Министерство образования Красноярского края

Краевое государственное бюджетное профессиональное образовательное учреждение

«Красноярский колледж радиоэлектроники и информационных технологий»

**ОТЧЕТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ**

09.02.02 Компьютерные сети

код и наименование специальности

Красноярский колледж радиоэлектроники и информационных технологий

место прохождения практики

Производственная практика (преддипломная)

код и наименование профессионального модуля и междисциплинарного курса

Студент 9КС-1.17, 25538 \_\_\_\_\_\_\_\_\_ /Е.В.Аверяскин

номер группы, зачетной книжки подпись, дата инициалы, фамилия

Руководитель от предприятия \_\_\_\_\_\_\_\_\_\_ /В.А. Кириллов

подпись, дата инициалы, фамилия

М.П.

оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель от колледжа \_\_\_\_\_\_\_\_\_\_ /Е.В.Харитонова

подпись, дата инициалы, фамилия

Красноярск, 2021 г.

**АННОТАЦИЯ**

Данный документ является пояснительной запиской к преддипломной практике.

Первый раздел пояснительной записки содержит изучение организации.

Второй раздел пояснительной записки содержит проектирование схемы подключения, описание настройки оборудования и программного обеспечения.

Третий раздел содержит описание расчет экономических затрат.

Четвертый раздел содержит описание охраны труда и технику безопасности.

Также имеются Аннотация, Содержание, Введение, Заключение, Список сокращений, Библиографическое описание и Приложения

Пояснительная записка по преддипломной практике оформлена на ПЭВМ (Ryzen 5 2600, RAM 16 Gb, SDD 480 Gb) под управлением операционной системы Windows 10 в текстовом процессоре Microsoft Word 19. Пояснительная записка содержит 58 страниц, 75 рисунков, 2 таблицы, 5 приложений.

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 4](#_Toc71714553)

[**1.** **Организационно-техническая часть** 5](#_Toc71714554)

[**1.1** **Краткая характеристика организации** 5](#_Toc71714555)

[**1.2** **Спецификация оборудования организации** 6](#_Toc71714556)

[**1.3** **Спецификация программного обеспечения организации** 7](#_Toc71714557)

[**1.4.** **Анализ существующей сети** 8](#_Toc71714558)

[2 Рабочая часть 10](#_Toc71714559)

[**2.1.** **Проектирование схемы подключения** 10](#_Toc71714560)

[**2.2.** **Подключение и настройка оборудования** 11](#_Toc71714561)

[**2.3.** **Настройка программного обеспечения** 28](#_Toc71714562)

[3. Экономическая часть 40](#_Toc71714563)

[**3.1.** **Расчет** 40](#_Toc71714564)

[4 Охрана труда и техника безопасности 41](#_Toc71714565)

[ЗАКЛЮЧЕНИЕ 42](#_Toc71714566)

[СПИСОК СОКРАЩЕНИЙ 43](#_Toc71714567)

[БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ 44](#_Toc71714568)

**ВВЕДЕНИЕ**

Актуальность темы – в организации, которая имеет более ста рабочих станций, несколько десятков IP-камер видеонаблюдения и несколько сетевых МФУ большую опасность может сыграть широковещательный трафик на втором уровне сетевой модели OSI, который могут генерировать все устройства в сети. При обычном режиме работы такой трафик можно контролировать, но если кто-то запустить на рабочей станции вредоносную программу, которая каждую секунду будет генерировать широковещательный трафик, то это может существенно ухудшить производительность сети, а если сетевое оборудование не сможет справиться с таким объемом трафика и попросту зависнет, что может парализовать работу все локальной сети. Для решения такой проблему существует технология VLAN.

VLAN – это технология, которая позволяет сетевым администраторам создавать логические широковещательные домены, позволяющие охватывать один или более коммутаторов, вне зависимости от физического расположения самих устройств. Это позволяет сокращать размер доменов широковещательной передачи, а также логически объединять группы, не располагая объекты в одном конкретном месте.

Оптимизация – повышение эффективности работы локальной компьютерной сети, путем логического разделения рабочих станций их друг от друга с помощью технологии VLAN.

1. **Организационно-техническая часть**
   1. **Краткая характеристика организации**

«Красноярский колледж радиоэлектроники и информационных технологий» (далее колледж) официально начинает свою деятельность 12 января 2015 года. И вместе с тем, история эта насчитывает не одно десятилетие. Дело в том, что КГБПОУ «Красноярский колледж радиоэлектроники и информационных технологий» образовался в результате реорганизации путем слияния двух заведений среднего профессионального образования города Красноярска – КГБОУ СПО «Красноярский техникум информатики и вычислительной техники» и КГБОУ СПО «Красноярский колледж радиоэлектроники, экономики и управления».

Красноярский техникум информатики и вычислительной техники зарекомендовал себя как современное, динамично развивающееся учебное заведение, вошел в рейтинг «100 лучших ссузов России», в 2012 году стал победителем конкурсного отбора в рамках долгосрочной целевой программы по модернизации сети образовательных учреждений среднего профессионального образования в номинации «Высокотехнологичный центр профессионального образования по отрасли «Информатизация и телекоммуникация».

В настоящее время Красноярский колледж радиоэлектроники и информационных технологий приглашает получить качественное образование по 5 направлениям подготовки:

09.00.00 Информатика и вычислительная техника

11.00.00 Электроника, радиотехника и системы связи

15.00.00 Машиностроение

20.00.00 Техносферная безопасность и природообустройство

38.00.00 Экономика и управление

Организационная структура колледжа (рисунок 1) представляет собой структурную модель, выступающую базой распределения обязанностей сотрудников данной организации.

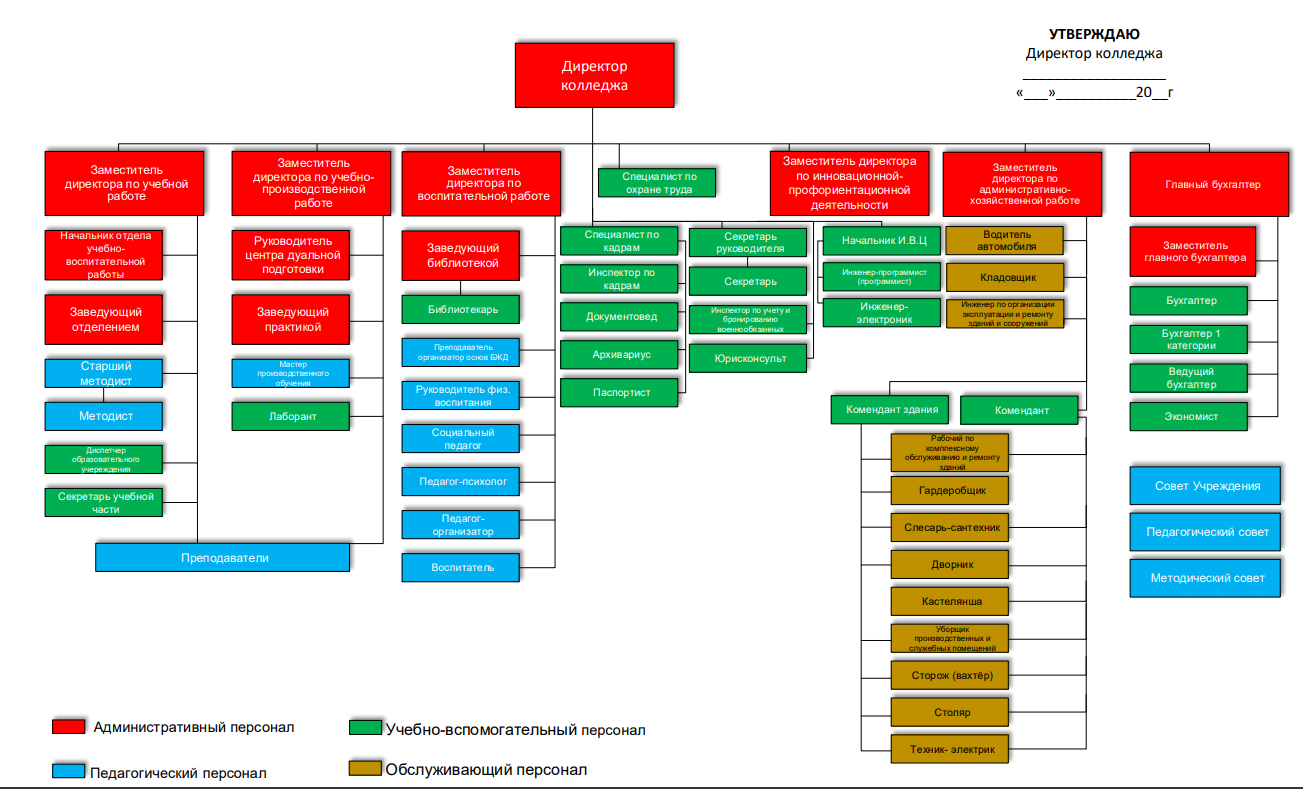


Рисунок 1 – Организационная структура организации

* 1. **Спецификация оборудования организации**

В колледже используется сетевое оборудование (таблица 1), а также: рабочие станции, принтеры и МФУ, камеры видеонаблюдения.

