Министерство образования Красноярского края

Краевое государственное бюджетное профессиональное образовательное учреждение

«Красноярский колледж радиоэлектроники и информационных технологий»

**Допущена к защите**

Зам. директора по учебной работе

\_\_\_\_\_\_\_\_\_\_ / М.А. Полютова

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

**(ДИПЛОМНАЯ РАБОТА**

**или**

**ДИПЛОМНЫЙ ПРОЕКТ)**

Оптимизация локальной компьютерной сети КГБПОУ «ККРИТ» используя

технологию VLAN

тема

09.02.02 Компьютерные сети

код и наименование специальности

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись, дата инициалы, фамилия

Руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись, дата инициалы, фамилия

Консультант \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись, дата инициалы, фамилия

Нормоконтроль \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись, дата инициалы, фамилия

Рецензент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись, дата инициалы, фамилия

Красноярск, 2021г

**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](#_Toc69987338)

[1. Организационно-техническая часть 5](#_Toc69987339)

[1.1 Краткая характеристика организации 5](#_Toc69987340)

[1.2 Спецификация оборудования организации 6](#_Toc69987341)

[1.3 Спецификация программного обеспечения организации 8](#_Toc69987342)

[1.1 Анализ существующей сети 8](#_Toc69987343)

[2.1. Проектирование схемы подключения 9](#_Toc69987344)

[2.2. Подключение и настройка оборудования 9](#_Toc69987345)

[2.3. Настройка программного обеспечения 9](#_Toc69987346)

[3. Экономическая часть 10](#_Toc69987347)

[3.1. Расчет 10](#_Toc69987348)

[4. Охрана труда и техника безопасности 11](#_Toc69987349)

[4.1. Охрана труда в учебном заведении 11](#_Toc69987350)

[СПИСОК СОКРАЩЕНИЙ 13](#_Toc69987351)

[БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ 14](#_Toc69987352)

[ПРИЛОЖЕНИЕ А 15](#_Toc69987353)

[ПРИЛОЖЕНИЕ Б 17](#_Toc69987354)

[ПРИЛОЖЕНИЕ В 19](#_Toc69987355)

[ПРИЛОЖЕНИЕ Г 21](#_Toc69987356)

[ПРИЛОЖЕНИЕ Д 23](#_Toc69987357)

**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.

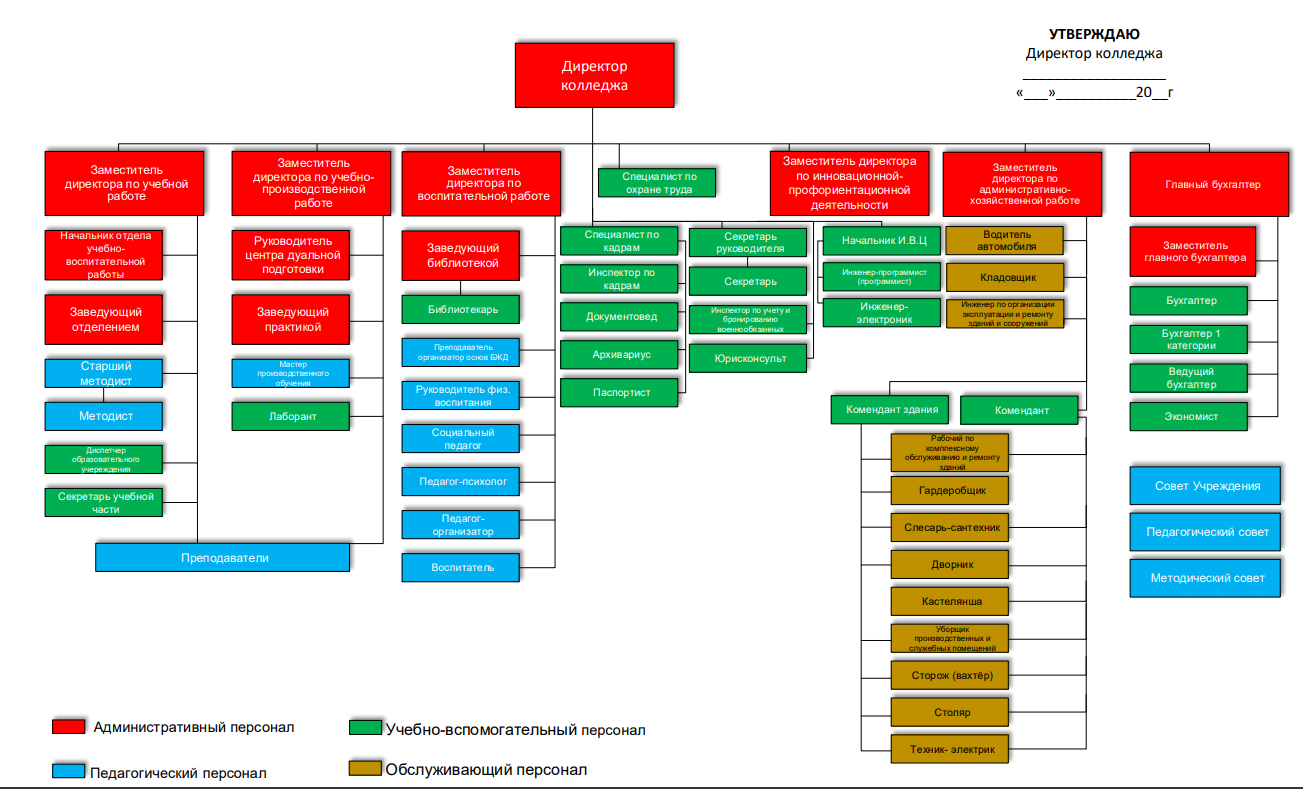


Рисунок 1 – Организационная структура организации

* 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 организации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |
| 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 |
| Окончание таблицы 1 | | |  |  |
| 1 | 2 | | | 3 |
|  | 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 |

