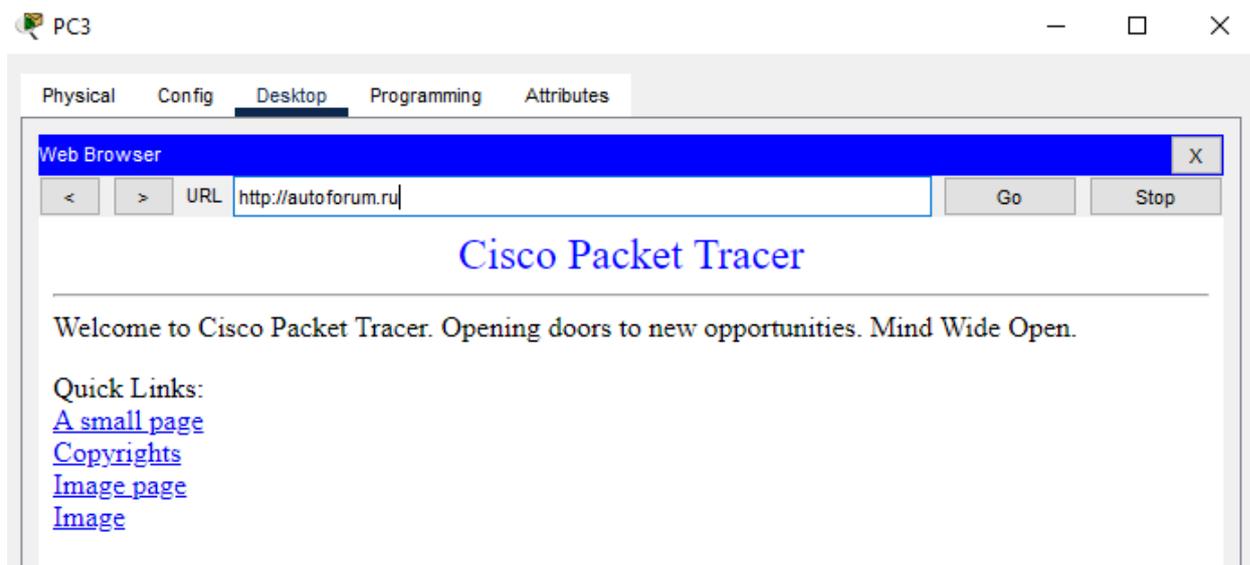


Рисунок 18 – Проверка доступа к Web-сайту филиала

Из рисунка 18, следует что доступ к сайту имеется, это означает, что протокол DNS настроен в правильном режиме.

Теперь производим проверку работоспособности электронной почты, для этого воспользуемся встроенным в «Cisco Packet Tracer» эмулятором работы электронной почты. Отправим с одного ящика письмо в другой. Рисунок 19 демонстрирует результат отправки электронного письма с одного электронного почтового ящика на другой и ответной сообщении.

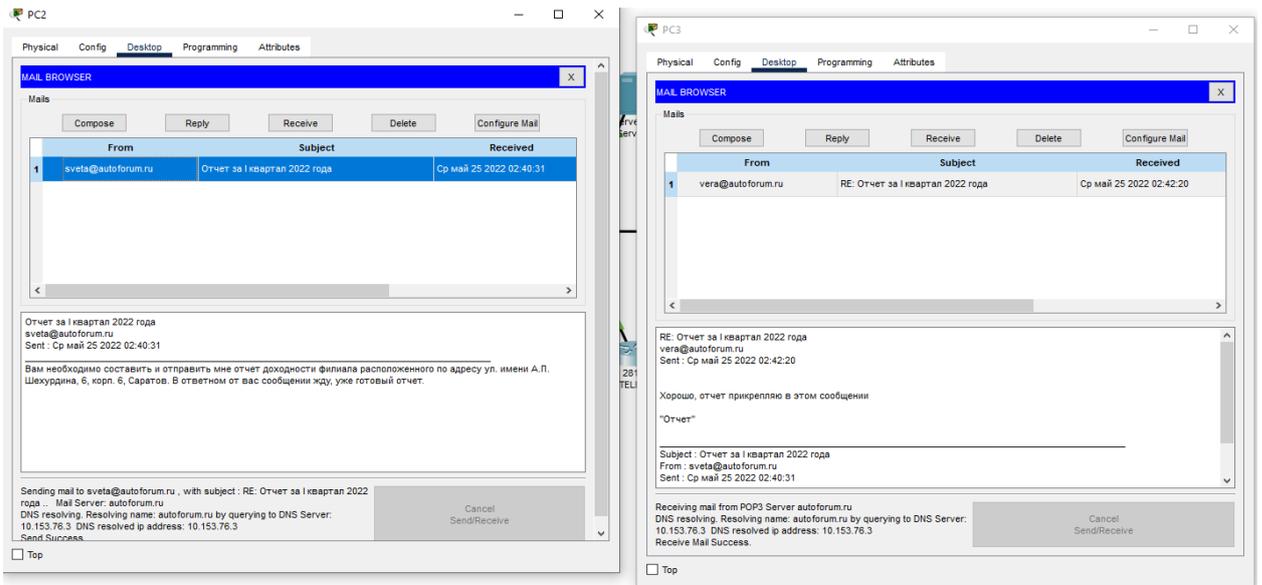


Рисунок 19 – Проверка работоспособности электронной почты

Исходя из рисунка 19 видно, что с помощью электронной почты, два сотрудника вели диалог о необходимости предоставления квартального отчета.

В заключительном этапе проверки работоспособности компьютерной сети, произведем проверку IP-телефонии, для этого произведем тестовый звонок из одного отдела в другой. Рисунок 20 демонстрирует результат соединения двух IP-телефонов, при помощи тестового звонка.