Таблица 1 – Сетевое оборудование сети колледжа

|  |  |  |
| --- | --- | --- |
| Тип | Технические характеристики | Кол-во |
| 1 | 2 | 3 |
| Межсетевой экран | Модель: Cisco ASA 5505  Количество портов: 8 x RJ-45  Пропускная способность: до 150 Мбит/с  Дополнительные возможности: поддерживает механизмы шифрования AES | 1 |

|  |  |  |
| --- | --- | --- |
| Окончание таблицы 2 | | |
| 1 | 2 | 3 |
| Коммутатор | Модель: Cisco Catalyst 2960  Объем оперативной памяти: 64 Мб  Объем флеш-памяти: 32 Мб  Количество портов коммутатора: 24 x 10/100 Мбит/сек  Внутренняя пропускная способность: 16 Гбит/с  Размер таблицы MAC адресов: 8192  Поддержка стандартов: Auto MDI/MDIX, Priority tags, VLAN, STP | 3 |
| Модель: [D-Link DES-1016D](https://market.yandex.ru/product--kommutator-3com-baseline-switch-2948-sfp-plus/1570436?nid=55404)  Количество портов: 16  Пропускная способность: 3,2 Гбит/сек | 1 |
| Модель: TP-Link TL-SG1024D  Количество портов коммутатора: 24 порта 10/100/1000 Мбит/с  Внутренняя пропускная способность: 48 Гбит/с  Размер таблицы MAC адресов: 8192 | 1 |
| Модель: PLANET GSD-802PS  Количество портов коммутатора: 8 Gigabit PoE  Внутренняя пропускная способность: 16 Гбит/с  Размер таблицы MAC адресов: 8192 | 1 |
| Модель: Allied Telesis AT-GS950/24  Количество портов коммутатора: 24 x Ethernet 10/100/1000  Внутренняя пропускная способность: 32 Гбит/с  Размер таблицы MAC адресов: 8192 | 1 |
| Сервер | Модель: HP DL160 G6  Процессор: 2x Xeon 4C E5640  ОЗУ: 64 Gb  Хранилище: 2 SAS, 2 HDD | 2 |
| HP DL380 G4  Процессор: Intel Xeon 4215R  ОЗУ: 32Gb  Хранилище: 2 HDD | 1 |
| Thecus N8800 PRO  Процессор: Intel® Core™ 2 Duo  ОЗУ: 4 ГБ DDR2  Хранилище: 8 HDD | 1 |

* 1. **Спецификация программного обеспечения организации**

В колледже установлено программное обеспечение для управления локальной сетью и оборудованием (таблице 2), а также программное обеспечения для обучения студентов: КОМПАС-3D, Cisco Packet Tracer, Microsoft Office, Autodesk Inventor, Delphi, Microsoft Visual Studio,

Таблица 2 – Программное обеспечение сети колледжа

|  |  |
| --- | --- |
| Название | Описание |
| 1 | 2 |
| Cisco Adaptive Security Device Manager (ASDM) | Веб-интерфейс для управления межсетевым экраном Cisco ASA 5505 |
| PuTTY | Программное обеспечние для различных протоколов удалённого доступа, включая SSH, Telnet, rlogin |
| WireShark | Программное обеспечение для анализа сетевого трафика сетей Ethernet |
| AnyDesk | Программное обеспечение для удаленного управления компьютером |
| VMWare Workstation | Программное обеспечение для создания виртуальных машин |
| TeamViewer | Программное обеспечение для удаленного управления компьютером |
| Acronis True Image | Программное обеспечение клонирования жестких дисков |
| WinSCP | Программное обеспечение для защищенного подключения к FTP-серверу |
| Veeam Backup & Replication | Программное обеспечение для резервного копирование виртуальных машин и их восстановления |
| Windows 10 Для образовательных учреждений | Операционная система для пользователей |
| Windows Server 2016 | серверная операционная система |

* 1. **Анализ существующей сети**

В колледже имеется локальная сеть с древовидной топологией, корнем которой является межсетевой экран Cisco ASA 5505, c его помощью осуществляется связь локальной сети со вторым учебным отделением, находящимся по адресу пр. им. газеты Красноярский рабочий 156, а также с сетью Интернет. К межсетевому экрану подключен неуправляемый коммутатор D-Link DES-1016D, к которому подключены сервера и управляемый коммутатор Cisco Catalyst 2960. Он используется для подключения других коммутаторов, находящихся в кабинетах, камер видеонаблюдения, а также к нему подключен еще один управляемый коммутатор Cisco Catalyst 2960 для увеличения количества подключаемых устройств (рисунок 2).

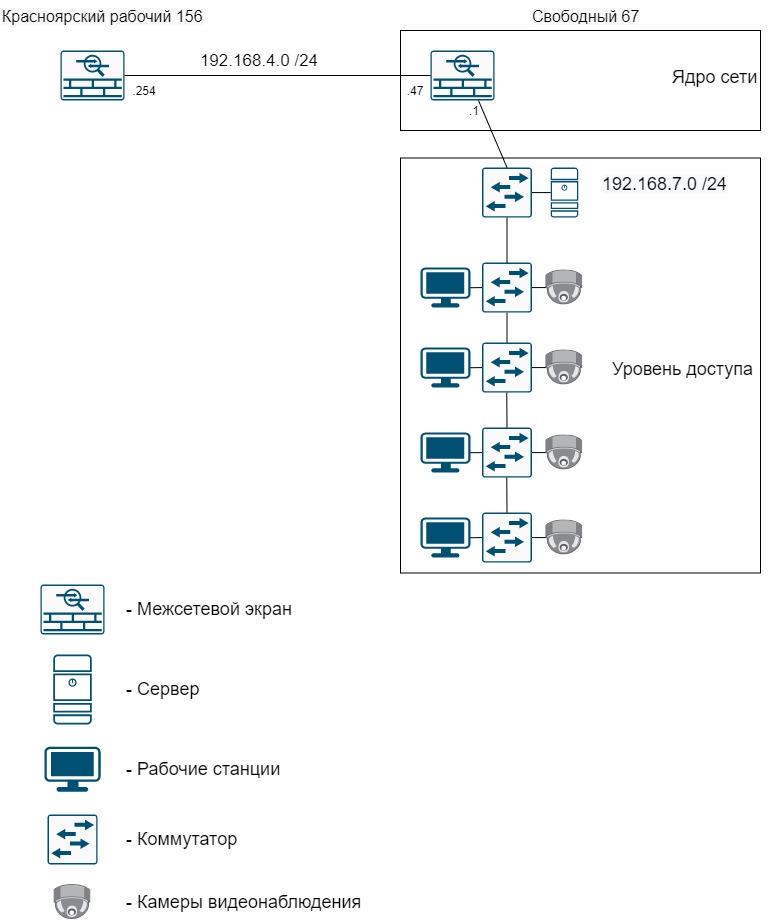


Рисунок 2 – Текущая иерархия сети колледжа

Такая схема сети сложна для администрирования из-за отсутствия уровня распределения. Все устройства находятся в одном широковещательном домене, что предполагает большое количество широковещательного трафика, который значительно уменьшает производительность сети. Также из-за отсутствия сегментации сети разные типы трафика смешаны между собой и, например, трафик камер видеонаблюдения, которые двадцать четыре часа в сутки ведут запись и отправляют данные на сервер тоже нагружают сеть.

Из-за большого количества коммутаторов, к которым могут быть подключены, как и конечные устройства, такие как рабочие станции, сетевые МФУ, камеры видеонаблюдения, так и другие коммутаторы локальная сеть менее отказоустойчива ведь в случае выхода какого-нибудь коммутатора из строя без сети могут остаться устройства разного типа, разной важности и в разных местах.

Поэтому планируется добавить новый уровень распределения, установить имеющийся управляемый коммутатор, который, используя технологию VLAN будет разделять между собой трафик пользователей, кабинета 227, в которой оборудована компьютерная лаборатория, трафик управления, а также трафик камер видеонаблюдения. VLAN 7 и 8 будут иметь идентификатор по цифре в третьем октете IP-адреса подсети, VLAN 227 будет иметь идентификатор по номеру кабинета, VLAN для камер видеонаблюдения будет идентификатор 100. Кроме того, будет настроена защита от петель второго уровня, защита от неавторизованных DHPC-серверов, контроль за широковещательным трафиком. Будет организован безопасный удаленный доступ к управляемым коммутаторам по протоколу SSH.

1. **Рабочая часть**
   1. **Проектирование схемы подключения**

В иерархию сети будет добавлен новый уровень распределения, который будет разделять сеть колледжа на три подсети для подключения рабочих станций и одну подсеть для камер видеонаблюдения. Все четыре подсети будут ограничены друг от друга с помощью VLAN, так подсеть для администрации будет иметь ip-адрес 192.168.7.0 /24 и идентификатор VLAN 7, подсеть для учебных аудиторий будет иметь ip-адрес 192.168.8.0 /24 и идентификатор VLAN 8, подсеть для кабинета 227 иметь ip-адрес 192.168.9.0 /24 идентификатор VLAN 227 и подсеть для камер видеонаблюдения будет иметь идентификатор VLAN 100 (рисунок 3).

Все также корнем сети будет межсетевой экран Cisco ASA 5505, который подключен к отделению по адресу пр. им. газеты Красноярский рабочий 156, будет иметь три виртуальных интерфейса, которые в свою очередь связаны с физическими интерфейсами. Виртуальные интерфейсы будут иметь первый ip-адрес из подсети и будут выступать основными шлюзами. Каждый физический интерфейс представляет отдельную подсеть и имеет свой номер VLAN.

От межсетевого экрана будут идти три кабеля в главный управляемый коммутатор Cisco Catalyst 2960, интерфейсы которого будут иметь номер VLAN в соответствие с номером VLAN на интерфейсе Cisco ASA. Все остальные устройства будут подключены к главному коммутатору с соответствующим номером VLAN.