* 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 организации

|  |  |
| --- | --- |
| Название | Описание |
| 1 | 2 |
| Cisco Adaptive Security Device Manager (ASDM) | понятный и удобный веб-интерфейс, которым можно пользоваться без специальных знаний командной оболочки устройства |
| PuTTY | свободно распространяемый клиент для различных протоколов удалённого доступа, включая SSH, Telnet, rlogin |
| Служба Удаленного рабочего стола Windows | компонент Microsoft Windows, позволяющий пользователям удаленно запускать приложения или управлять сервером с любой машины |
| WireShark | программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других |
|  |  |
|  |  |
| Windows Server 2016 | серверная операционная система от Microsoft |

* 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).

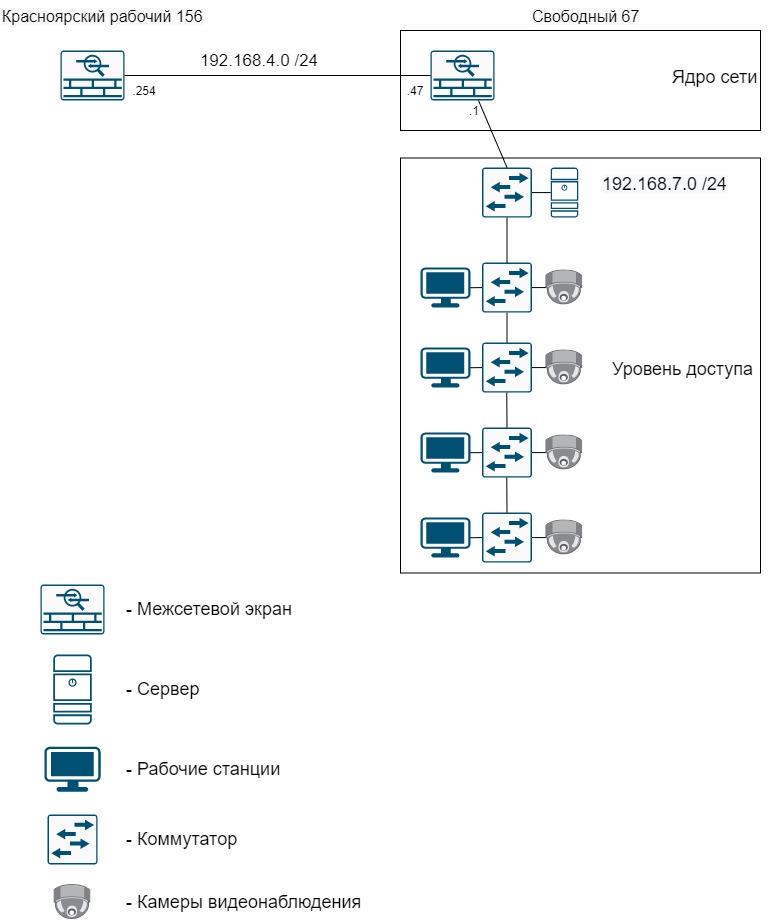


Рисунок – Текущая иерархия сети колледжа

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.

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.