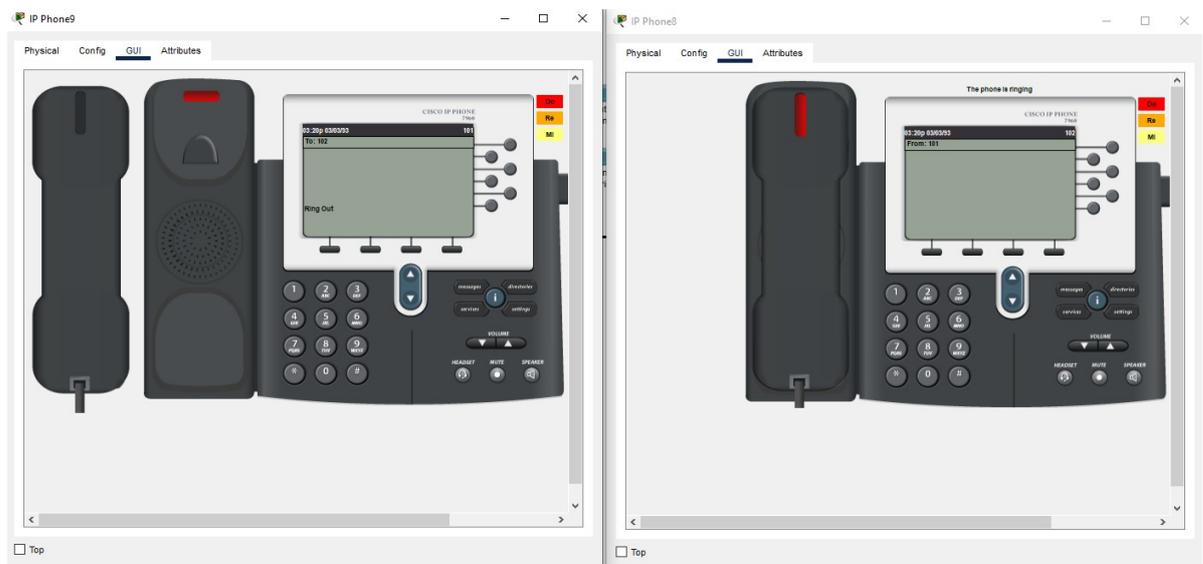


Рисунок 20 - Проверка работоспособности IP-телефонии

Исходя из рисунка 20, видно, что соединение устанавливается, из этого можно подвести итог, что вся сетевая конфигурация VoIP настроенная на активном сетевом оборудовании произведена верно.

3.2. Выбор программно-аппаратных средств мониторинга и технического контроля

Исходя из того, что на рабочих станциях будет развернута операционная система Windows 10 для обеспечения защиты будет использоваться антивирусное программное обеспечение от компании «Kaspersky», а именно: пакет «Kaspersky Endpoint Security». Ниже представлены рисунке с этапом использования данного антивирусного обеспечения. На рисунке 21 демонстрируется вид интерфейса антивирусного программного обеспечения при сканировании системы.

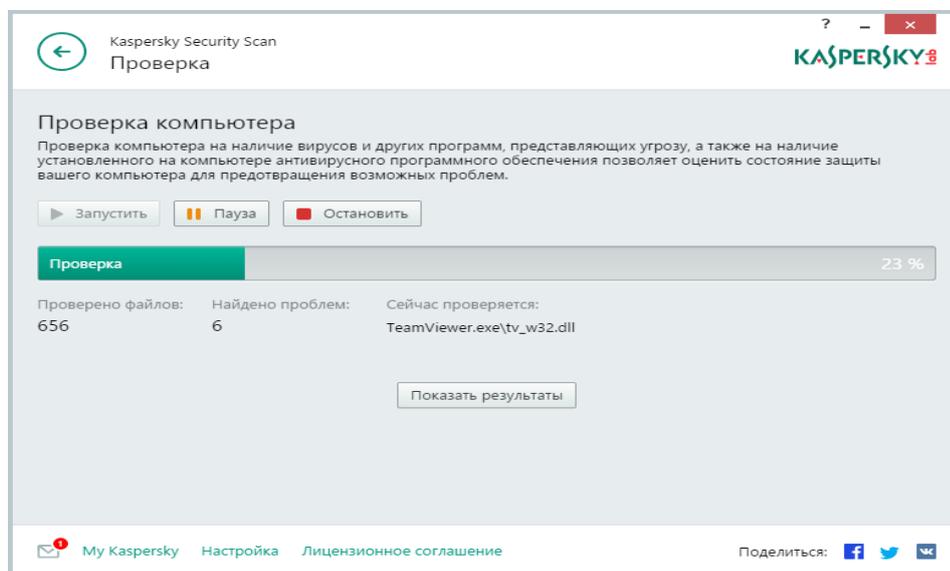


Рисунок 21 – Пример проверки рабочей станции с помощью «Kaspersky Endpoint Security»

Также при помощи данного антивирусного программного обеспечения можно произвести сканирования рабочих станций на наличие необходимых

программно-аппаратных средств, для стабильной работы рабочей станции. Рисунок 22 демонстрирует возможность при помощи антивирусного программного обеспечения производить обновления программы.

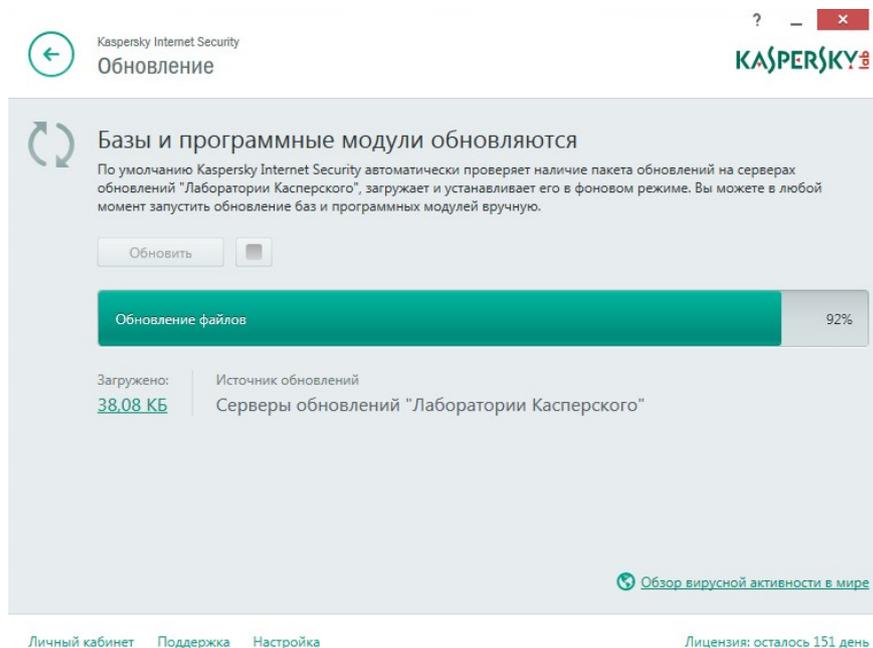


Рисунок 22 – Проверка рабочей станции на наличие новых версий программно-аппаратных средств

После развертывания на рабочих станциях антивирусного программного обеспечения произведем выбор системы мониторинга, который будет отслеживать состояние работы компьютерной сети и вести записи в базу данных развернутым на сервере. В таблице 6 представлены несколько популярных систем мониторинга.