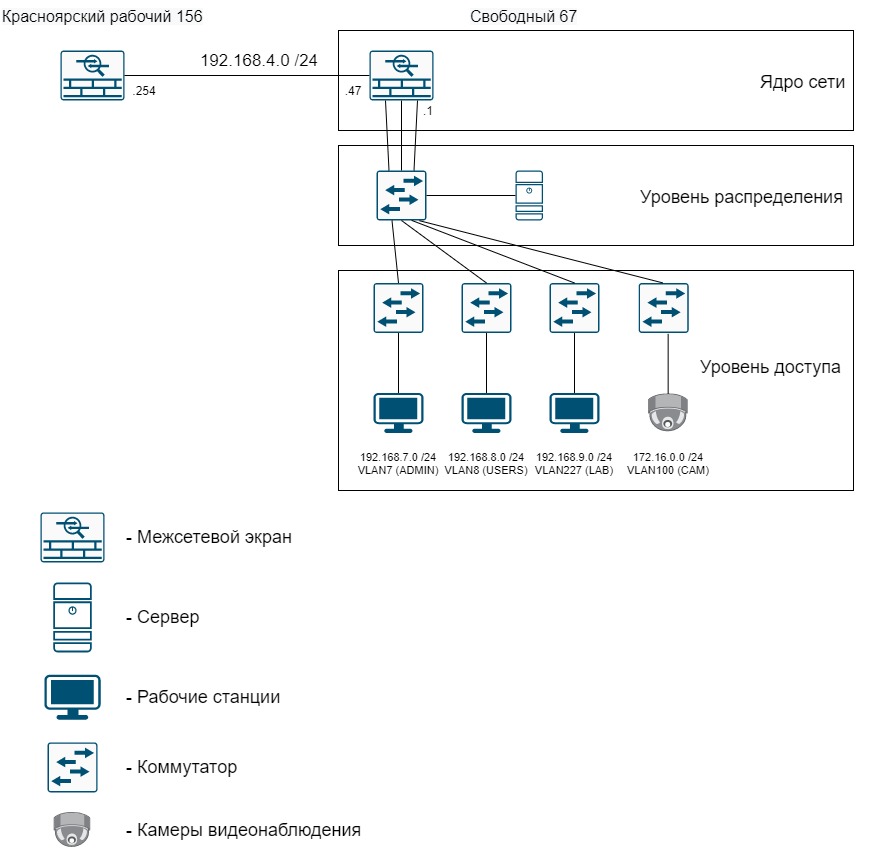
****

Рисунок – Новая иерархия сети колледжа

* 1. **Подключение и настройка оборудования**

В этом подразделе описан процесс подключения и настройки межсетевого экрана Cisco ASA 5505 и управляемых коммутаторов Cisco Catalyst 2960.

* + 1. Подключение уровня распределения сети

Межсетевой экран Cisco ASA имеет 8 физических интерфейсов, к интерфейсу Ethernet0/0 был подключен кабель, который идет от провайдера. К интерфейсам Ethernet0/1, Ethernet0/2 и Ethernet0/3 подключены кабели (рисунок 4), соединяющие межсетевой экран с интерфейсами коммутатора FastEthernet0/1, FastEthernet0/2 и FastEthernet0/3 (рисунок 5).



Рисунок 4 – Подключение межсетевого экрана

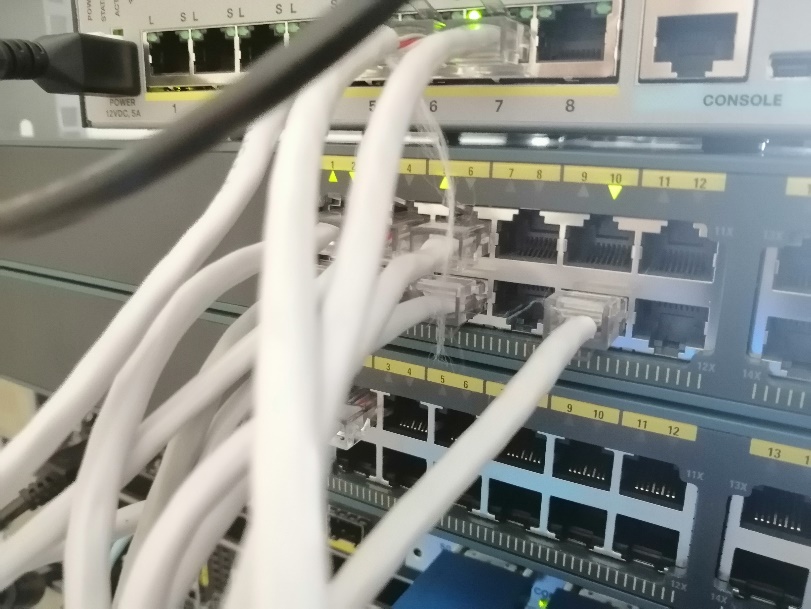


Рисунок 5– Подключение главного коммутатора

В интерфейс FastEthernet0/4 подключен коммутатор для рабочих станций в VLAN 8 (рисунок 6)

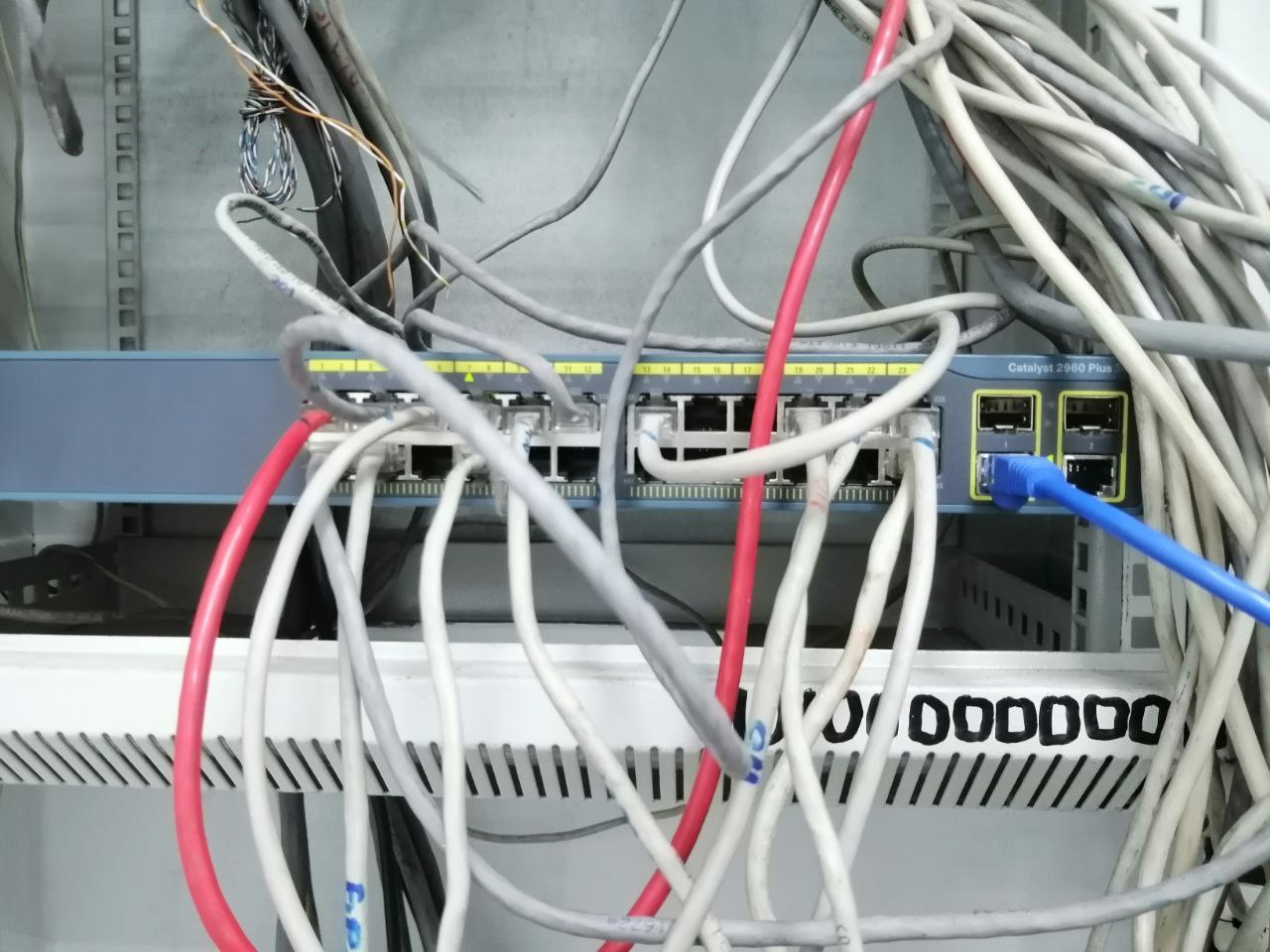
. 

Рисунок 6 – Коммутатор для рабочих станций в VLAN 8

В интерфейс FastEthernet0/6 подключен коммутатор для рабочих станций в VLAN 227 (рисунок 7).

