Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

ЛАБОРАТОРНЫЙ ПРАКТИКУМ «ОСНОВЫ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ»

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»
профилизации «Информационная безопасность»

Идентификационный номер ВКР: 301

Екатеринбург 2018

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующая кафедрой ИС
_____ Н. С. Толстова
«26» июня 2018 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ЛАБОРАТОРНЫЙ ПРАКТИКУМ «ОСНОВЫ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ»

Исполнитель:
обучающаяся группы № ИБ-401 А. А. Кашапова
Руководитель:
ст. преподаватель С. С. Венков
Нормоконтролер: Т. В. Рыжкова

Екатеринбург 2018

АННОТАЦИЯ

Выпускная квалификационная работа состоит из лабораторного практикума «Основы безопасности компьютерных сетей» и пояснительной записки на 50 страницах, содержащей 18 рисунков, 1 таблицу, 31 источник литературы, а также 1 приложение на 2 страницах.

Ключевые слова: ЛАБОРАТОРНЫЙ ПРАКТИКУМ, ТЕХНОЛОГИИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ.

Кашапова А. А., Лабораторный практикум «Основы безопасности компьютерных сетей»**:** выпускная квалификационная работа / А. А. Кашапова; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2018. — 50 с.

Объектом исследования является процесс обучения студентов в рамках дисциплины «Защита сетевых информационных систем», направление подготовки 44.03.04 «Профессиональное обучение (по отраслям)», профиль подготовки «Информационные технологии».

Предмет исследования — лабораторный практикум «Основы безопасности компьютерных сетей».

Цель работы — разработать электронный лабораторный практикум «Основы безопасности компьютерных сетей».

В соответствии с поставленной целью в работе необходимо решить следующие задачи:

- проанализировать интернет-источники и учебную документацию по теме «Основы безопасности компьютерных сетей»;
- определить содержание лабораторного практикума;
- разработать контент;
- создать лабораторный практикум.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современный мир живет в век информационного общества. Поэтому информация является наиболее ценным объектом. Коммерческие и государственные предприятия заинтересованы в том, чтобы их информация была надежно защищена от ее неправомерного использования: нежелательного разглашения, фальсификации, незаконного тиражирования, блокировки или уничтожения. Злоумышленники часто пытаются взломать сети предприятий, чтобы украсть важные документы, деньги или просто навредить. Чтобы не стать их жертвой, необходимо защищать компьютеры и сеть организации.

Одним из способов защиты является настройка различных технологий безопасности на коммутаторах и маршрутизаторах.

Для настройки коммутаторов и маршрутизаторов требуются специалисты, ознакомленные с технологиями безопасности. Их задача — обезопасить информацию в компании от утечек, потерь, злоумышленников и шпионов.

Технологии осваиваются достаточно сложно. На просторах интернета недостаточно структурированной информации по настройке технологий и настройке технологий с «чистого листа». Новичкам сложно найти подходящую информацию.

В связи с этим становится актуальной проблема разработки лабораторного практикума, которой предназначен для студентов Федерального государственного автономного образовательного учреждения высшего образования «Российский государственный профессионально-педагогический университет» (РГППУ). В лабораторном практикуме содержится как теоретический материал, так и практический с подробной инструкцией подготовки рабочего места к настройке технологии на примере аудитории сетевых технологий РГППУ. Это существенно поможет студентам легко сориентироваться в оборудовании, на котором им предстоит работать.

Объектом исследования является процесс обучения студентов в рамках дисциплины «Защита сетевых информационных систем», направление подготовки 44.03.04 «Профессиональное обучение (по отраслям)», профиль подготовки «Информационные технологии».

Предмет исследования — лабораторный практикум «Основы безопасности компьютерных сетей».

Цель работы — разработать электронный лабораторный практикум «Основы безопасности компьютерных сетей».

В соответствии с поставленной целью в работе необходимо решить следующие задачи:

- проанализировать интернет-источники и учебную документацию по теме «Основы безопасности компьютерных сетей»;
- определить содержание лабораторного практикума;
- разработать контент;
- создать лабораторный практикум.