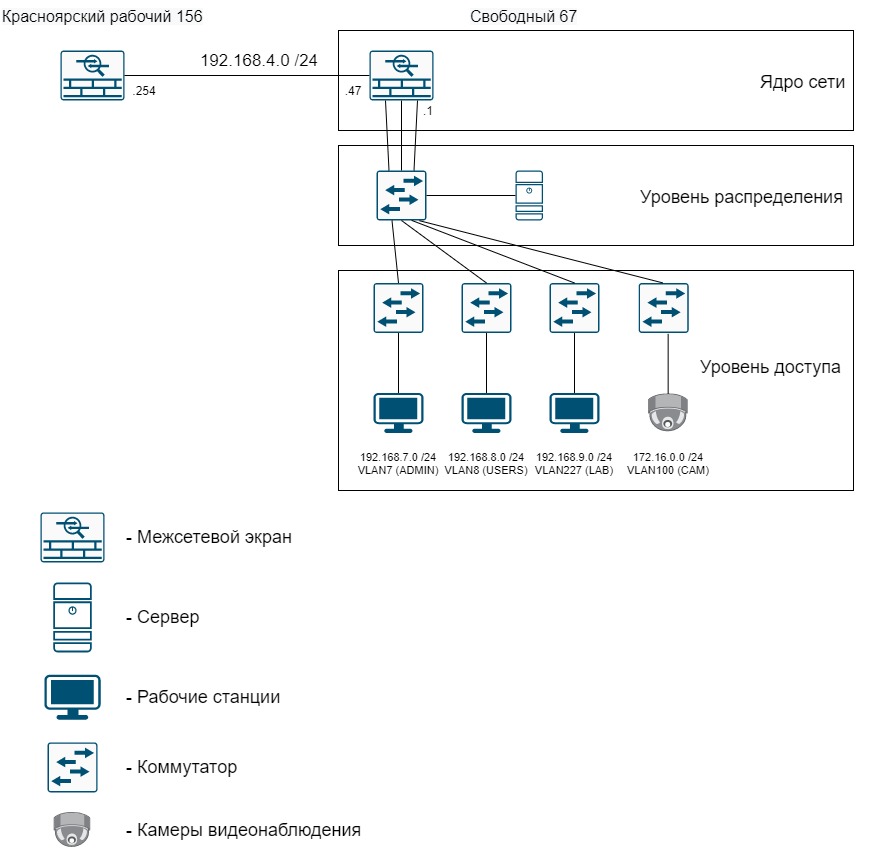
****

Рисунок 3 – Новая иерархия сети колледжа

* 1. **Подключение и настройка оборудования**

В этом разделе 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 – Подключение межсетевого экрана

Рисунок коммутатора

Рисунок – Подключение межсетевого экрана

* + 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 6).



Рисунок – Программное обеспечение ASDM

Были добавлены виртуальные интерфейсы по номеру VLAN (рисунок 2), заданы ip-адреса, каждому из них (рисунок 2). Виртуальные интерфейсы были связаны с физическими портами Cisco ASA (рисунок 2). Были настроены необходимые списки доступа (ACL) (рисунок 2)

трансляция адресов (NAT) (рисунок 2),

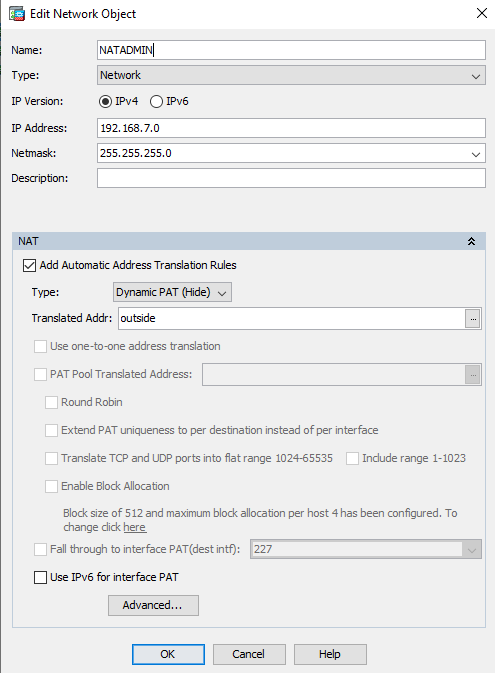


Рисунок – NAT для VLAN 7

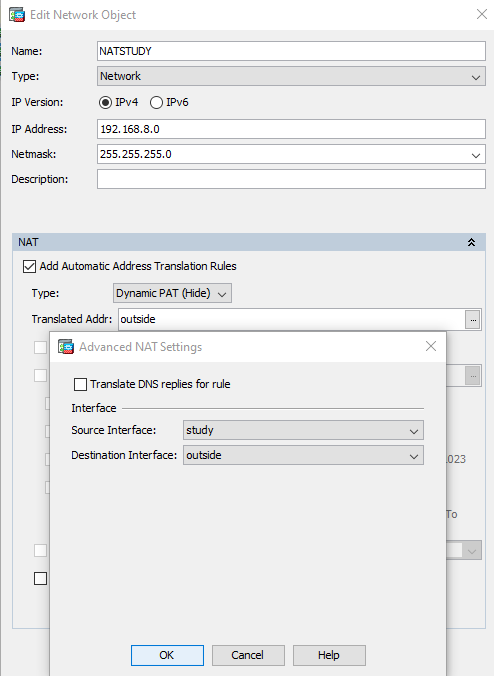


Рисунок – NAT для VLAN 8

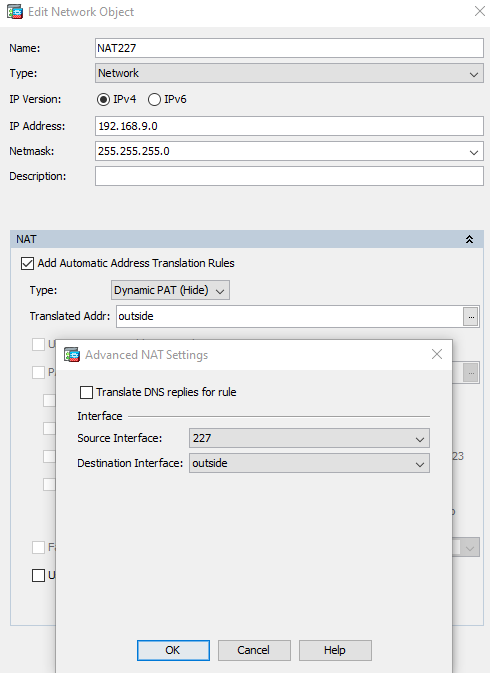


Рисунок – NAT для VLAN 227

настроен статический маршрут до второго учебного корпуса (рисунок 2).