Таблица 6 – Сравнительный анализ систем мониторинга

Наименование	Описание преимуществ	Описание недостатков
Zabbix	<ul style="list-style-type: none"> - Open source. Неограниченные возможности для обработки и кастомизации. - Визуализация данных с Grafana. Интеграция с Grafana дает возможность строить графики и создавать действительно удобные дашборды. 	<ul style="list-style-type: none"> - Долгие обновления. Во время обновления базы данных сервис мониторинга был недоступен. - Недостаточная гибкость ролевой модели. В Zabbix предусмотрено всего четыре роли пользователя с жестко фиксированными возможностями.
Network Olympus	<ul style="list-style-type: none"> - Бесплатна если в компьютерной сети используются до 100 устройств; - Простота настройки; - Несложно освоить; - Конструктор сценариев мониторинга; - Групповые сенсоры. 	<ul style="list-style-type: none"> - Только веб-интерфейс; - Установка только под Windows; - Нет многопользовательского доступа.

Проводя сравнительный анализ этих двух систем мониторинга, можно подвести небольшой итог, хоть Zabbix и является более функциональным решением с более гибкой системой которую можно настроить полностью под удобное использование конкретным системным администратором, но чаще всего такую систему мониторинга используют, более крупные организации в которых устройств в компьютерной сети большего размера, в свою очередь же Network Olympus предлагает бесплатную реализацию продукции для небольших компьютерных сетей, удобный и понятный Web-интерфейс, простую настройку, возможность реализации групповых разделений.

Рисунок 23 демонстрирует внешний интерфейс системы мониторинга о состоянии сервера и сетевого оборудования.

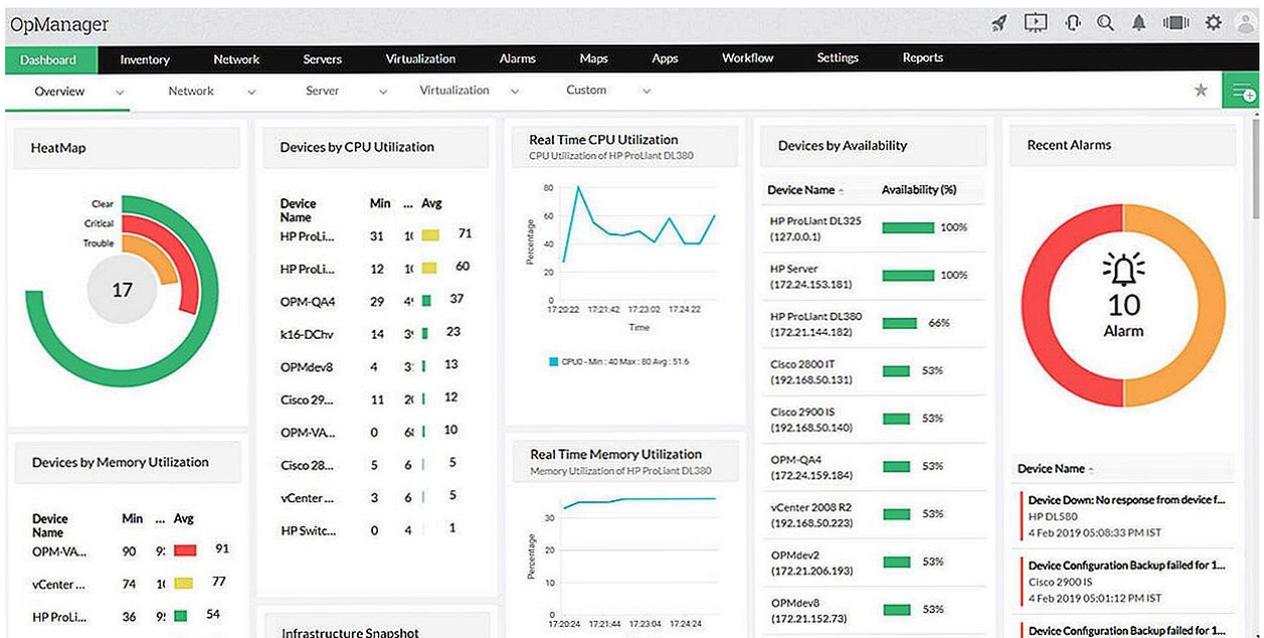


Рисунок 23– Web-интерфейс Network Olympus

Как можно видеть на рисунке 23, система мониторинга удобно демонстрирует в виде отдельного окна в котором отображается различные оповещение о критических ошибках и мелких сбоях работы сервера.

Следующим действием необходимо развернуть систему мониторинга действий её пользователей. Данный тип мониторинга производит запись логов с каждой рабочей станции на сервер с развернутой на нем базой данных. Это позволит отслеживать деятельность сотрудников в рабочие время.

Для развертывания была выбрана система мониторинга «BitCop», данная система производит запись практически всей деятельности сотрудник на рабочих станциях.

На рисунке 24 представлен начальный этап установки данной системы на сервер с операционной системой Windows Server 2016 и развернутой на нем Active Directory



Рисунок 24 – Установка на системы мониторинга на сервер

После завершения установки системы, откроется Web-интерфейс и теперь необходимо произвести установку агента мониторинга на рабочие станции сотрудников. Это можно произвести несколькими способами, устанавливая агента в ручную на каждую рабочую станцию либо же осуществить установку при помощи «Active Directory», так как на сервере будет развернута система базы данных будет использоваться метод установки с её помощью.

Рисунок 25 демонстрирует окно с авторизацией пользователя.

Установка с помощью Active Directory

Информация об Active Directory

Строка подключения к Active Directory: LDAP://domain.local

Логин: domain\user

Пароль:

Установка агента в скрытом режиме:

Получить информацию из AD | Установить агенты | Удалить агенты | Остановить процесс

Компьютер: comp10.domain.local Операция выполнена успешно
 Компьютер: comp11.domain.local Служба агента найдена
 Компьютер: comp11.domain.local Операция выполнена успешно
 Компьютер: comp06.domain.local Служба агента найдена
 Компьютер: comp06.domain.local Операция выполнена успешно
 Компьютер: comp04.domain.local Сервер RPC недоступен. (Исключение из HRESULT: 0x800706BA)
 Установка...

88.2 % (39/64)

Имя компьютера	DNS-имя компьютера	Операционная система	Процесс установки	Информационное сообщение
<input checked="" type="checkbox"/> SATURN	saturn.domain.local	Windows Server 2003	100 %	Операция выполнена успешно
<input checked="" type="checkbox"/> MARS	mars.domain.local	Windows Server® 2008 Enterprise	100 %	Операция выполнена успешно
<input checked="" type="checkbox"/> COMP11	comp11.domain.local	Windows XP Professional	100 %	Операция выполнена успешно
<input checked="" type="checkbox"/> COMP04	comp04.domain.local	Windows XP Professional	100 %	Сервер RPC недоступен. (Исключение из HRESULT: 0x800706BA)
<input checked="" type="checkbox"/> COMP05	comp05.domain.local	Windows 7 Профессиональная	60 %	Файлы агента скопированы

Рисунок 25 – Установка агента при помощи «Active Directory»

Как видно на рисунке 25, перед началом установки необходимо указать следующие данные:

- Строка подключения к Active Directory. Выглядит в формате LDAP://server/dc (например, LDAP://domain.local). Строка подключения определяется автоматически, в случае, если система не смогла определить строку по умолчанию, следует указать ее вручную.