1 ЛАБОРАТОРНЫЙ ПРАКТИКУМ «ОСНОВЫ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ»

1.1 Анализ литературы и интернет-источников

Проводя анализ литературы и интернет-источников нужно изучить проблему и подробно ознакомиться с областью исследования. Целью анализа источников является выявление достоинств и недостатков, существующих на настоящий момент учебных ресурсов для настройки технологий безопасности в компьютерных сетях.

Анализ литературы и интернет-источников проводится на основании следующих критериев:

- объективность — информация не зависит от чьего-либо мнения, суждения, а также отражает разные точки зрения на проблему;
- достоверность — информация отражает действительное положение текущих дел;
- полнота — информации вполне достаточно для понимания проблемы и дальнейшего принятия решений;
- актуальность — содержательная новизна информации и своевременность: только вовремя полученная информация может быть полезна.

Учебное пособие Смирнова Е. В. «Построение коммутируемых компьютерных сетей» [17]. В книге описаны принципы построения и обслуживания коммутируемых компьютерных сетей, приведено полное описание фундаментальных технологий коммутации. Большой объем практических занятий посвящен самостоятельному конфигурированию, администрированию и мониторингу сетей на примере коммутаторов компании D-Link. Адресовано студентам, обучающимся по направлению «Информатика и вычислительная техника», аспирантам, сетевым администраторам, специалистам предприятий, внедряющим новые информационные технологии. В учебном пособии

представлен в основном теоретический материал, команды по настройке не рассчитаны на подготовку рабочего места к технологии.

На официальном сайте D-Link [10] есть информация по настройке различных технологий, их описание, какие технологии могут поддерживать конкретные коммутаторы, где их можно приобрести и многое другое. Недостаток этого сайта в том, что не всегда можно найти подходящее решение для вашей задачи, он не рассчитан на настройку технологий с «чистого листа».

Веб-сайт [19] «Списки контроля доступа ACL» рассматривает разницу между фильтрацией трафика на входе и выходе интерфейса маршрутизатора, как работают списки доступа и что они из себя представляют, виды и настройка access control list (ACL), работа инвертированных масок показана на примерах. Рассматривается настройка стандартных, расширенных, именованных списков доступа, пример использования списков доступа. Сайт не содержит подробных инструкций по настройке рассматриваемой технологии.

На сайте [24] размещена статья «Что такое ACL и как его настраивать». В этой статье речь идет о списках листов доступа, рассматриваются общие принципы создания ACL, о применении ACL на интерфейсах, о правилах просмотра ACL.

ACL — это набор правил. Каждое правило состоит из действия (permit или deny) и критерия. ACL бывают двух видов: стандартные и расширенные.

Стандартные позволяют отфильтровывать трафик только по одному критерию: адрес отправителя.

Расширенный ACL позволяет фильтровать трафик по большому количеству параметров: адрес отправителя, адрес получателя, transmission control protocol и user datagram protocol (TCP/UDP) порт отправителя, TCP/UDP порт получателя, протоколу, завёрнутому в internet protocol (IP), типу трафика для данного протокола.

Статья [20] описывает суть технологии ACL, что она собой представляет и из чего состоит. Так же настройку ограничения доступа пользователей в

Интернет по media access control (MAC) адресу. Сайт не рассчитан на настройку технологии с нуля.

В статье [25] рассматривают, что такое secure shell (SSH), определение протокола, зачем нужен SSH, как по нему подключиться, подключение по паролю и без, генерация ключей, загрузка публичного ключа на сервер.

SSH — это защищенный сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и передачу файлов. SSH так же необходим для подключения к коммутатору без консольного кабеля. Не все представленные на сайте команды поддерживаются коммутатором D-Link.

На сайте [26] «Что такой SSH» рассказывается о том, что такое SSH, как работает SSH и помогает понять технологии, позволяющие протоколу предоставлять защищенное удаленное управление. Подробно рассматривается каждый из слоёв и типов шифрования, а также значение каждого из них. На сайте нет информации о настройке технологии SSH.