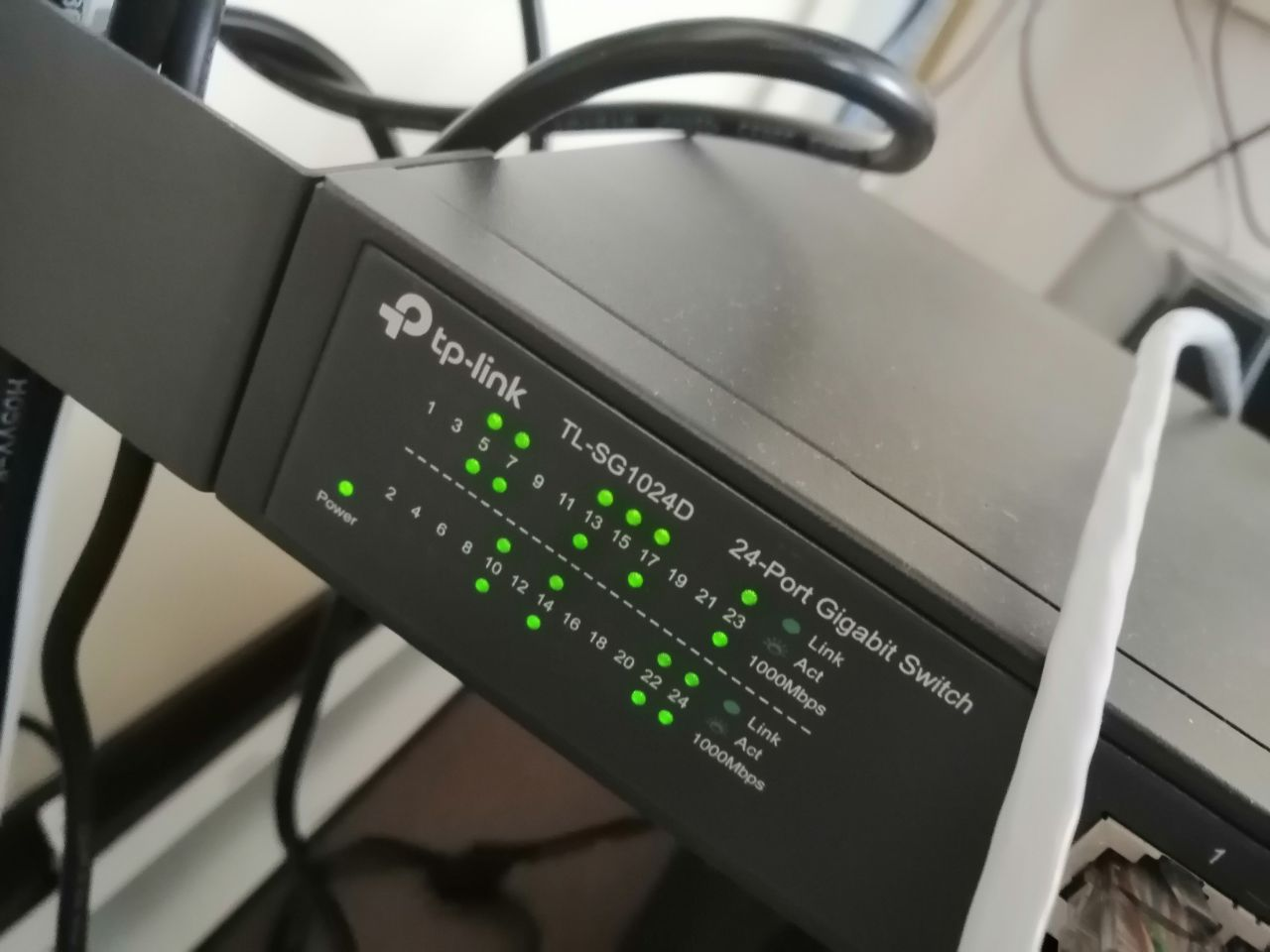


Рисунок – Коммутатор для рабочих станций в VLAN 227

* + 1. Настройка межсетевого экрана Cisco ASA 5505

После подключения распределительного коммутатора был настроен межсетевой экран. Так как он был уже предварительно настроен все дальнейшие действия были выполнены с помощью программного обеспечения ASDM (рисунок 8).



Рисунок 8 – Программное обеспечение ASDM

Трем интерфейсам были заданы идентификаторы VLAN (рисунки 9–11), каждому из них были заданы ip-адреса, имена и уровень безопасности (рисунки 12–15).