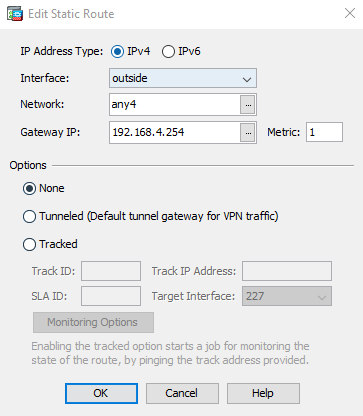


Рисунок – Статический маршрут

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 (рисунок 2).

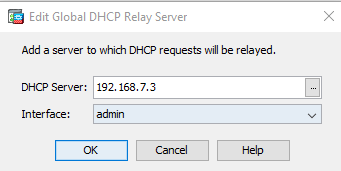


Рисунок – IP-адрес DHCP-сервера



Рисунок – Активация DHCP Relay



Рисунок – Настройка удаленного доступа

* + 1. Настройка управляемых коммутаторов Cisco Catalyst 2960

Настройка управляемого коммутатора уровня распределения заключалась в том, чтобы произведена первоначальная настройка (рисунок 2), добавлены и назначены соответствующим интерфейсам VLAN (рисунок 2), настроена защита от неавторизованных DHCP- серверов (рисунок 2),

* 1. **Настройка программного обеспечения**

В этом разделе описан процесс настройки Windows Server 2016.

* + 1. Настройка Windows Server

Так как DHCP-сервер уже автоматически раздаёт ip-адреса из сети 192.168.7.0 /24 (рисунок 6), были добавлены еще два области ip-адресов для VLAN 8 и 227, 192.168.8.0 /24 и 192.168.9.0 /24.

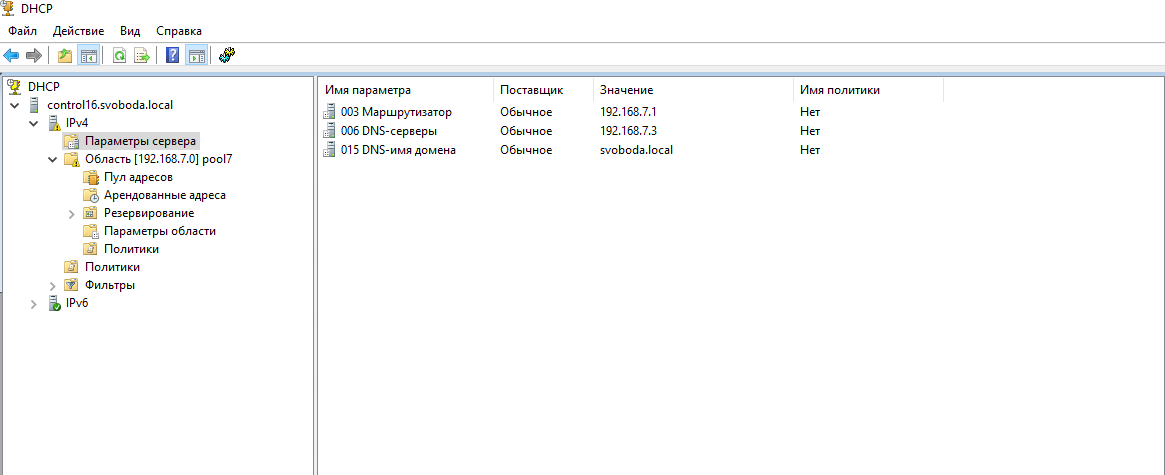


Рисунок – Область для VLAN 7

Создание области ip-адресов производилась в операционной системе Windows Server 2016 с помощью Мастера создания области (рисунок 7).

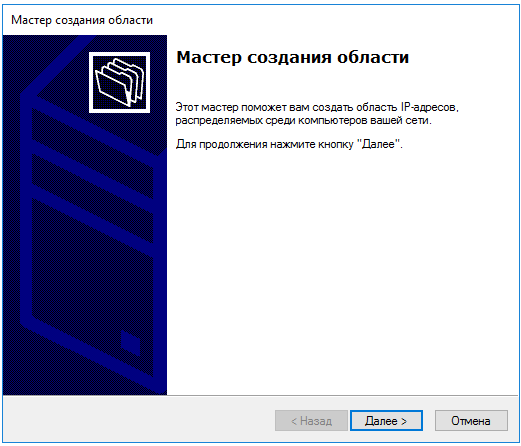


Рисунок – Мастер добавления области

Новой области было дано имя с соответсвии с идентификатором VLAN, имя pool8 для VLAN 8 (рисунок 8) и pool227 для VLAN 227 (рисунок 9).