- Логин пользователя в формате DOMAIN\user. Данный пользователь должен обладать правами администратора на машинах в домене, например, администратор домена.

- Пароль пользователя

- Установка агента в скрытом режиме. Вариант установки в скрытом режиме характерен отсутствием каких-либо всплывающих окон и уведомлений на компьютере конечного пользователя в процессе инсталляции агента. Рисунок 26 демонстрирует окно выбора роли для рабочих группы и конкретных пользователей.

-

Роли

Добавить роль		Редактировать роль		Удалить	
<input type="checkbox"/>	Роль				
<input type="checkbox"/>	Администратор				
<input type="checkbox"/>	Руководитель отдела				
<input type="checkbox"/>	Сотрудник				

Рисунок 26 – Задача роли в системе мониторинга

Как следует из рисунка 26, рабочим станциям необходимо задать роли, имеются следующие роли:

- **Администратор.** Имеет полный доступ к системе.

- **Руководитель отдела.** Имеет доступ к сотрудникам своего отдела, может просматривать отчеты, но не может редактировать настройки.

- **Сотрудник.** Имеет доступ только к персональной статистике. Может просматривать отчеты, но не может изменять данные.

После выбора роли можно произвести дополнительные настройки, связанные с тем к каким данным пользователи со статусам «Сотрудник» будут иметь доступ, данную систему можно использовать как для рабочих групп, так и для отдельно взятой рабочей станции. Рисунок 27 демонстрирует дополнительные параметры которые можно настраивать.

Добавить роль ×

Название
Введите название роли

Доступ к отчетам		Разрешить
Доступ к настройкам	Учет времени	<input checked="" type="checkbox"/>
Доступ к структуре компании	Продуктивность	<input checked="" type="checkbox"/>
Доступ к задачам	Приложения	<input checked="" type="checkbox"/>
Доступ к лицензии	Структура дня	<input checked="" type="checkbox"/>
Доступ к личным данным	Хронометраж дня	<input checked="" type="checkbox"/>
	Работа с программами	<input checked="" type="checkbox"/>
	Снимки экрана	<input checked="" type="checkbox"/>
	Задачи	<input checked="" type="checkbox"/>
	Поисковые запросы	<input checked="" type="checkbox"/>
	Оперативная сводка	<input checked="" type="checkbox"/>
	События	<input checked="" type="checkbox"/>

Рисунок 27 – Выбор параметров возможности просмотра отчета системы для сотрудников с заданной ролью «Сотрудник»

Профили сотрудника в «BitCop» содержит подробную информацию о самом сотруднике (ФИО, должность и т.п.), а также информацию об учетных записях Windows, привязанных к этому профилю. Каждый профиль сотрудника соответствует одной лицензии, при этом, одному профилю сотрудника могут соответствовать разные учетные записи (локальные и/или доменные). При наличии нескольких учетных записей внутри одного профиля, статистика по каждой записи будет суммироваться. На рисунке 28 продемонстрировано интерфейс настроенной системы.

Сотрудники

Группы						
Сотрудники						
Активные		Неактивные		Все		
Создать группу		Удалить группу		Переместить		Редактировать
Активировать сотрудников		Деактивировать сотрудников		Удалить сотрудников		Объединить сотрудников
				Объединить похожих сотрудников		Разъединить сотрудников
<input type="checkbox"/>	Сотрудник	Учетная запись	Настройки мониторинга	Расписание	Настройки продуктивности	Последняя активность
<input type="checkbox"/>	➤ Администрация		Общие	Общее 9-18	Общее	
<input type="checkbox"/>	➤ Маркетинг		Общие	Общее 9-18	Маркетолог	
<input type="checkbox"/>	▼ Финансовый отдел		Общие	Общее 9-18	Экономист	
<input type="checkbox"/>	▼ Бухгалтерия		Общие	Общее 9-18	Бухгалтер	
<input type="checkbox"/>	Смирнов Алексей	ASUS\ladmin	Общие	Общее 9-18	Общее	16 дек. 2018, 18:35

Рисунок 28 – Итоговый интерфейс работы системы мониторинга действий её пользователей «BitCop»

После проведения развертывания антивирусного программного обеспечения, системы мониторинга работы сервера и мониторинга действий пользователей, компьютерная сеть защищена от угроз как внутренних, так и от угроз из вне компьютерной сети компании.

4. Оформление Проекта кабельной структуры компьютерной сети в соответствии с требованиями заказчика

4.1. Разработка проектной документации

Перейдем к построению структурной схемы кабельной сети, развернутой в учебном заведении. Для построения будет использоваться программа «КОМПАС 3D». На рисунке 29, продемонстрирована данная схема.