В статье [1] рассказывается о базовой настройке и подключении свитча D-Link desktop ethernet switch (DES)-3200-26, а также как включить SSH и SSL (веб). С этого ресурса понадобилась лишь часть команд. Использование всей информации не подходит для настройки технологии SSH.

На сайте [6] рассказывается, как научиться управлять подключением узлов к портам коммутатора и изучить настройку функции IP-MAC-port binding на коммутаторах D-Link. Функция IP-MAC-port binding (IMPB), реализованная в коммутаторах D-Link, позволяет контролировать доступ компьютеров в сеть на основе их IP- и MAC-адресов, а также порта подключения. На сайте присутствует теоретическая часть, в которой рассказывается, что позволяет функция IP-MAC-port binding, режимы работы функции, использование режимов работы. Практическая часть включает в себя цель работы, необходимое оборудование и команды для настройки работы функции IP-MAC-port binding в режиме address resolution protocol (ARP) с пояснения-

ми. Недостатком является то, что сайт не рассчитан на аудиторию сетевых технологий РГППУ.

Ресурс [7] рассматривает настройку работы функции IP-MAC-port binding в режиме ACL на коммутаторе D–Link DES-3200-28. Так же настройку работы функции IP-MAC-port binding в режиме dynamic host configuration protocol (DHCP) snooping. На сайте пошагово объясняется, как на коммутаторе D–Link DES-3200-28 настроить функцию IP-MAC-port binding и эту же функцию в режиме DHCP snooping. На сайте нет теоретической части, некоторые команды не соответствуют с командами на коммутаторе в РГППУ.

На сайте [23] присутствует только теоретическая часть. В ней рассказывается, что позволяет функция IMPB, раскрывается суть работы данной функции, применение IMPB, режимы работы функции, использование режимов работы. Недостаток — отсутствие практической части.

На сайте [8] говорится о том, что позволяет функция port security, какие режимы работы port security существуют. Дана схема подключения и список команд для настройки управления количеством подключаемых к портам коммутатора пользователей путем ограничения максимального количества изучаемых MAC-адресов и настройки защиты от подключения к портам, основанной на статической таблице MAC-адресов.

Функция port security позволяет настроить какой-либо порт коммутатора так, чтобы доступ к сети через него мог осуществляться только определенными устройствами.

Существует три режима работы функции port security:

- permanent (постоянный) — занесенные в таблицу коммутации MAC-адреса никогда не устаревают, даже если истекло время, установленное таймером aging time, или коммутатор был перезагружен;
- delete on timeout (удалить по истечении времени) — занесенные в таблицу коммутации MAC-адреса устареют после истечения времени, установленного таймером aging time, и будут удалены. Если состояние канала связи на подключенном порте изменяется, MAC-адреса, изученные на нем,

удаляются из таблицы коммутации, что аналогично выполнению действий по истечении времени, установленного таймером aging time;

- delete on reset (удалить при сбросе настроек) — занесенные в таблицу коммутации MAC-адреса будут удалены после перезагрузки коммутатора (этот режим используется по умолчанию).

Недостатком является то, что на сайт не рассчитан на аудиторию РГППУ.

Сайт [30] рассматривает, что такое port security и лишь малую часть команд для настройки функции. Недостатком является не полный список команд для настройки и не все команды подходят для настройки коммутатора DES 3200-10, не рассчитан на аудиторию сетевых технологий РГППУ.

На основании проделанного анализа литературных источников можно сделать вывод, что печатные издания не содержат демонстрации практических работ. Имеющаяся информация в интернет-источниках сложна для понимания, не позволяет полностью отследить ход настройки технологий, так как имеет различное оборудование с аудиторией сетевых технологий в РГППУ и не показывает, как обратить систему к изначальному состоянию.

1.2 Понятие лабораторный практикум

Лабораторный практикум — важная составляющая учебного процесса, в ходе которого обучающиеся сталкиваются с самостоятельной практической деятельностью [28]. Это наиболее важный и эффективный компонент профессиональной и специальной подготовки в технической области. Такие занятия хорошо сочетают элементы теоретического занятия и практической работы. Основными целями лабораторного практикума являются:

- приобретение навыков работы на реальном оборудовании;
- закрепление знаний, полученных на теоретическом занятии;
- приобретение способности к анализу и синтезу, организации и планированию.