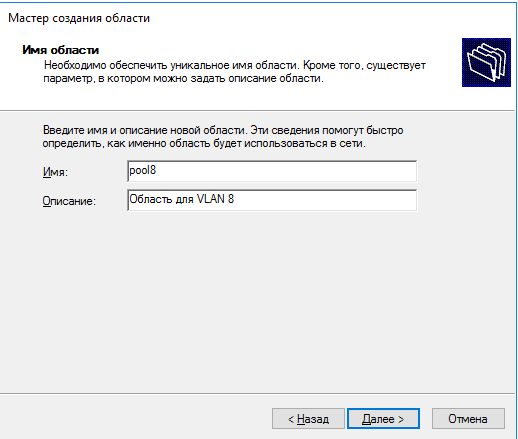


Рисунок – Имя области для VLAN 8

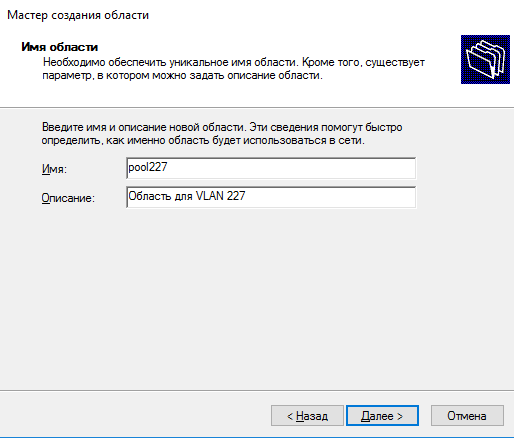


Рисунок – Имя области для VLAN 227

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 10), для VLAN 227 это 192.168.9.1–192.168.9.254 c маской подсети 24 бит (рисунок 11).

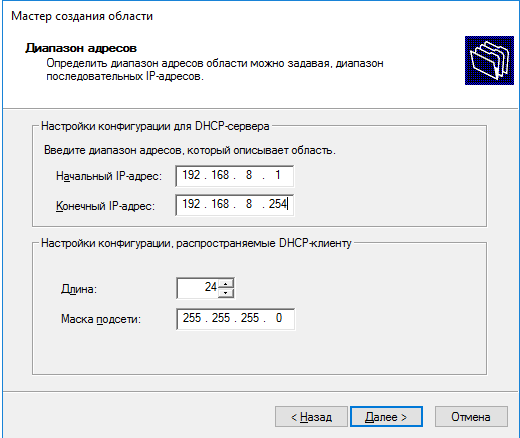


Рисунок – Диапазон ip-адресов для VLAN 8

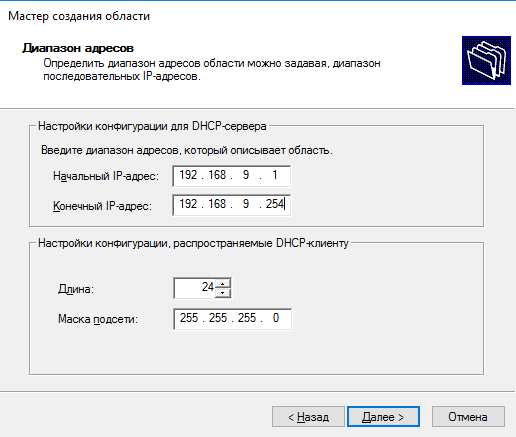


Рисунок – Диапазон ip-адресов для VLAN 227

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 12), для VLAN 227 это 192.168.9.1–192.168.9.20 (рисунок 13).

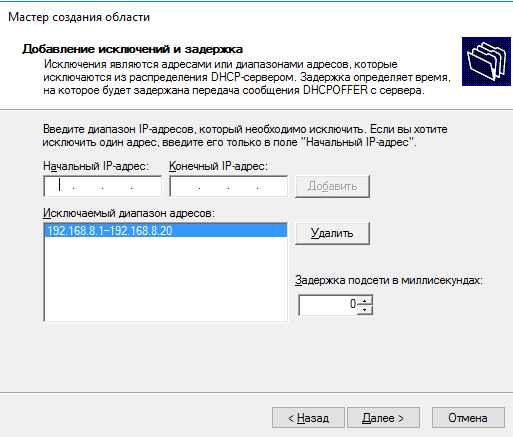


Рисунок – Исключаемый диапазон адресов для VLAN 8

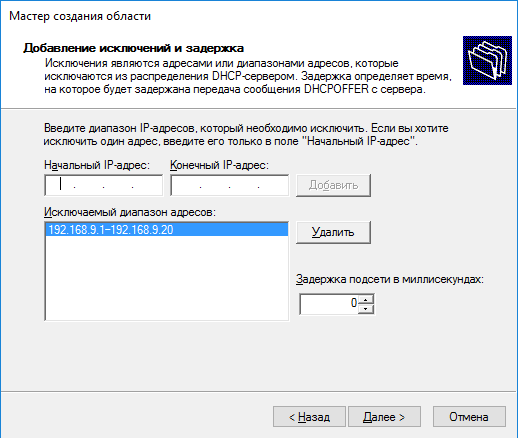


Рисунок – Исключаемый диапазон адресов для VLAN 227

Срок аренды ip-адреса для VLAN 8 и 227 был указан 12 часов (рисунок 14).