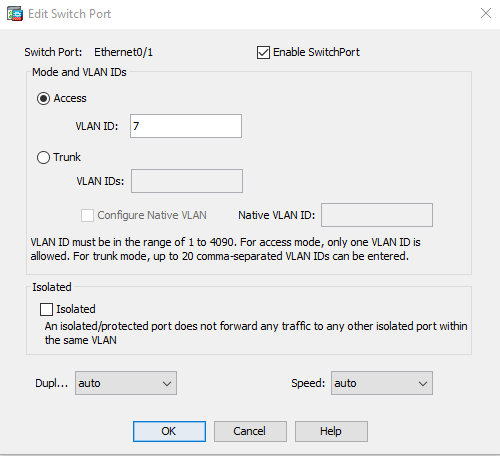


Рисунок 9 – Настройка идентификатора VLAN для интерфейса Ethernet0/1

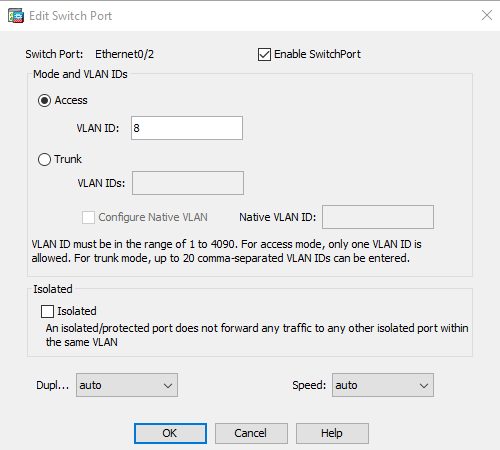


Рисунок 10 – Настройка идентификатора VLAN для интерфейса Ethernet0/2

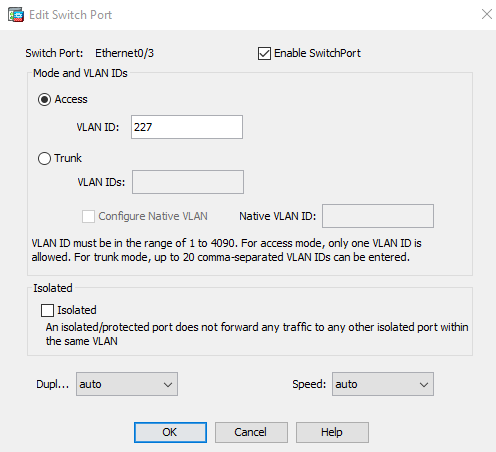


Рисунок 11 – Настройка идентификатора VLAN для интерфейса Ethernet0/3

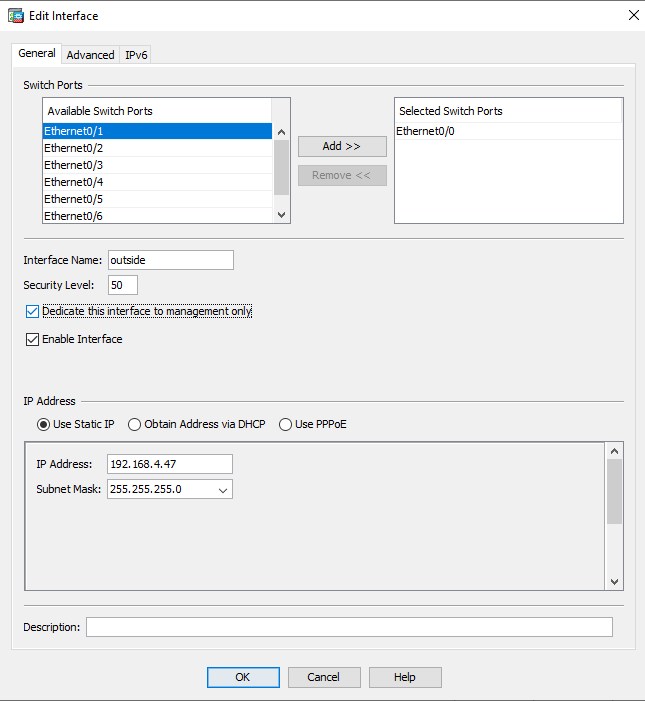


Рисунок 12 – Настройка IP-адреса для интерфейса Ethernet0/0

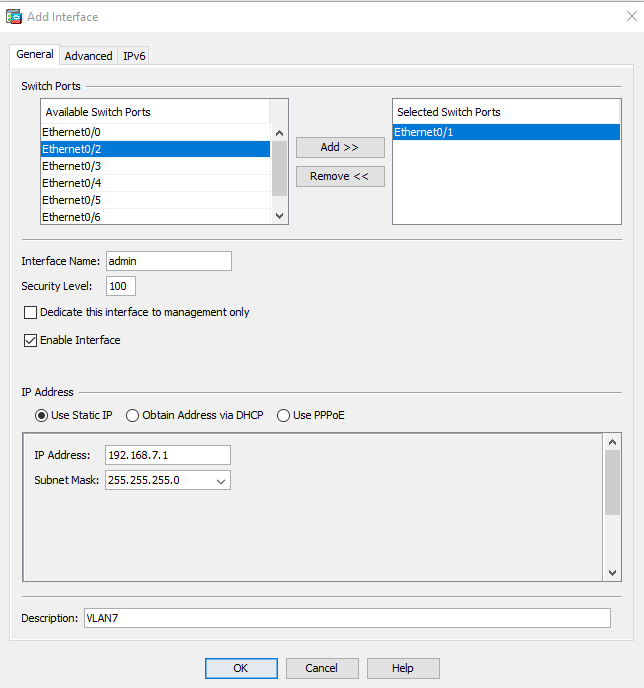


Рисунок 13 – Настройка IP-адреса для интерфейса Ethernet0/1

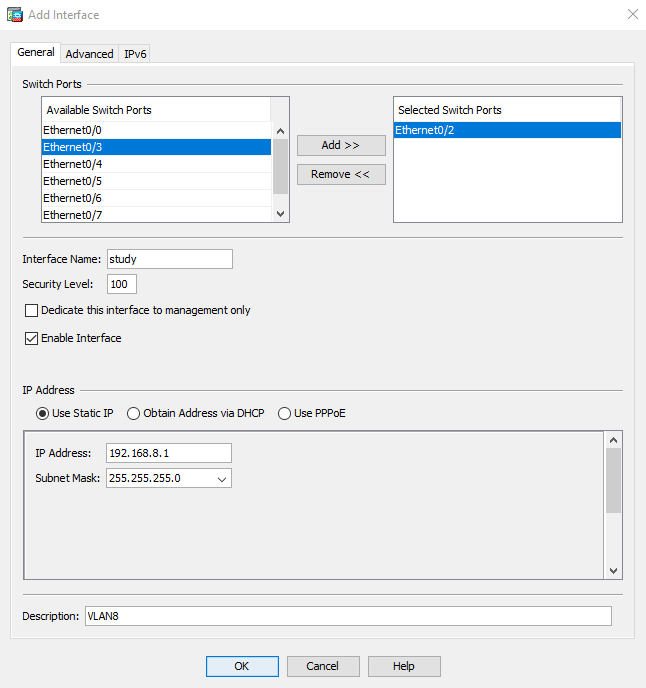


Рисунок 14 – Настройка IP-адреса для интерфейса Ethernet0/2

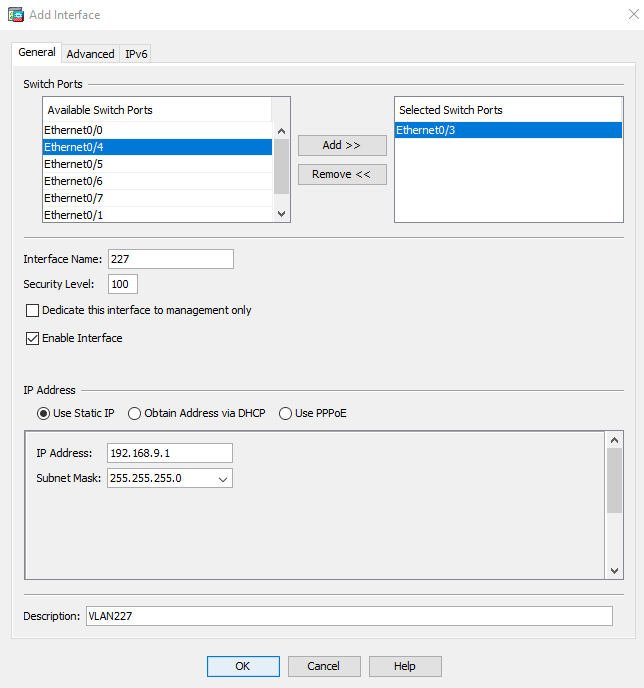


Рисунок 15 – Настройка IP-адреса для интерфейса Ethernet0/3

Были настроены необходимые списки доступа (ACL) (рисунок 16)

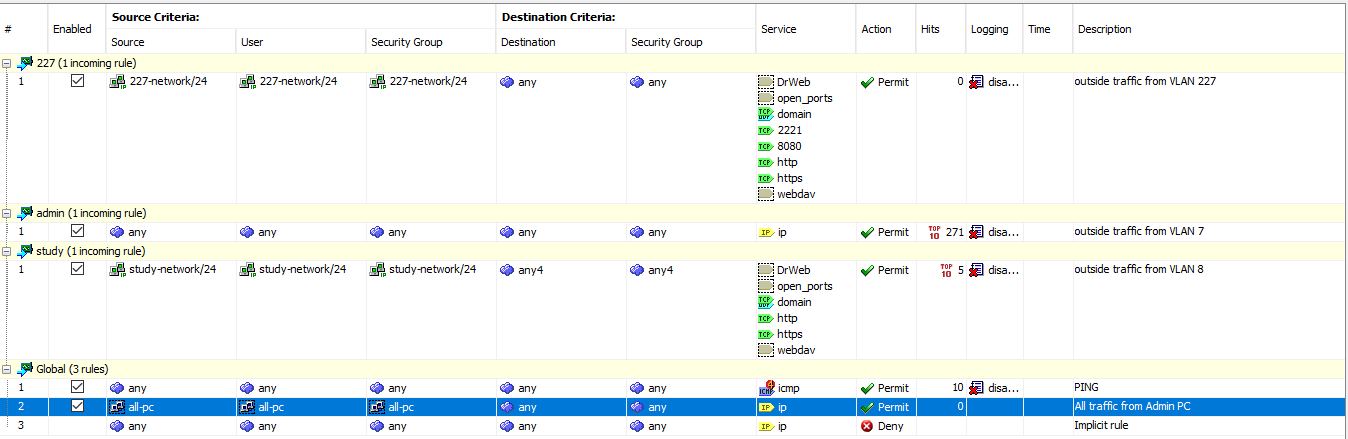


Рисунок 16 – Списки доступа

Была настроена трансляция сетевых адресов (NAT) для трёх подсетей (рисунки 17–19).

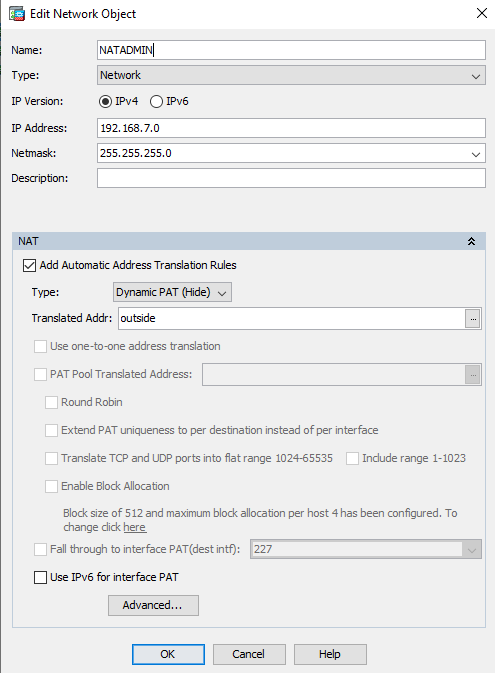


Рисунок 17 – NAT для VLAN 7

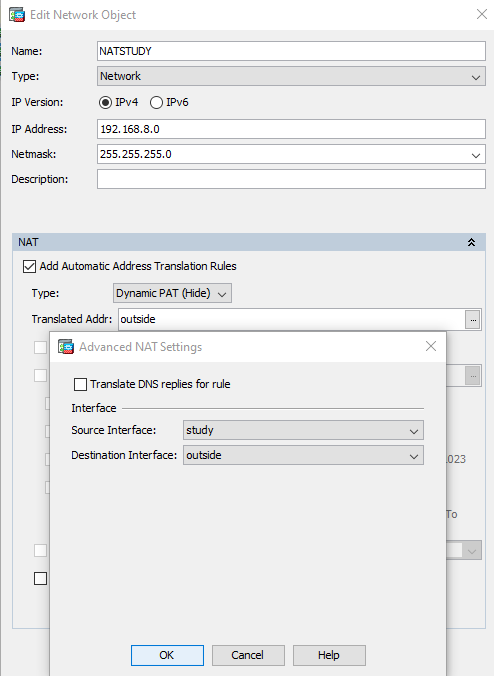


Рисунок 18 – NAT для VLAN 8

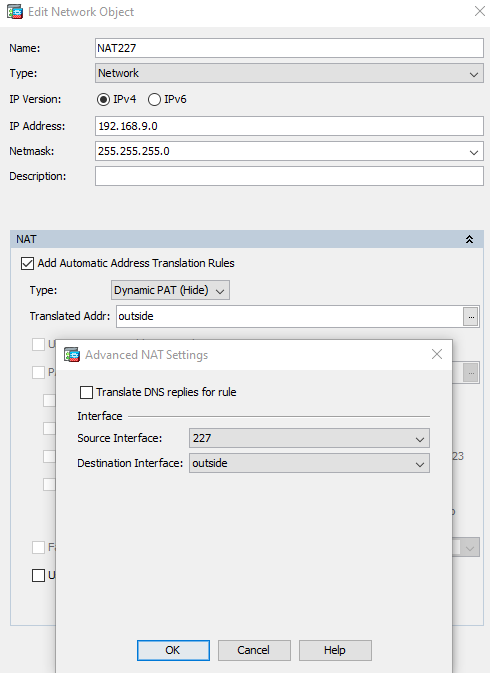


Рисунок 19 – NAT для VLAN 227

Был настроен статический маршрут до второго учебного корпуса (рисунок 20).

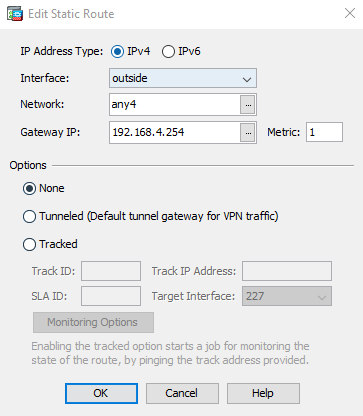


Рисунок 20 – Статический маршрут

Так как теперь DHCP-сервер находится в отдельной подсети, была настроена функция DHCP-ретрансляции (DHCP Relay), которая перехватывает запросы от DHCP-клиентов из других подсетей и отправляет их DHCP-серверу (рисунки 21–22).