В состав лабораторного практикума входят как лабораторные, так и практические работы. Лабораторный практикум проводится в специализированных учебных аудиториях, которые могут быть оснащены оборудованием, с которым бедующему специалисту, возможно, придется столкнуться в реальной жизни.

Эффективность лабораторного практикума в большей степени зависит от:

- оснащения учебной аудитории современным оборудованием;
- выбора объектов изучения;
- содержания лабораторных работ.

К задачам лабораторного практикума относят:

- закрепление полученных теоретических знаний на практике;
- выбор оборудования для выполнения работы;
- обработка и объяснение результатов работы;
- приобретение навыка самостоятельной работы на реальном оборудовании;
- сопоставление теоретических знаний с результатами работы.

1.3 Обзор оборудования D-Link

В настоящее время одним из всемирно известных разработчиков и производителей сетевого и телекоммуникационного оборудования является компания D-Link. Она предлагает широкий набор решений для домашних пользователей, корпоративного сегмента, провайдеров интернет-услуг. Также компания предоставляет решения для учебных заведений. В частности, образовательным учреждением «Российский государственный профессионально-педагогический университет» было закуплено соответствующее оборудование для выполнения лабораторных работ. Комплект состоит из одного коммутатора третьего уровня D-Link DES-3810-28, десяти управляемых коммутаторов второго уровня D-Link DES-3200-10.

Рассмотрим подробнее оборудование лабораторного стенда.

Коммутаторы третьего уровня серии DES-3810 [12], входящие в семейство D-Link xStack, обеспечивают высокую производительность, широкие функциональные возможности, в том числе и уровня 3. Коммутаторы оснащены 24 и 48 портами. Коммутатор DES-3810-28 оснащен 24 портами 10/100 Мбит/с Fast Ethernet и 4 комбо-портами 1000 Base-T/SFP Gigabit Ethernet. Порты Fast Ethernet обеспечивают подключение к другим коммутаторам локальной сети. Комбо-порты обеспечивают гибкое подключение к магистрали сети и центральным коммутаторам.

Коммутаторы серии DES-3810 поддерживают две различные версии программного обеспечения — стандартную версию (SI) и расширенную версию (EI). Стандартная версия поддерживает усовершенствованные функции для построения сетей масштаба кампуса или предприятия, включая расширенные настройки quality of service (QoS), ограничение трафика, туннелирование 802.1Q, маршрутизацию многоадресную рассылку IPv4 и различные функции безопасности. Расширенная версия программного обеспечения поддерживает маршрутизацию IPv6, протокол border gateway protocol (BGP) и протокол multi protocol label switching (MPLS), применяемые в сетях нового поколения с поддержкой IPv6 в сетях Metro Ethernet. Помимо этого, расширенная версия также поддерживает switch resource management (SRM). Эта функция предоставляет пользователям возможность оптимизировать распределение ресурсов коммутатора для решения различных сетевых задач.

Данные коммутаторы серии DES-3810 предназначены для сетей предприятий, а также для пользователей, которым требуется высокий уровень сетевой безопасности и максимальная надежность. Коммутатор DES-3810-28 поддерживает подключение внешнего резервного источника питания, обеспечивая, таким образом, непрерывную работоспособность. Коммутатор также поддерживает функции 802.1D spanning tree (STP), 802.1w rapid spanning tree (RSTP) и 802.1s multiple spanning tree (MSTP), loopback detection (LBD) и контроль широковещательного шторма, которые увеличивают отказоустой-

чивость сети. Для обеспечения распределения нагрузки и резервного копирования данных при использовании нескольких коммутаторов/приложения сервера, серия DES-3810 поддерживает функцию dynamic 802.3ad link aggregation port trunking [12].