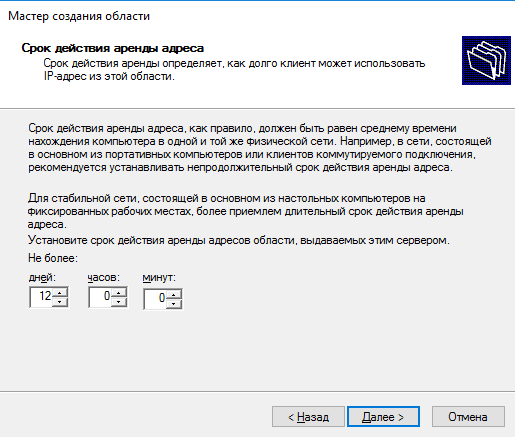


Рисунок – Срок аренды адреса

Адресами основного шлюза были выбраны ip-адреса виртуальных интерфейсов Cisco ASA, для VLAN 8 это 192.168.8.1 (рисунок 15), для VLAN 227 это 192.168.9.1 (рисунок 16).

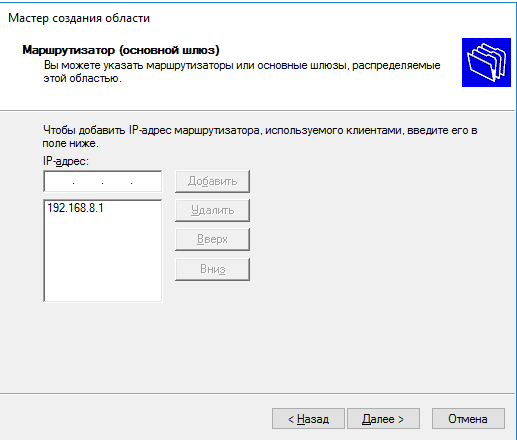


Рисунок – Адрес основного шлюза для VLAN 8

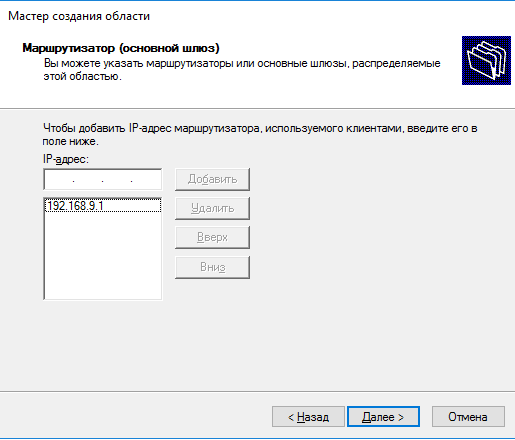


Рисунок – Адрес основного шлюза для VLAN 227

Адресом DNS-сервера и WINS-сервера был выбран ip-адрес данного Windows Server 2016 для VLAN 8 и 227 (рисунки 17–18).

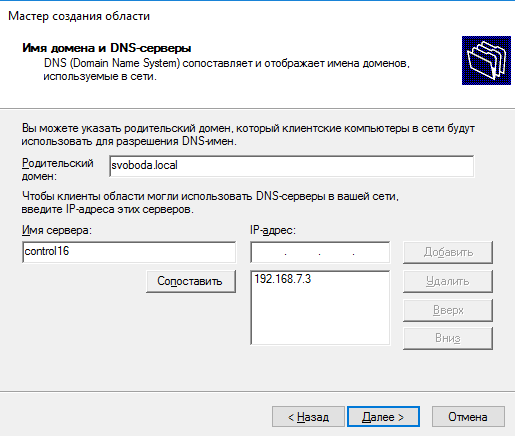


Рисунок – Адрес DNS-сервера

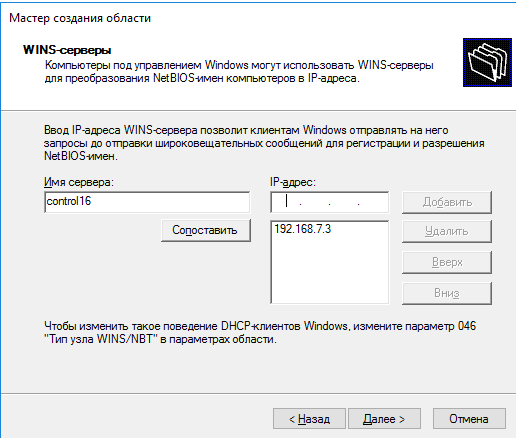


Рисунок – Адрес WINS-сервера

Теперь для каждой подсети есть своя область ip-адресов и устройства будут получать параметры сетевых адаптеров автоматически (рисунок 19).

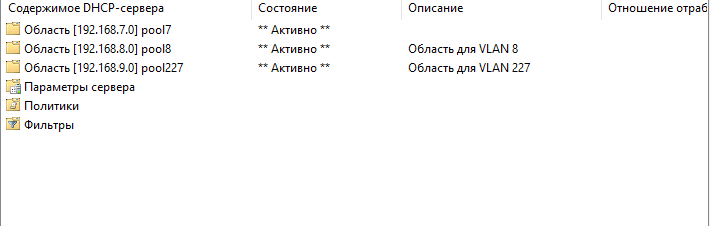


Рисунок – Области DHCP-сервера

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 21).