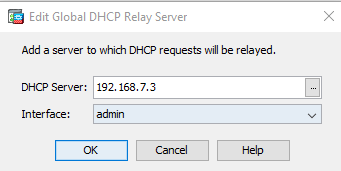


Рисунок 21 – IP-адрес DHCP-сервера

Рисунок 22 – Активация DHCP Relay

Был настроен удаленный доступ к межсетевому экрану. Подключиться к нему можно с помощью протокола SSH, а также с помощью ПО ASDM (рисунок 23).



Рисунок – Настройка удаленного доступа

* + 1. Настройка управляемых коммутаторов Cisco Catalyst 2960

Для настройки коммутаторов использовалось консольное подключение и ПО PuTTY (рисунки 24–25).



Рисунок 24 – Консольное подключение

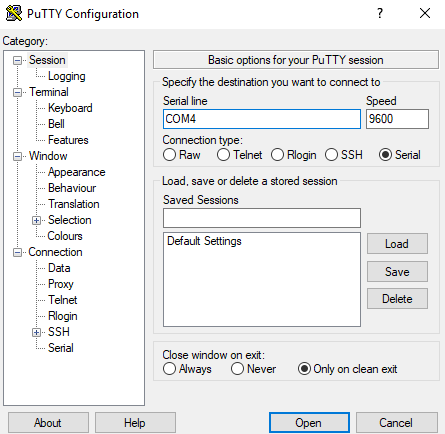


Рисунок 25 – Программное обеспечение PuTTY

Была выполнена первоначальная настройка управляемого коммутатора уровня распределения (рисунки 26–30).

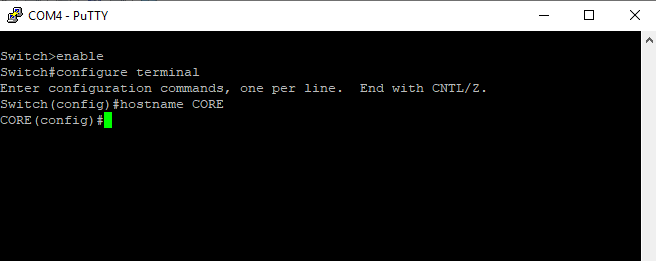


Рисунок 26 – Назначение имени главному коммутатору

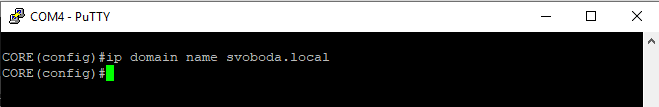


Рисунок 27 – Назначение домена

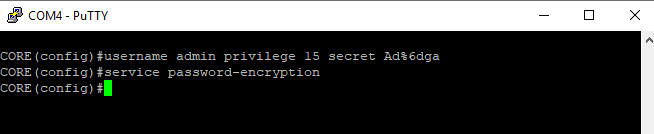


Рисунок 28 – Добавление пользователя и шифрование паролей

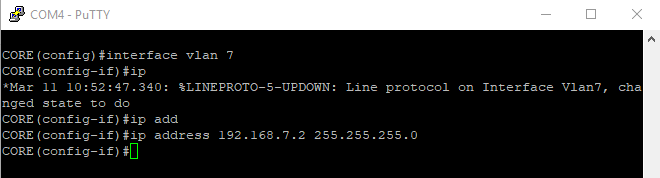


Рисунок 29 – Назначение IP-адреса главному коммутатору

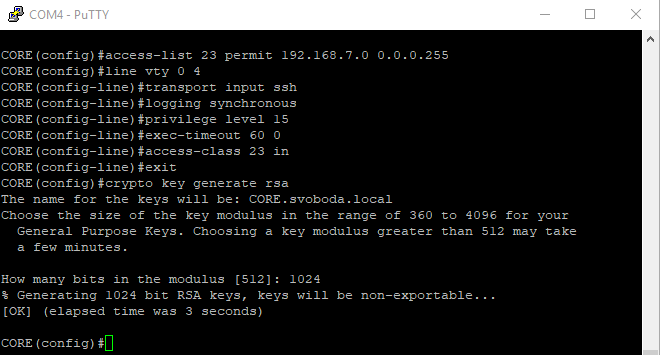


Рисунок 30– Настройка удаленного доступа SSH

Были добавлены VLAN (рисунок 31).

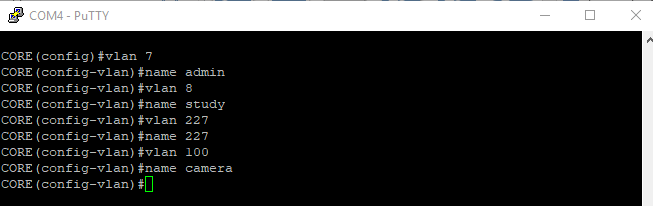


Рисунок 31 – Добавление VLAN

Интерфейсам были назначены идентификаторы VLAN (рисунки 32–35).



Рисунок 32 – Назначение идентификатора VLAN 7

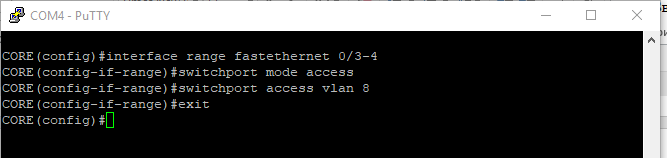


Рисунок 33 – Назначение идентификатора VLAN 8

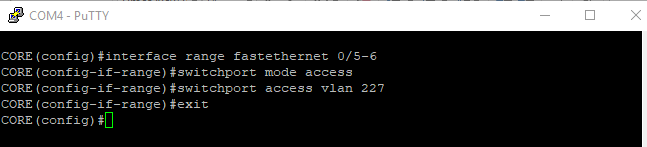


Рисунок 34 – Назначение идентификатора VLAN 227



Рисунок 35 – Назначение идентификатора VLAN 100

Была настроена защита от неавторизованных DHCP-серверов (рисунок 36).

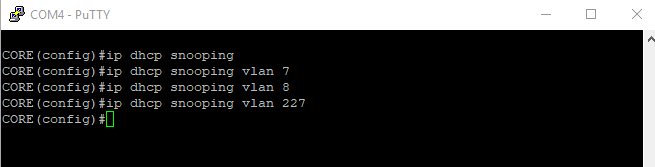


Рисунок 36 – Активация DHCP Snooping на существующих VLAN

DHCP-сервер подключен к главному коммутатору к интерфейсу FastEthernet0/10 и он был указан как доверительный интерфейс (рисунок 37).

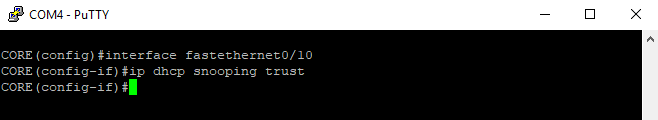


Рисунок 37 – Настройка доверительного интерфейса

Также был настроен коммутатор для подключения рабочих станций для студентов и преподавателей, который находится в VLAN 8 (рисунок 38).

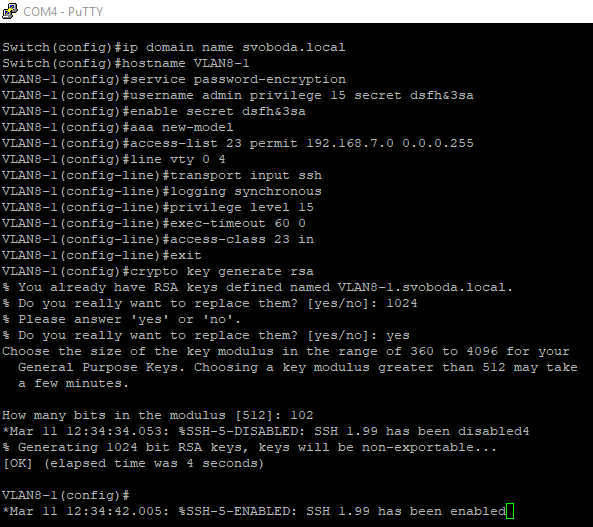


Рисунок 38 – Настройка коммутатора для VLAN 8

Теперь рабочие станции и другие сетевые устройства логически разделены друг от друга на втором уровне OSI, но вcё равно могут использовать общие ресурсы локальной сети. В случае выхода из строя сетевого оборудования, стало возможно легко отследить его принадлежность к определенной сети VLAN и уменьшить время решения проблемы.

* 1. **Настройка программного обеспечения**

В этом подразделе описан процесс настройки DHCP-сервера в Windows Server 2016.

* + 1. Настройка Windows Server

Так как DHCP-сервер уже автоматически раздаёт ip-адреса из сети 192.168.7.0 /24 (рисунок 39), были добавлены еще два области ip-адресов для VLAN 8 и 227, 192.168.8.0 /24 и 192.168.9.0 /24.