Коммутаторы DES-3200 [11] входят в линейку управляемых коммутаторов D-Link 2 уровня серии xStack, предназначенную для сетей Metro Ethernet (ETTX и FTTX) и корпоративных сетей. Коммутаторы оснащены 8/16/24/48 портами 10/100 Мбит/с Fast Ethernet, а также 2/4 комбо-портами Gigabit Ethernet/SFP у аппаратной ревизии A1 или 1 портом 100/1000 SFP + 1 комбо-портом Gigabit Ethernet/SFP / 2 порта 100/1000 SFP + 2 комбо-порта Gigabit Ethernet/SFP у аппаратных ревизий B1 и C1. Коммутаторы DES-3200-10/18 выполнены в корпусе шириной 9 дюймов и оснащены пассивной системой охлаждения, подходящей как для настольного использования, так и для установки в телекоммуникационных и распределительных шкафах.

Коммутаторы серии DES-3200 поддерживают управление доступом 802.1x на основе порта/хоста, гостевой VLAN. Функция IMPB обеспечивает привязку IP-адреса и MAC-адреса пользователя к определенному номеру порта на коммутаторе, запрещая тем самым пользователю самостоятельно менять сетевые настройки. Более того, благодаря функции DHCP snooping коммутатор автоматически определяет пары IP/MAC-адресов, выданных сервером, отслеживая DHCP-пакеты и сохраняя их в «белом» списке IMPB. Эти функции играют важную роль в поддержке безопасности сети. Встроенная функция D-Link safeguard engine обеспечивает идентификацию и приоритизацию пакетов, предназначенных для обработки непосредственно процессором коммутатора, с целью предотвращения намеренных атак и нейтрализации воздействия паразитного трафика на CPU коммутатора. Помимо этого, DES-3200 поддерживает списки управления доступом (ACL). Данный функционал предоставляет администраторам возможность ограничить доступ к

сетевым сервисам и не оказывает влияния на производительность коммутатора [11].

В лабораторных работах для подключения к коммутаторам понадобятся консольные кабели и кабели Ethernet. Рассмотрим их подробнее.

Консольный кабель используется для соединения компьютера и коммутатора (маршрутизатора, роутера, модема) через консольный порт. При подключении к консольному порту коммутатора терминала или компьютера с установленной программой эмуляции терминала осуществляется доступ к интерфейсу командной строки коммутатора. Этот метод доступа наиболее удобен при первоначальном подключении к коммутатору, когда значение IP-адреса неизвестно или не установлено, в случае необходимости восстановления пароля и при выполнении расширенных настроек коммутатора [9].

В лабораторном стенде РГППУ используется UTP кабель Ethernet для технологии 100Base-TX. Он наиболее актуален для небольших локальных сетей. Пропускная способность такой сети равняется 100 Мбит/с. Пропускной способностью называется скорость передачи данных по линии связи. Единица измерения пропускной способности сети — бит в секунду. В качестве среды передачи данных используется витая пара — наиболее распространенная среда передачи данных для локальных сетей. Витая пара — вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных между собой, покрытых пластиковой оболочкой [5]. Используется неэкранированная (кабель не имеет защитного экрана) витая пара пятой категории. Экранирование обеспечивает лучшую защиту от внешних и внутренних электромагнитных наводок. Категории определяют эффективный пропускаемый частотный диапазон. Чем выше категория кабеля, тем больше пар проводников содержит каждая пара и тем больше витков на единицу длины.

Для того чтобы кабель можно было подключить к нужным устройствам кабели обжимают. От качества его обжатия, напрямую зависит, насколько хорошей будет скорость соединения и сама работа устройства. Для обжима

кабеля используются коннекторы. Для витой пары пятой категории используют коннекторы типа RJ-45 (24AWG). В его разъеме 8 позиций, в которые вставляется 8 проводников [21].

Рассмотренное оборудование хорошо подходит для обучения студентов. Оборудование поддерживает основные технологии безопасности компьютерных сетей.

1.4 Основные технологии безопасности в компьютерных сетях

Коммутаторы D-Link серии DES-3200-10 поддерживают такие функции обеспечения безопасности и ограничения доступа к сети, как secure shell (SSH), access control list (ACL), IP-MAC-port binding, функция port security [17].