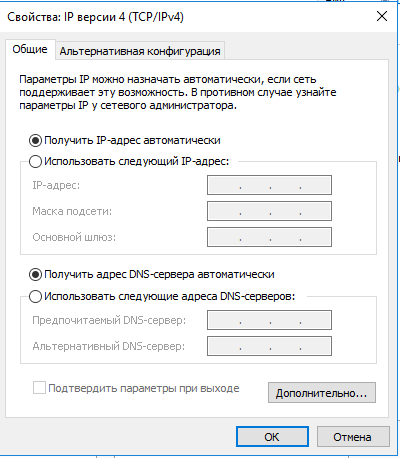


Рисунок – Параметры сетевого адаптера

Через пару секунд рабочая станция автоматически получила ip-адрес из подсети для VLAN 8 (рисунок 21), а другая из подсети для VLAN 227 (рисунок 22).

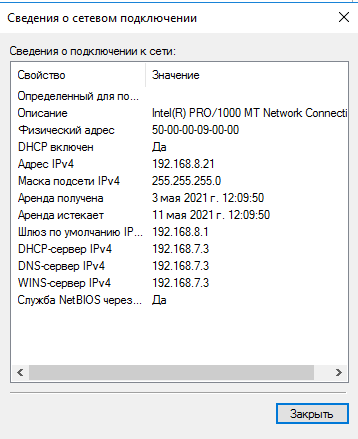


Рисунок – Сведения о сетевом подключении VLAN 8

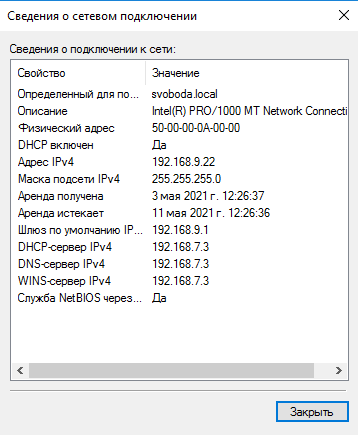


Рисунок – Сведения о сетевом подключении VLAN 227

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 23).

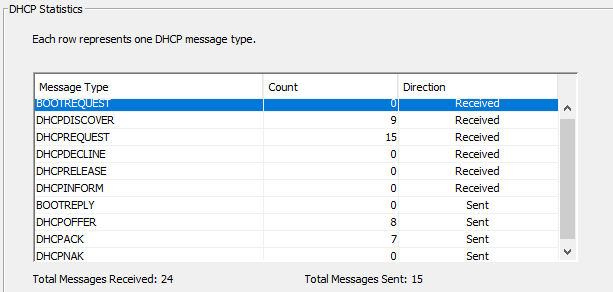


Рисунок – Статистика DCHP

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

Охрана труда – это система сохранения жизни и здоровья работников в процессе трудовой деятельности, включающая в себя правовые, социально-экономические, организационно-технические, санитарно-гигиенические, лечебно-профилактические, реабилитационные и иные мероприятия, образующие механизм реализации конституционного права граждан на труд (ст. 37 Конституции РФ) в условиях, отвечающих требованиям безопасности и гигиены.

Техника безопасности — вид деятельности (система организационных и технических мероприятий, защитных средств и методов) по обеспечению безопасности любой деятельности человека, в том числе и трудовой деятельности. Ранее под таким же названием выступала и наука, предметом которой выступает такой вид деятельности, а в настоящее время развивается дисциплина синдиника с более широким кругом предметной области, поглощающая и предмет науки о технике безопасности.

# 4.1. Особенности охраны труда в образовательном учреждении

Система управления охраной труда в общеобразовательных школах, в дошкольных образовательных учреждениях, в учреждениях дополнительного образования имеет одинаковый порядок и одинаковую структуру управления охраной труда. Обеспечением безопасности жизнедеятельности в системе образования, служит правовой и организационно-методической основой формирования управленческих структур, нормативных документов.

Главной целью управления охраной труда и в целом обеспечением безопасности жизнедеятельности в системе образования является сохранение жизни и здоровья воспитанников, обучающихся и работающих в процессе труда, обучения, воспитания и организованного отдыха.

Деятельность по управлению охраной труда в системе образования направлена на:

* обеспечение выполнения требований законодательных, нормативных правовых актов по созданию здоровых и безопасных условий труда и образовательного процесса;
* организацию и проведение профилактической работы по предупреждению травматизма, профессиональной и производственно-обусловленной заболеваемости среди работающих, обеспечение их средствами индивидуальной защиты;
* предотвращение несчастных случаев с обучающимися (воспитанниками) во время проведения образовательного процесса, дорожно-транспортном, бытового травматизма и происшествий на воде;
* соблюдение требований нормативных документов по радиационной и пожарной безопасности, защите окружающей среды и действиям в чрезвычайных ситуациях;
* обеспечение безопасности эксплуатации учебных и бытовых зданий и сооружений, используемых в образовательном процессе, оборудования, приборов и технических средств обучения;
* охрану и укрепление здоровья работающих, обучающихся (воспитанников), организацию их лечебно-профилактического обслуживания, создание оптимального сочетания режимов труда, обучения, организованного отдыха;
* создание и совершенствование непрерывной системы образования в области обеспечения безопасности жизнедеятельности, включающей дошкольное, все виды общего, начальное профессиональное, среднее и высшее педагогическое образование, систему переподготовки и повышения квалификации кадров.