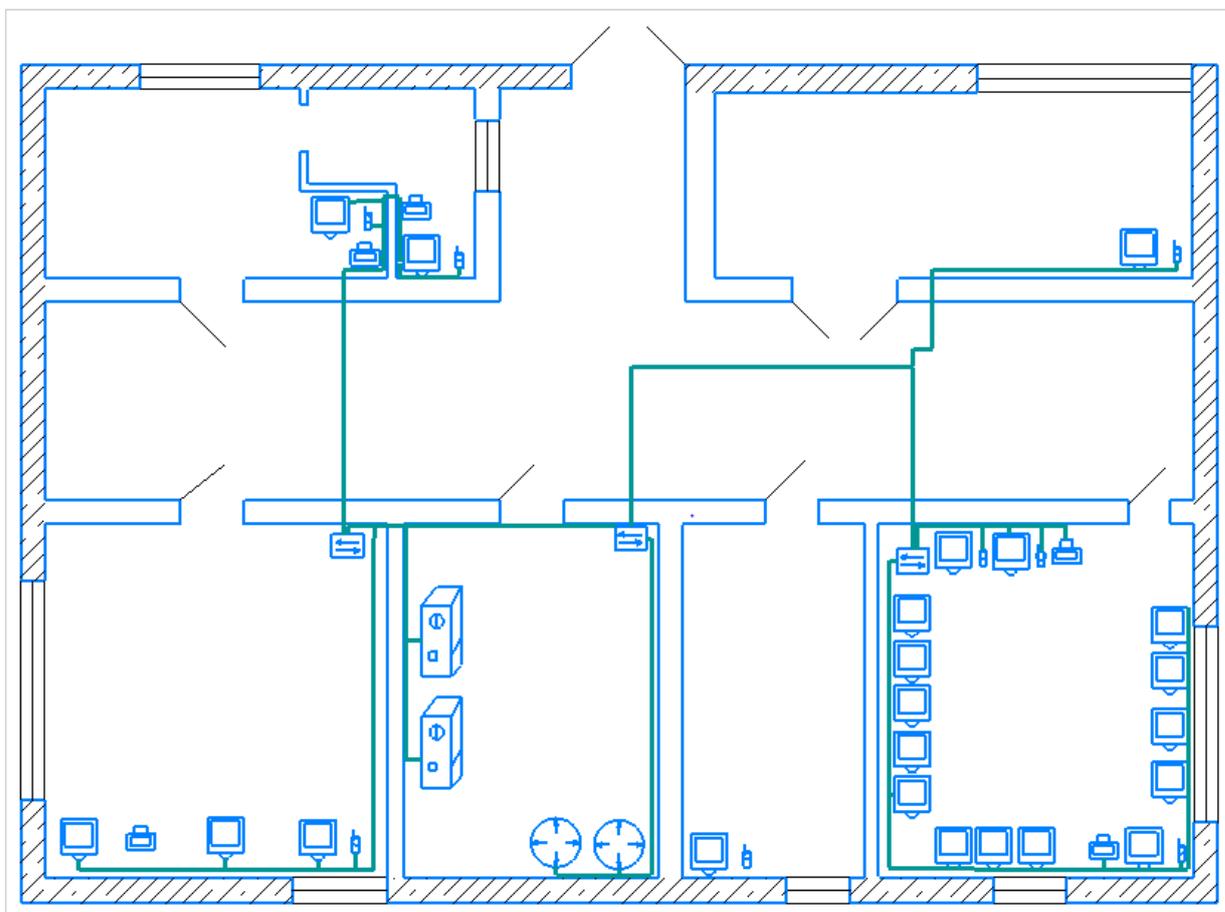


Рисунок 29 - Структурная схема кабельной сети

После построения схемы необходимо перейти к выбору пассивного оборудования которые будет использоваться, а именно сетевой кабель. Для этого произведем сравнение характеристик, данные показатели будут продемонстрированы в таблице 7.

Таблица 7 – Выбор сетевого кабеля

Наименование кабеля	Краткое описание
FTP 4PR 24AWG CAT5e	Не экранированный четырех жильный медный кабель категории 5e со скоростью до 100 Мбит/с,
Netlink UTP 4PR STANDART 24AWG CAT5e	Огнестойки экранированный четырех жильный медный кабель категории 5e со скоростью до 100 Мбит/с,

Был выбран сетевой кабель «Netlink UTP 4PR STANDART 24AWG CAT5e», он обладает огнестойким экранирование, обладает подходящий пропускной способностью. Данный кабель будет прокладываться от коммутационного оборудования к рабочим станциям, но так-как нагрузка на магистральные линии между коммутационным оборудованием и линии с сервером скорость передачи данных будет превышать скорость 100 мбит/с, из-за наличия развернутой системы мониторинга компьютерной сети её пользователей, был выбран кабель отечественного производства «СПЕЦЛАН U/UTP Cat 6», скорость передачи данных на дистанции до 55 метров может достигать 10 Гбит/с. После выбора типа кабеля произведем расчёт необходимого количества для провидения монтажных работ по его прокладке в офисе компании.

Для объединения всего оборудования в одну сеть, нужно высчитать среднюю длину кабеля по формуле (1):

$$L_{cp} = \frac{(L_{мин} + L_{макс})}{2} * 1,3 + X(1)$$

Где,

$L_{мин}$ и $L_{макс}$ — это длины наиболее короткой и наиболее длинной кабельных линий, м;

X – это запас на разделку кабеля (обычно 0,6 – 1,0 м), м;

1,3 — это коэффициент технологического запаса равный 13%

Произведем расчет средний длины для кабеля «СПЕЦЛАН U/UTP Cat 6»

$$\frac{(30+50)}{2} * 1,3 + 1 = 53 \text{ м.}$$

По этой же формуле произведем расчет для кабеля «Netlink UTP 4PR STANDART 24AWG CAT5e»:

$$\frac{(10+25)}{2} * 1,3 + 1 = 23,75 \text{ м.}$$

Затем рассчитывается количество кабельных пробросов с одной упаковки кабеля по формуле (2):

$$N = \frac{L_{\text{кат}}}{L_{\text{ср}}} (2)$$

Где,

$L_{\text{кат}}$ — количество кабеля в одной упаковке (100, 305, 500, 1000), м;

$L_{\text{ср}}$ - средняя длина кабеля, м.

Количество пробросов для кабеля «СПЕЦЛАН U/UTP Cat 6»:

$$\frac{305}{53} = 5,75 \text{ пр.}$$

При помощи этой же формулы произведем расчет для «Netlink UTP 4PR STANDART 24AWG CAT5e»:

$$\frac{305}{23,75} = 12,84 \text{ пр.}$$

Делим общее количество портов на число пробросов с одной упаковки кабеля, округляем в большую сторону и получаем необходимое количество упаковок кабеля.

Рассчитаем необходимое количество упаковок сетевого кабеля «СПЕЦЛАН U/UTP Cat 6»:

$$14/5,75 = 6 \text{ упаковок.}$$

При помощи этой же формулы произведем расчет для «Netlink UTP 4PR STANDART 24AWG CAT5e»:

$$70/23,75 = 3 \text{ упаковок.}$$

Вычисляем необходимое количество кабеля умножая количество упаковок на длину кабеля в каждой упаковке.

Определим метраж кабеля «СПЕЦЛАН U/UTP Cat 6»:

$$6 * 305 = 1830 \text{ м.}$$

При помощи этой же формулы произведем расчет для «Netlink UTP 4PR STANDART 24AWG CAT5e»:

$$3 * 305 = 915 \text{ м.}$$

Теперь необходимо произвести выбор активного сетевого оборудования. Начальный элемент выбора будет являться сервер. В таблице 8, произведены краткие сравнительные характеристики нескольких серверов.

Таблица 8 – Сравнение характеристик серверов.