Безопасная оболочка (SSH) — это защищенный сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и передачу файлов. SSH так же необходим для подключения к коммутатору без консольного кабеля. Иными словами, SSH — это дистанционная командная строка. Визуально вы работаете на своем компьютере, но в реальности — на другом компьютере или коммутаторе.

Протокол — это набор соглашений, правил, по которым разные программы могут обмениваться информацией. SSH — это набор правил, который известен и вашему компьютеру, и физически отдаленному компьютеру.

Возможность подключиться к коммутатору через консольный кабель есть не всегда. С помощью SSH можно находиться на большом расстоянии от коммутатора и настроить на нем необходимые технологии. Ключевая особенность заключается в том, что SSH шифрует трафик, делая подключения безопасными.

Для работы по SSH нужен SSH-сервер и SSH-клиент. Сервер прослушивает соединения от клиентских машин и при установлении связи производит аутентификацию, после чего начинает обслуживание клиента. Клиент

используется для входа на удаленную машину и выполнения команд. SSH-клиенты и SSH-серверы имеются для большинства сетевых операционных систем. Пользователи Windows могут воспользоваться SSH-клиентом вроде PuTTY. Вы можете выполнять команды также, как если бы вы напрямую подключились к коммутатору.

В SSH существует три метода аутентификации клиентов:

- host-based аутентификация;
- парольная аутентификация;
- аутентификация с помощью открытых ключей.

Благодаря host-based аутентификации, можно сделать так чтобы пользователи одного хоста заходили на другой хост без пароля, на котором включена данная функция. Такой вид аутентификации может быть полезен в средах с одним доверенным хостом (trusted) и несколькими хостами, к которым осуществляется доступ с него (untrusted). В этом случае на хосты, к которым осуществляется доступ, пароли не передаются. Этот метод является потенциально небезопасным, рекомендуется не использовать его. Для повышения уровня своей безопасности метод может быть дополнен RSA-аутентификацией клиентского хоста.

Аутентификация с помощью пароля. По сети пароль передается в зашифрованном виде. Это усложняет возможность его кражи путем перехвата сетевого трафика. Пароль не хранится на машине клиента, а использование пустого пароля запрещено по умолчанию. Как правило, сервер предоставляет ограниченное число попыток ввода пароля, что делает неэффективным использование грубой атаки путём подбора с помощью словаря.

Однако зашифрованная передача данных не защищает от слабых паролей. Сложность пароля полностью зависит от пользователя. Слишком простой пароль легко подобрать методами социальной инженерии, а слишком сложный пользователь может забыть. К тому же, парольный доступ не позволяет серверу абсолютно точно идентифицировать клиента. Поскольку использование пароля не может обеспечить абсолютной безопасности клиента,

при подключении по SSH надёжнее использовать аутентификацию клиента с помощью ключа.

Аутентификация по SSH с помощью ключа гораздо безопаснее парольной аутентификации, так как обеспечивает более надёжную проверку подлинности пользователя. При аутентификации используются два ключа: публичный и приватный. Публичный ключ хранится на сервере и представляет собой цифровой «замок», который можно открыть только с помощью ключа, который находится у клиента. Если кто-либо захочет получить доступ к данным на сервере, ему сначала придётся завладеть цифровым ключом пользователя. Даже если злоумышленник попытается выступить посредником между сервером и клиентом, пользователь получит сообщение о том, что данные хоста были изменены и передача ключа по этому соединению небезопасна.

Главное правило обеспечения безопасности — секретный ключ действительно должен быть секретным, как со стороны пользователя, так и со стороны сервера. Если кто-то завладеет файлом приватного ключа, то легко сможет получить доступ к серверу.

Приватный ключ дополнительно можно защитить паролем. Это сильно усложнит попытку взлома, т.к. придётся не только завладеть парой уникальных ключей, но и подобрать к ним пароль. Один приватный ключ пользователь может использовать для подключения сразу к нескольким серверам. В таком случае на ряд серверов устанавливается один и тот же публичный ключ. Таким образом, клиенту нет необходимости использовать разные ключи к разным серверам или запоминать множество паролей, если используется парольный доступ. Самым безопасным способом аутентификации в SSH, является аутентификация с помощью ключа, при этом защищенный паролем.