# 4.2. Структура службы охраны труда в образовательном учреждении

Функциональные обязанности и права работников службы охраны труда разрабатываются с учетом того, что ответственность за состояние условий и охраны труда в образовательном учреждении возложена на работодателя, а работники образовательного учреждения обязаны соблюдать нормы, правила и инструкции по охране труда, правильно применять коллективные и индивидуальные средства защиты.

В образовательном учреждении, где службе вменяются дополнительно функции по обеспечению экологической, радиационной и пожарной безопасности, создается служба (управление, отдел, сектор и др.) безопасности труда и жизнедеятельности.

Основные задачи службы охраны труда:

* организация разработки и осуществления мероприятий, направленных на улучшение состояния условий труда, предупреждение производственного травматизма и профессиональной заболеваемости;
* мониторинг и анализ состояния охраны труда на объектах образовательного учреждения;
* контроль за соблюдением требований охраны труда, выявление нарушений требований охраны труда и контроль за их своевременным устранением;
* участие в работе комиссий по контролю за состоянием охраны труда в образовательном учреждении.

Организация проведения инструктажей, обучения, проверки знаний по охране труда образовательных учреждений. Для решения своих задач служба охраны труда выполняет следующие функции:

* доводит до сведения работников вводимые в действие новые законодательные и иные нормативные правовые акты по охране труда.
* выявляет опасные и вредные производственные факторы на рабочих местах.
* выявляет опасные конструктивные недостатки оборудования, механизмов, систем защиты, контроля и управления, принимает меры для их исключения с целью предупреждения производственного травматизма.

# 4.3. Техника безопасности в компьютерной аудитории

При эксплуатации оборудования необходимо остерегаться:

* поражения электрическим током;
* механических повреждений, травм.

Требования безопасности перед началом работы:

1. запрещено входить в кабинет в верхней одежде, головных уборах, с громоздкими предметами и едой;
2. запрещено входить в кабинет информатики в грязной обуви без бахил или без сменной обуви;
3. запрещается шуметь, громко разговаривать и отвлекать других учащихся;
4. запрещено бегать и прыгать, самовольно передвигаться по кабинету;
5. перед началом занятий все личные мобильные устройства учащихся (телефон, плеер и т.п.) должны быть выключены;
6. разрешается работать только на том компьютере, который выделен на занятие;
7. перед началом работы учащийся обязан осмотреть рабочее место и свой компьютер на предмет отсутствия видимых повреждений оборудования;
8. запрещается выключать или включать оборудование без разрешения преподавателя;
9. напряжение в сети кабинета включается и выключается только преподавателем.

Требования безопасности во время работы:

1. с техникой обращаться бережно: не стучать по мониторам, не стучать мышкой о стол, не стучать по клавишам клавиатуры;
2. при возникновении неполадок: появлении изменений в функционировании аппаратуры, самопроизвольного её отключения необходимо немедленно прекратить работу и сообщить об этом преподавателю;
3. не пытаться исправить неполадки в оборудовании самостоятельно;
4. выполнять за компьютером только те действия, которые говорит преподаватель;
5. контролировать расстояние до экрана и правильную осанку;
6. не допускать работы на максимальной яркости экрана дисплея;
7. в случае возникновения нештатных ситуаций сохранять спокойствие и чётко следовать указаниям преподавателя.

Запрещается:

1. эксплуатировать неисправную технику;
2. при включённом напряжении сети отключать, подключать кабели, соединяющие различные устройства компьютера;
3. работать с открытыми кожухами устройств компьютера;
4. касаться экрана дисплея, тыльной стороны дисплея, разъёмов, соединительных кабелей, токоведущих частей аппаратуры;
5. касаться автоматов защиты, пускателей, устройств сигнализации;
6. во время работы касаться труб, батарей;
7. самостоятельно устранять неисправность работы клавиатуры;
8. нажимать на клавиши с усилием или допускать резкие удары;
9. пользоваться каким-либо предметом при нажатии на клавиши;
10. передвигать системный блок, дисплей или стол, на котором они стоят;
11. загромождать проходы в кабинете сумками, портфелями, стульями;
12. брать сумки, портфели за рабочее место у компьютера;
13. брать с собой в класс верхнюю одежду и загромождать ею кабинет;
14. быстро передвигаться по кабинету;
15. класть какие-либо предметы на системный блок, дисплей, клавиатуру;
16. работать грязными, влажными руками, во влажной одежде;
17. работать при недостаточном освещении;
18. работать за дисплеем дольше положенного времени.

Запрещается без разрешения преподавателя:

1. включать и выключать компьютер, дисплей и другое оборудование;
2. использовать различные носители информации (дискеты, диски, флешки);
3. подключать кабели, разъёмы и другую аппаратуру к компьютеру;
4. брать со стола преподавателя дискеты, аппаратуру, документацию и другие предметы;
5. пользоваться преподавательским компьютером.

Требования безопасности по окончанию работы:

1. По окончании работы дождаться пока преподаватель подойдёт и проверит состояние оборудования, сдать работу, если она выполнялась;
2. Медленно встать, собрать свои вещи и тихо выйти из класса, чтобы не мешать другим учащимся.

**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).
9. Красноярского колледжа радиоэлектроники и информационных технологий URL: http://www.kraskrit.ru/ (дата обращения: 01.04.2021).

ПРИЛОЖЕНИЕ А

Физическая схема сети первого этажа

(на 1 листе)