Наименование	Описание
Сервер Dell EMC PowerEdge R650 (1U)	Идеальный вариант для традиционных корпоративных ИТ-систем, баз данных и аналитики, инфраструктуры виртуальных рабочих столов, использования искусственного интеллекта, машинного обучения и формирования логических выводов
LENOVO THINKSYSTEM SR5908SFF (2U)	Универсальный и масштабируемый сервер. Оптимальное конструктивное решение, баланс производительности и цены для поддержки практически любой рабочей нагрузки Общие компоненты в рамках всего портфеля ThinkSystem для сокращения количества запасных частей, ускорения обслуживания и повышения доступности Высокая энергоэффективность благодаря соответствию требованиям стандартов ASHRAE A2 и A4 (с ограничениями), непрерывная эксплуатация при температуре окружающей среды до 45 °С

По краткому описанию можно подвести итог, что сервер «LENOVO THINKSYSTEM SR5908SFF (2U)», является хорошим выбором. Он обладает средними параметрами, но более гуманной ценовой политикой, мощностей данного сервера хватит для реализации построения компьютерной сети и

обеспечения стабильной сетевой работы учреждения. В таблице 9 можно увидеть полную спецификацию данного оборудования. Таблица 9 – Спецификация стоечного сервера

«LENOVO THINKSYSTEM SR5908SFF» (2U)	
Наименование	Описание
1	2
Поддержка операционных систем	Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Vmware vSphere.
Форм-фактор и высота	Стойный сервер 2U
Оперативная память	До 3 ТБ в 24 слотах при использовании модулей DIMM по 128 ГБ; память TruDDR4 2666 МГц Поддержка до 1,5 ТБ на дату начала отгрузки. Модули DIMM объемом 128 ГБ станут доступны для заказа в ближайшее время.
Отсеки для накопителей	До 24 отсеков с поддержкой «горячей» замены (включая 4 или 8 AnyBay): а также до двух зеркалируемых загрузочных дисков M.2 (доп. RAID 1)
Сетевые интерфейсы	2/4-портовая плата LOM 1GbE; 2/4-портовая плата LOM 10GbE (Base-T или SFP+); 1 выделенный порт управления 1GbE

Ниже также представлено изображение данного стоечного сервера.



Рисунок 30 - Изображение стоечного сервера «LENOVO THINKSYSTEM SR5908SFF (2U)»

После выбора серверного оборудования, произведем выбор маршрутизатора, подходящего по параметрам. Маршрутизатор также будет монтироваться в стойку, были выбраны несколько стоечных маршрутизаторов от компании «Cisco». В таблице 10 можно ознакомиться со сравнительными характеристиками маршрутизатора.

Таблица 10 – Сравнительные характеристики маршрутизаторов

Наименования	Описание
Cisco 888	<ul style="list-style-type: none"> - Имеется возможность установки в стойку; - Отсутствует web-интерфейс; - Наличие функций: DHCP-сервер, DHCP-relay, межсетевой экран (Firewall), NAT, демилитаризованная зона (DMZ);
Cisco RV345P-K8	<ul style="list-style-type: none"> - Имеется возможность установки в стойку; - Наличие Web интерфейса, и поддержка SNMP; - Возможность реализации VPN туннеля; - Наличие функций: DHCP-сервер, DHCP-relay, VOIP, межсетевой экран (Firewall), NAT;
Cisco C881-K9	<ul style="list-style-type: none"> - Имеется возможность установки в стойку; - Наличие Web интерфейса; - Возможность реализации VPN туннеля.

Из таблицы 10 следует, что маршрутизатор «Cisco RV345P-K8», обладает функцией поддержки VoIP протокола, наличие данного протокола

является важным, это связано с тем, что в учреждение будет использоваться IP-Телефония, также данный маршрутизатор является бюджетным вариантом, что удовлетворяет потребность заказчика. На рисунке 32 изображен данный маршрутизатор.



Рисунок 31 – Маршрутизатор «Cisco RV345P-K8»

Обосновав вывод, рассмотрим более подробно техническую составляющую этого маршрутизатора. В таблице 11 представлена его спецификация с полными техническими характеристиками.

Таблица 11 – Спецификация маршрутизатора

«Cisco RV345P-K8»	
Количество LAN-портов	16 штук
Базовая скорость передачи данных	1 Гбит/с
Количество WAN-портов	2 штуки
Объем флэш-памяти	256 Мбайт

После выбора маршрутизирующего оборудования необходимо перейти к выбору коммутационного оборудования. Коммутаторы будут выбираться также из бюджетного сегмента предоставляемыми компанией «Cisco», основными параметрами сравнения будут является наличие необходимого

функционала для реализации компьютерной сети и возможностью дальнейшего её расширения.

Таблица 12 – Сравнительные характеристики коммутаторов

Наименование	Описание
Коммутатор Cisco SF220-24	Является оптимальным решением, где требуется соединение нескольких сегментов сети за счет обеспечения обработки данных на общей скорости 8.8 Гбит/с. Обеспечивает такой высокий уровень коммутационной способности наличие 24 портов с применением технологии PoE. Данное расширение позволяет подключать не только интернет кабеля, но и IP телефоны, видеокамеры
Коммутатор Cisco SG220-26	Является решением для реализации компьютерный сетей средних и крупных размеров, позволяющих создать надежную и безопасную сеть бизнес класса.
Коммутатор Cisco WS-C2960-24	Обладает расширенным диапазоном функций и использование инновационных технологий обеспечивает простоту настройки и управления, безотказность работы и высокую производительность сети.

Из описания коммутационного оборудования которое продемонстрировано в таблице 12, подводиться итог, что коммутатор «Cisco SF220-24», является хорошим решением для реализации компьютерной сети небольших и средних масштабов, так как в общеобразовательном учреждении размер компьютерной сети, является небольшим. Также данный коммутатор отлично подойдет в дальнейшем для расширения компьютерной сети в небольших масштабах, например, подключение ещё нескольких

рабочих станций, IP-Телефонии, IP-сканера, общая пропускная способность в размере 8.8 Гбит/с позволяет это. В таблице 13 проведены полные характеристики этого коммутационного оборудования.

Таблица 13 – Спецификация коммутатора

«Коммутатор Cisco SF220-24»	
Количество LAN-портов	24 штуки
Мониторинг и конфигурирование	консольный порт, Web-интерфейс, поддержка Telnet
Базовая скорость передачи данных	100 Мбит/с
Максимальная скорость uplink/SFP-портов	1 Гбит/с
Внутренняя пропускная способность	8.8 Гбит/сек
Размер таблицы MAC адресов	8192
Тип управления коммутатора	2-й уровень

На рисунке 32 представлено изображение данного коммутатора.



Рисунок – 32 Коммутатор «Cisco SF220-24»

Перейдем к выбору компьютерного оборудования. Из технического задания, компьютеры должны выполнять без каких-либо затруднений следующие задачи:

- Использование программы «Yandex Browser». Данная программа позволит использовать различные WEB-ресурсы для нахождения необходимой дополнительной информации, для выполнения поставленных цели.

- Использования стандартного офисного пакета «Word». Данная пакет офисных программ необходим для ведения отчетности и заполнение различной документации.

Следуя из этих задач выберем бюджетный сегмент компьютеров, которые смогут справляться с поставленными задачами. В таблице 14 представлены модели компьютеров в бюджетном сегменте.