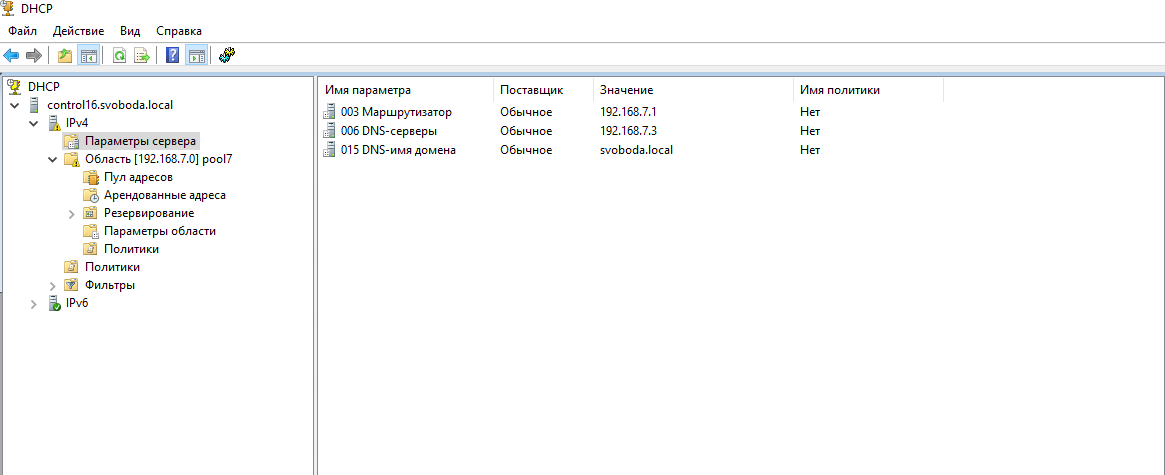


Рисунок 39 – Область для VLAN 7

Создание области ip-адресов производилась в операционной системе Windows Server 2016 с помощью Мастера создания области (рисунок 40).

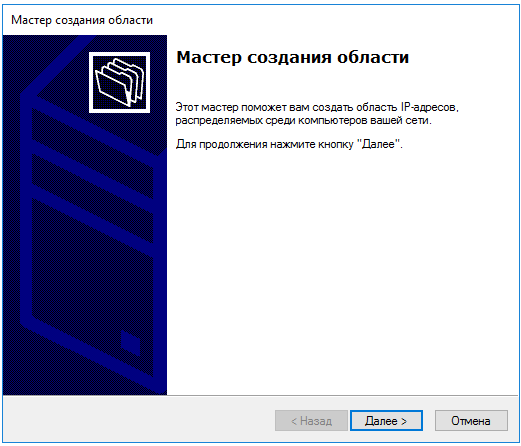


Рисунок 40 – Мастер добавления области

Новой области было дано имя с соответсвии с идентификатором VLAN, имя pool8 для VLAN 8 (рисунок 41) и pool227 для VLAN 227 (рисунок 42).

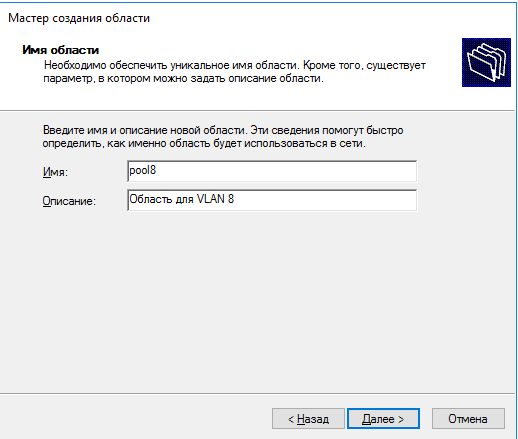


Рисунок 41 – Имя области для VLAN 8

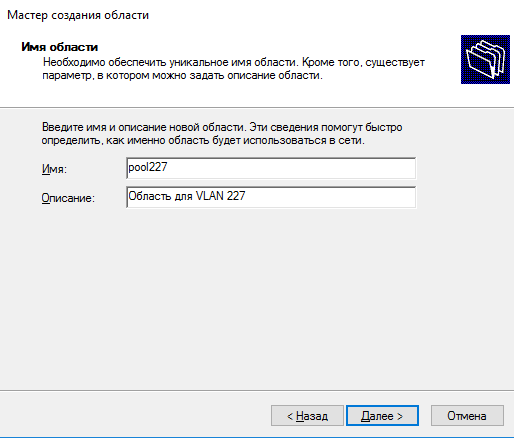


Рисунок 42 – Имя области для VLAN 227

Был указан диапазон ip-адресов для новой области, для VLAN 8 это 192.168.8.1–192.168.8.254 c маской подсети 24 бит (рисунок 43), для VLAN 227 это 192.168.9.1–192.168.9.254 c маской подсети 24 бит (рисунок 44).

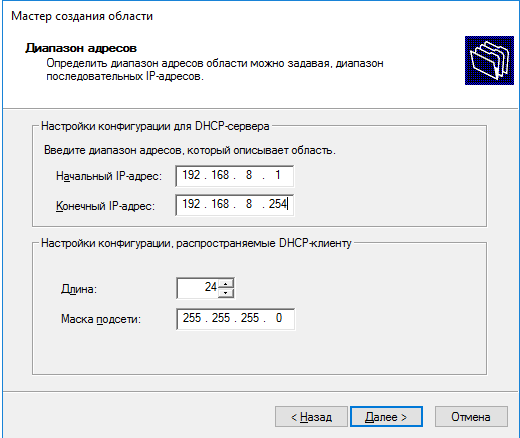


Рисунок 43 – Диапазон ip-адресов для VLAN 8

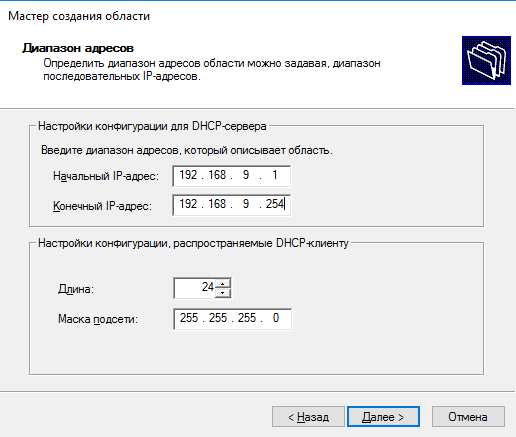


Рисунок 44 – Диапазон ip-адресов для VLAN 227

Были указаны первые двадцать адресов из области, которые DHCP-сервер не должен раздавать клиентам, они будут указаны вручную системными администраторами, для VLAN 8 это 192.168.8.1–192.168.8.20 (рисунок 45), для VLAN 227 это 192.168.9.1–192.168.9.20 (рисунок 46).

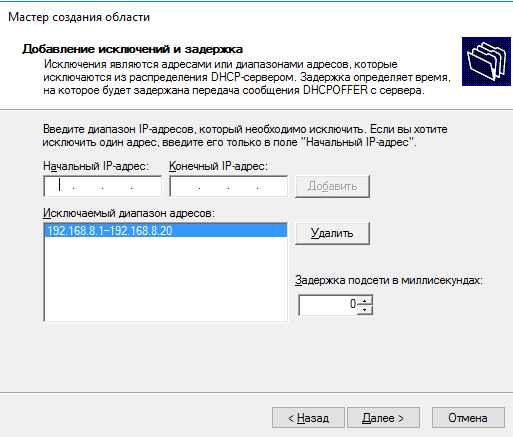


Рисунок 45 – Исключаемый диапазон адресов для VLAN 8

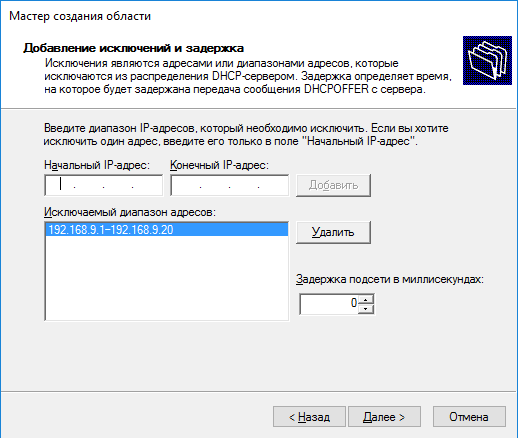


Рисунок 46 – Исключаемый диапазон адресов для VLAN 227

Срок аренды ip-адреса для VLAN 8 и 227 был указан 12 часов (рисунок 47).

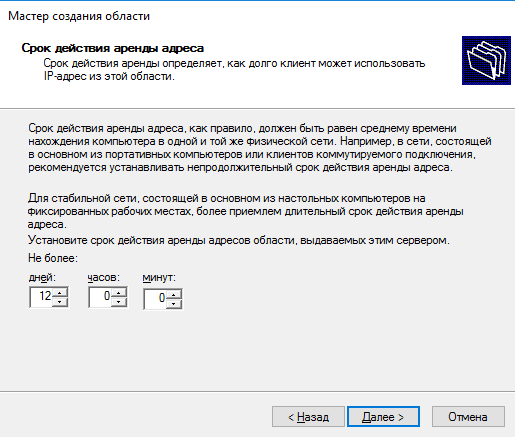


Рисунок 47 – Срок аренды адреса

Адресами основного шлюза были выбраны ip-адреса виртуальных интерфейсов Cisco ASA, для VLAN 8 это 192.168.8.1 (рисунок 48), для VLAN 227 это 192.168.9.1 (рисунок 49).