Списки управления доступом (ACL) — это мощное средство фильтрации потоков данных без потери производительности, т.к. проверка содержимого пакетов выполняется на аппаратном уровне. Фильтруя потоки данных, администратор может ограничить типы приложений, разрешенных для использования в сети, контролировать доступ пользователей к сети и опреде-

лять устройства, к которым они могут подключаться. ACL представляют собой последовательность условий проверки параметров пакетов данных. При поступлении сообщений на входной порт, коммутатор проверяет параметры пакетов данных на совпадение с критериями фильтрации, определенными в ACL, и выполняет над пакетами одно из действий: permit (разрешить) или deny (запретить).

Списки управления доступом состоят из профилей доступа и правил. Профили доступа определяют типы критериев фильтрации, которые должны проверяться в пакете данных, а в правилах непосредственно указываются значения их параметров. Каждый профиль может состоять из множества правил.

Когда коммутатор получает кадр, он проверяет его поля на совпадение с типами критериев фильтрации и их параметрами, заданными в профилях и правилах. Последовательность, в которой коммутатор проверяет кадр на совпадение с параметрами фильтрации, определяется порядковым номером профиля и порядковым номером правила. Профили доступа и правила внутри них работают последовательно, в порядке возрастания их номеров. Т.е. кадр проверяется на соответствие, условиям фильтрации, начиная с первого профиля и первого правила в нем. Если ни одно из правил текущего профиля не совпало с параметрами кадра, то коммутатор продолжит проверку на совпадение параметров кадра с условиями первого правила и следующего профиля. При первом совпадении параметров кадра с правилом к кадру будет применено одно из действий, определенных в правиле: «Запретить», «Разрешить» или «Изменить содержимое поля пакета». Дальше кадр проверяться не будет. Если ни одно из правил не подходит, применяется политика по умолчанию, разрешающая прохождение всего трафика.

Функция port security позволяет настроить какой-либо порт коммутатора так, чтобы доступ к сети через него мог осуществляться только определенными устройствами. Устройства, которым разрешено подключаться к порту, определяются по MAC-адресам. Помимо этого, функция port security

позволяет ограничивать количество изучаемых портом MAC-адресов, тем самым ограничивая количество подключаемых к нему узлов.

Существует три режима работы функции port security:

- permanent (постоянный) — занесенные в таблицу коммутации MAC-адреса никогда не устаревают, даже если истекло время, установленное таймером FDB aging time, или коммутатор был перезагружен;
- delete on timeout (удалить по истечении времени) — занесенные в таблицу коммутации MAC-адреса устареют после истечения времени, установленного таймером FDB aging time, и будут удалены. Если состояние канала связи на подключенном порте изменяется, MAC-адреса, изученные на нем, удаляются из таблицы коммутации, что аналогично выполнению действий при истечении времени, установленного таймером FDB aging time;
- delete on reset (удалить при сбросе настроек) — занесенные в таблицу коммутации MAC-адреса будут удалены после перезагрузки коммутатора. При подключении неавторизованного пользователя к порту коммутатора он будет заблокирован, а коммутатор отправит сообщение SNMP trap или создаст запись в log-файле, если администратор настроил выполнение этих действий. Порт коммутатора будет отбрасывать трафик, поступающий с неизвестного MAC-адреса.

Функция IP-MAC-port binding (IMPB), реализованная в коммутаторах D-Link, позволяет контролировать доступ компьютеров в сеть на основе их IP- и MAC-адресов, а также порта подключения. Администратор может создать записи «белый лист», связывающие MAC- и IP-адреса компьютеров с портами подключения коммутатора. На основе этих записей, в случае совпадения всех составляющих, клиенты будут получать доступ к сети. В том случае, если при подключении клиента, связка MAC-IP-порт будет отличаться от параметров заранее сконфигурированной записи, коммутатор заблокирует MAC-адрес соответствующего узла с занесением его в «черный лист».

Функция IP-MAC-port binding включает три режима работы: ARP mode (по умолчанию), ACL mode и DHCP Snooping mode.