Таблица 14 – Выбор компьютерного оборудования

Наименование	Описание
Моноблок Acer Aspire C22-820, 21.5	Бюджетный компьютер, предназначенных для выполнения простых и средних задач. Система выстроена на базе процессора от компании AMD. Имеет SDD накопитель, интегрированный видеочип R5.
HP Slimline S01-aF1010ur	Бюджетных компьютер, предназначенный для выполнения офисных задач. Система выстроена на базе от компании Intel, имеет SSD накопитель и интегрированный видеочип Intel UHD Graphics 600.
Моноблок HP 21-b0034ur	Более дорогой вариант офисного моноблока. Подходит для выполнения легких офисных задач и серфинга интернет ресурсов. Обладает повышенной ценовым сегментом.

Следуя из таблицы, предпочтение отдается моноблоку «Acer Aspire C22-820, 21.5», а не «Моноблок HP 21-b0034ur» из-за более мощного процессора, и встроенного видеочипа, которые демонстрирует неплохие показатели в нагрузках.

Таблица 15 – Характеристики рабочей станции

«Acer Aspire C22-820, 21.5»	
Наименование	Описание
1	2
Процессор	AMD A6 9500

Продолжение таблицы 15

1	2
Графика	AMD Radeon R5
Объем SSD	240 ГБ
Установленная операционная система	Windows 10
Процессор, частота	3.5 ГГц (3.8 ГГц, в режиме Turbo)
Оперативная память	8 ГБ, DDR4, DIMM, 2400 МГц

На рисунке 33 продемонстрирован данный моноблок.



Рисунок 33 – Моноблок «Acer Aspire C22-820, 21.5»

Периферийное оборудование, а именно компьютерные мыши и клавиатуры приобретаются с запасом. Для быстрой замены в случаи поломки использующего. Был выбран офисный набор «DEXP KM-3004BU», данный набор оснащен проводной клавиатурой и мышью, преимуществом является, удобный и прочный материал из которого выполнен корпус, клавиши клавиатуры и мыши.

Для обеспечения передачи документация между вышестоящими отделами оснастим данные отделы принтерами, был выбран следующий принтер «МФУ лазерное «HP LaserJet Pro M28a, ч/б, А4,», бюджетный вариант качественного сетевого принтера. Изображение данного принтера представлена ниже.

Для реализации IP-телефонии был выбран «VoIP-телефон Cisco 6961-C», он является бюджетным вариантом, прост в обслуживании и внедрения в компьютерную сеть, данный телефон способен удовлетворить потребность в развертывание внутренней IP-Телефонии. Данная технология обеспечит более удобную систему взаимодействий между отделами. Рисунок 34 представляет вид данного телефона.



Рисунок 34 – «VoIP-телефон Cisco 6961-C»

4.2. Расчет технико-экономических показателей

Последним этапом выполнения данной выпускной квалификационной работы является подведение итоговых экономических затрат, для реализации компьютерной сети для филиала ООО «АвтоФорум». В таблице 16 предоставлена информация о затраченных ресурсах на покупке пассивного и активного сетевого оборудования, а также для проведения монтажных работ развертывания кабельной структуры в учебном заведении.

Таблица 16 – Экономические затраты на приобретение и реализацию компьютерной сети.

Наименование оборудования	Стоимость за одну единицу (Руб.)	Количество (шт.)	Общая стоимость (Руб.)
1	2	3	4
Netlink FTP 4PR STANDART 24AWG CAT5e (305м.)	9 800 руб.	3 бухт	29 400 руб.
СПЕЦЛАН U/UTP Cat 6	16 750 руб.	6 бухт	100 500 руб.
Кабель-канал УРАЛ ПАК Белый 12х12 2м КК-3112012-200	125 руб.	975 шт.	121 875 руб.
Cisco RV345P-K8	18 000 руб.	2 шт.	36 000 руб.
Cisco SF220-24	11 400 руб.	3 шт.	34 200 руб.
Шкаф телекоммуникационный 12U 600х600 C126060BWTWOF	12 300 руб.	1 шт.	12 300 руб.
Коннектор разъем RJ45 (8p8c), cat. 5e.	19 руб.	75 шт.	1425 руб.
Реализация подрозетника	275 руб.	45 шт.	12 375 руб.
Установка сетевой розетки	250 руб.	45 шт.	11 250 руб.

Продолжение таблицы 16

1	2	3	4
Интернет розетка Schneider Electric ATN000183 AtlasDesign, белый	200 руб.	45 шт.	9000 руб.
Lenovo ThinkSystem SR650 (2U)	132 560 руб.	2 шт.	265 120 руб.
Моноблок «iRU Home 320A3SE»	24 650 руб.	22 шт.	542 300 руб.
VoIP-телефон Cisco 6961-C	9 600 руб.	8 шт.	76 800 руб.
Прокладка кабеля	45 руб./м	4570 м.	205 740 руб.
Клавиатура+мышь проводная DEXP KM-3004BU	799 руб.	25 шт.	19 975 руб.
МФУ лазерное HP LaserJet Pro M28a, ч/б, А4	18 500 руб.	5 шт.	92 500руб.
ИТОГО:	1 570 760 руб.		

ЗАКЛЮЧЕНИЕ

Локальные вычислительные сети в настоящее время получили широкое распространение в самых различных областях науки, техники и производства.

Особенно широко ЛВС применяются при разработке коллективных проектов, например, сложных программных комплексов.

На базе ЛВС можно создавать системы автоматизированного проектирования. Это позволяет реализовывать новые технологии проектирования изделий машиностроения, радиоэлектроники и вычислительной техники.

В условиях развития рыночной экономики появляется возможность создавать конкурентоспособную продукцию, быстро модернизировать ее, обеспечивая реализацию экономической стратегии предприятия.

ЛВС позволяют также реализовывать новые информационные технологии в системах организационно-экономического управления. Использование сетевых технологий значительно облегчает и ускоряет работу персонала, позволяет использовать единые базы данных, а также регулярно и оперативно их пополнять и обрабатывать.

Подводя итоги, были рассчитаны основные параметры локальной сети с учетом ее масштабирования для функционирования. Для проведения развертывания компьютерной сети было подсчитано необходимое количество требуемого телекоммуникационного оборудования. Описана конфигурация каждого элемента сети, показана система мониторинга состояния сервера, а также произведена установка и дальнейшее настройка системы мониторинга действий сотрудников внутри компьютерной сети. Разработана и изложена спецификация пассивного и активного оборудования.

Было осуществлено построение логической схемы в эмуляторе, а также произведена базовая настройка сетевого оборудования, также были установлены и настроены сетевые протоколы, которые были необходимы для

работоспособности нового сегмента компьютерной сети и выполняющие условия заданий.

Кроме того, был разработан комплекс мероприятия по защите информации в компьютерной сети компании.