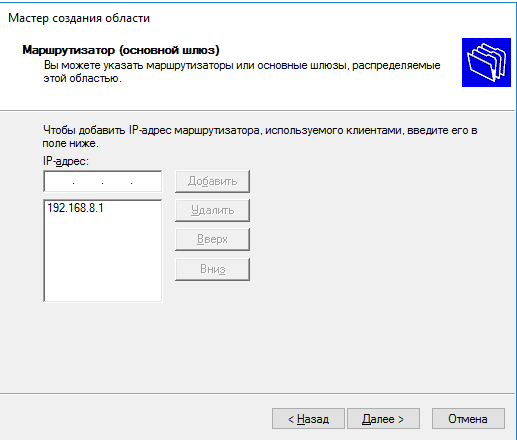


Рисунок 48 – Адрес основного шлюза для VLAN 8

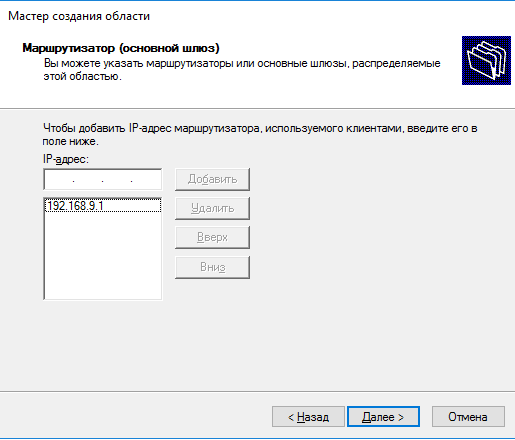


Рисунок 49 – Адрес основного шлюза для VLAN 227

Адресом DNS-сервера и WINS-сервера был выбран ip-адрес данного Windows Server 2016 для VLAN 8 и 227 (рисунки 50–51).

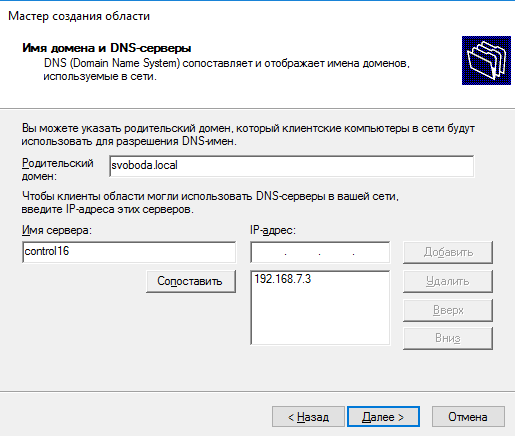


Рисунок 50 – Адрес DNS-сервера

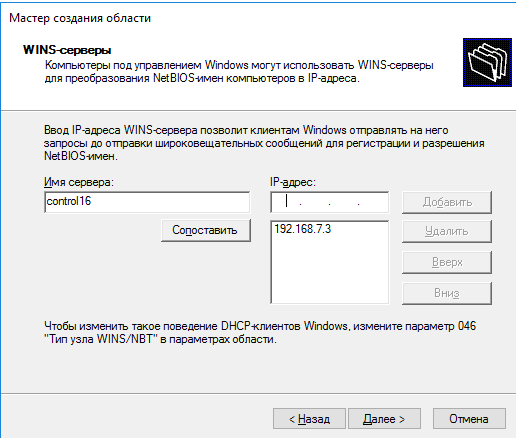


Рисунок 51 – Адрес WINS-сервера

Теперь для каждой подсети есть своя область ip-адресов и устройства будут получать параметры сетевых адаптеров автоматически (рисунок 52).

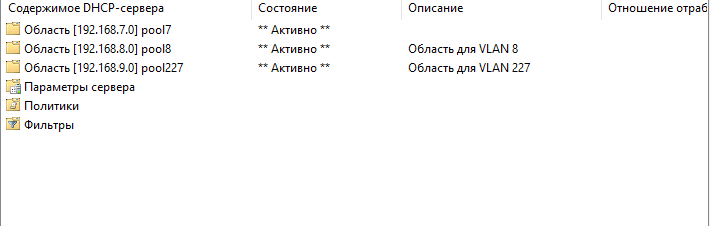


Рисунок 52 – Области DHCP-сервера

Для проверки работоспособности DCHP-сервера, на рабочей станции, подключённой к коммутатору в VLAN 8, в параметрах сетевого адаптера была включена опция «Получить IP-адрес автоматически» (рисунок 53).

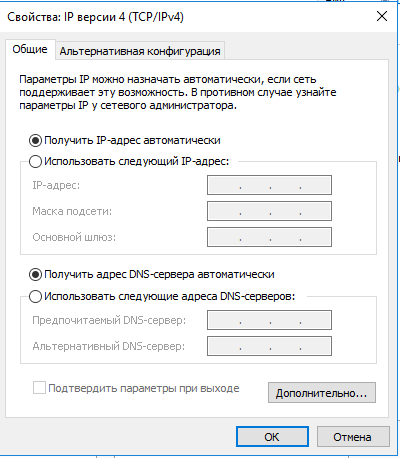


Рисунок 53 – Параметры сетевого адаптера

Через пару секунд рабочая станция автоматически получила ip-адрес из подсети для VLAN 8 (рисунок 54), а другая из подсети для VLAN 227 (рисунок 55).

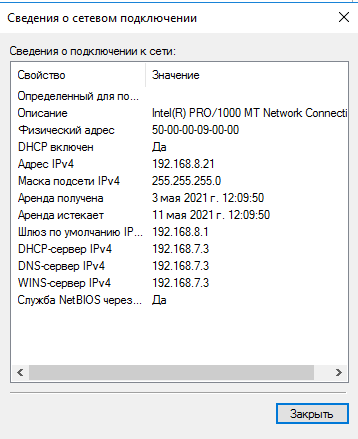


Рисунок 54 – Сведения о сетевом подключении VLAN 8

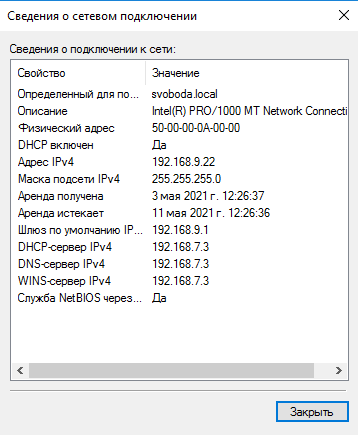


Рисунок 55 – Сведения о сетевом подключении VLAN 227

В программе ASDM теперь отображается статистика получения DHCP-запросов и ответов, хотя на самом межсетевом экране DHCP-сервер не настроен, он является ретранслятором для Windows Server 2016 (рисунок 56).

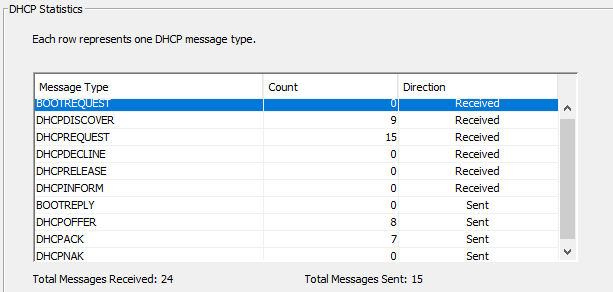


Рисунок 56 – Статистика DCHP

Теперь все устройства получают параметры сетевого подключения автоматически, исходя из принадлежности к подсети VLAN.

1. **Экономическая часть**
   1. **Расчет**
2. **Охрана труда и техника безопасности**

**ЗАКЛЮЧЕНИЕ**

В процессе прохождения преддипломной практики была достигнута цель и были выполнены следующие задания:

1. организована бесперебойная работа системы по резервному копированию и восстановлению информации;
2. выполнена установка, тестирование и эксплуатация информационных систем, согласно технической документации;
3. произведена настройка аппаратного и программного обеспечения сетевой инфраструктуры;
4. выполнены операции резервного копирования и восстановления данных;
5. выполнено обеспечение антивирусной защиты в организации;
6. произведена проверка контроля доступа, сохранение целостности данных и журналирование;
7. осуществлена диагностики и поиск неисправностей технических средств;
8. выполнено тестирование кабеля;
9. выполнена замена расходных материалов и выполнен мелкий ремонт периферийного оборудования.

**СПИСОК СОКРАЩЕНИЙ**

ПК – персональный компьютер

ФЗ – федеральный закон

ОС – операционная система

ОЗУ – оперативное запоминающее устройство

ПО – программное обеспечение

ИБ – информационная безопасность

ИБП – источник бесперебойного питания

ЭВМ – электронно-вычислительная машина

**БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ**

1. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры: учебник / А.В. Назаров, А.Н. Енгалычев, В.П. Мельников. - Москва: КУРС; ИНФРА-М, 2020. — 360 с.
2. Щеглов, А. Ю. Анализ и проектирование защиты информационных систем. Контроль доступа к компьютерным ресурсам: методы, модели, технические решения / А. Ю. Щеглов, К. А. Щеглов; под ред. М. В. Финкова. - Санкт-Петербург: Профессиональная литература, 2017. - 415 с.
3. Сандерс Крис Анализ пакетов. Практическое руководство по использованию Wireshark и tcpdump для решения реальных. - 3-е изд. - 448 с.
4. Михаил Михеев Администрирование VMware vSphere 5. - 3-е изд. ДМК Пресс, 2016. - 504 с.
5. Таненбаум Э.С., Уэзеролл Д. Компьютерные сети. - 5-е изд. Прогресс книга, 2021. - 960 с.
6. В. Ф. Шаньгин Информационная безопасность и защита информации. ДМК Пресс, 2017. - 702 с.
7. Решение для резервного копирования данных // Veeam URL: https://www.veeam.com/ru/vm-backup-recovery-replication-software.html (дата обращения: 08.04.2021).
8. Комплекты «Для школ» для учреждений дошкольного, начального, среднего и дополнительного образования // Dr. Web Антивирус URL: https://products.drweb.ru/bundles/safe\_school/ (дата обращения: 06.04.2021).