Ожидаемые результаты внедрения информационной системы:

- повышение безопасности и отказоустойчивости компьютерной сети, при помощи развернутой системы мониторинга;
- повышение работоспособности персонала при помощи автоматизации процессов;
- повышение трудовой способности персонала при помощи системы мониторинга действий пользователей компьютерной сети;
- дополнительные меры безопасности конфиденциальной информации и важной документации от внутреннего шпионажа и возможного воровства этой информации, благодаря реализованной системы мониторинга действий сотрудников компьютерной сети.

Список использованных источников

Нормативно-правовые акты

1. ГОСТ Р 53245-2008 «Информационные технологии. Системы кабельные структурированные. Монтаж основных узлов системы. Методы испытания»
2. ГОСТ Р 53246-2008 «Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования»
3. ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»
4. Федеральный закон от 18 марта 2019 г. N 30-ФЗ «О внесении изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации»»

Учебники и учебные пособия

5. Дибров, М.В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1: учебник и практикум для среднего профессионального образования / М.В. Дибров. – М.: Издательство Юрайт, 2020. – 333 с. – ISBN 978-5-534-04638-0.
6. Дибров, М.В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2: учебник и практикум для среднего профессионального образования / М. В. Дибров. – М.: Издательство Юрайт, 2020. – 351 с. – ISBN 978-5-534-04635-9.
7. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник. – СПб.: Питер, 2020. – 992 с. – ISBN: 978-5-496-01967-5.8ш
8. Новожилов, Е.О. Компьютерные сети. Учебное пособие / Е.О. Новожилов. - М.: Academia, 2016. - 288 с.
9. Таненбаум, 8Э. Компьютерные сети / Э. Таненбаум. - СПб.: Питер, 2019.

10. Таненбаум, Э.С. Компьютерные сети / Э.С. Таненбаум, Д. Уэзеролл. - СПб: Питер, 2018.

Дополнительные издания

11. Куроуз Д., Росс К. Компьютерные сети. Настольная книга системного администратора / пер. М. Райтман. – М.: Эксмо, 2018. – 912 с. – ISBN: 978-5-699-94358-6.

Интернет-ресурсы

12. Федеральный образовательный портал «Российское образование». – Режим доступа: www.edu.ru.

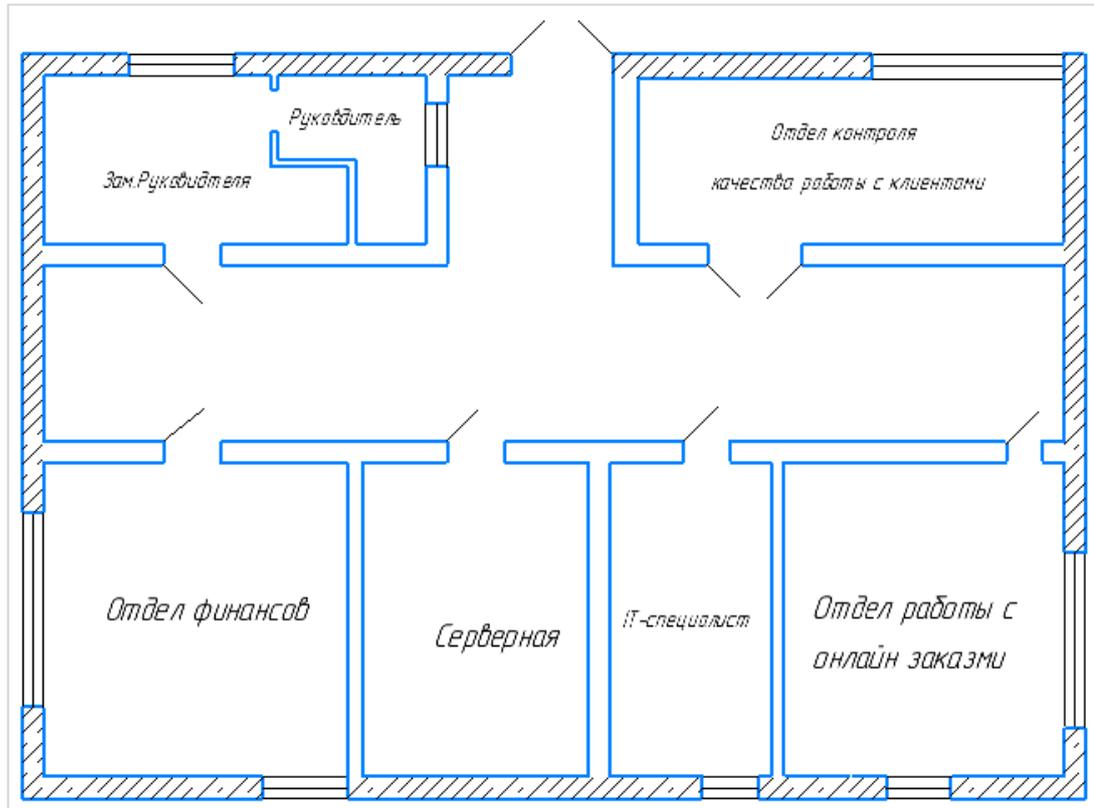
13. Сетевые технологии. – Режим доступа: <http://datanets.ru/>

14. Сайт по подбору и настройке сетевого оборудования <https://www.cisco.com/>

15. Интернет магазин электроники и компьютерного оборудования <https://www.dns-shop.ru/>

ПРИЛОЖЕНИЕ А

План помещение компании ООО «АвтоФорум»



ПРИЛОЖЕНИЕ Б

Анкета потребностей заказчика

1. Расположение абонентских розеток:
 - 1.1. Предоставляется заказчиком
 - 1.2. Выбирается вместе с заказчиком
 - 1.3. Выбирается проектировщиком

2. Монтаж коммутационного оборудования:
 - 2.1 На раму
 - 2.2 В стойку
 - 2.3 В шкаф
 - 2.4 Выбирается проектировщиком

3. Указано на планах расположение технических помещений или мест, куда можно установить оборудование:
 - 3.1 Да
 - 3.2 Нет

4. Линия, идущая от провайдера, для подключения Интернет
 - 4.1. DSL
 - 4.2. Ethernet
 - 4.3. Оптоволокно

5. Активное сетевое оборудование
 - 5.1. Предоставляется заказчиком
 - 5.2. Выбирается вместе с заказчиком

6. Покрытие сетью WI-FI
 - 6.1. Да
 - 6.2. Нет

7. Скорость сети внутренней передачи данных
 - 7.1. Не менее 100 Мб/сек
 - 7.2. Не менее 1000 Мб/сек

8. Выбор системы мониторинга действий пользователей компьютерной сети
 - 8.1 Выбирается заказчиком
 - 8.2 Выбирается самостоятельно