ARP mode является режимом, используемым по умолчанию при настройке функции IP-MAC-port binding на портах. При работе в режиме ARP коммутатор анализирует ARP-пакеты и сопоставляет параметры IP-MAC ARP-пакета с предустановленной администратором связкой IP-MAC. Если хотя бы один параметр не совпадает, то MAC-адрес узла будет занесен в таблицу коммутации с отметкой «Drop» («Отбрасывать»). Если все параметры совпадают, MAC-адрес узла будет занесен в таблицу коммутации с отметкой «Allow» («Разрешен»).

При функционировании в ACL mode коммутатор на основе предустановленного администратором «белого листа» IMPB создает правила ACL. Любой пакет, связка IP-MAC которого отсутствует в «белом листе», будет блокироваться ACL.

Режим DHCP snooping используется коммутатором для динамического создания записей IP-MAC на основе анализа DHCP-пакетов и привязки их к портам с включенной функцией IMPB. Таким образом, коммутатор автоматически создает "белый лист" IMPB в таблице коммутации или аппаратной таблице ACL (если режим ACL включен). При этом для обеспечения корректной работы сервер DHCP должен быть подключен к доверенному порту с выключенной функцией IMPB. Администратор может ограничить максимальное количество создаваемых в процессе автоизучения записей IP-MAC на порт, т.е. ограничить для каждого порта с активизированной функцией IMPB количество узлов, которые могут получить IP-адрес с DHCP-сервера. При работе в режиме DHCP snooping коммутатор не будет создавать записи IP-MAC для узлов с IP-адресом, установленным вручную.

При активизации функции IMPB на порте администратор должен указать режим его работы:

- strict mode — в этом режиме порт по умолчанию заблокирован;
- loose mode — в этом режиме порт по умолчанию открыт.

1.5 Анализ рабочей программы

Лабораторный практикум может применяться в рамках дисциплины «Защита сетевых информационных сетей». Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы 44.03.04 Профессиональное обучение (по отраслям), профиль подготовки «Информационные технологии» и дисциплиной вариативной части учебного плана [15].

Дисциплина направлена на формирование следующих компетенций:

- ОК-7 (способность использовать базовые правовые знания в различных сферах деятельности);
- ПК-19 (готовность к проектированию комплекса учебно-профессиональных целей, задач);
- ПСК-2 (способность применять современные технологии разработки микропроцессорных и информационных систем);
- ПСК-6 (способность использовать системы, инструментальные программные и аппаратные средства для изучения организации человеко-машинных интерфейсов).

В результате освоения дисциплины обучающийся должен:

знать:

- теорию информационной безопасности, методологию защиты информации;
- правовое обеспечение информационной безопасности, законодательную базу, систему государственного контроля и управления в области информационной безопасности;
- организационное обеспечение информационной безопасности;
- основные программные средства защиты информации;
- технические средства защиты информации;
- криптографические методы и средства обеспечения информационной безопасности;

уметь:

- проводить анализ для развертывания комплексной защиты информации;
- определять тип атаки и средство её нейтрализации;
- использовать стандартные программные средства по обеспечению безопасности системы;

владеть:

- базовой терминологией;
- базовыми средствами защиты информации.

Тематический план дисциплины включает в себя следующие разделы и темы (таблица 1):

Таблица 1 — Тематический план дисциплины

Наименование разделов и тем дисциплины (модуля)	Сем.	Всего, час.	Вид контактной работы, час.			СРС
			Лекции	Практ. занятия	Лаб. работы	
1. Основные цели и задачи курса	6	42	5	-	13	24
2. Классификация атак и угроз.	6	43	6	-	13	24
3. Программные средства защиты информации	6	41	5	-	12	24
4. Криптографические средства защиты	7	43	6	-	13	24
5. Организационно-правовые методы защиты информации	7	41	5	-	12	24
6. Методология построения комплексной системы защиты	7	42	5	-	13	24

Лабораторный практикум может применяться в разделе «Программные средства защиты информации». Содержание раздела включает:

Обзор компонентов для централизованного управления подсистемой защиты, обеспечивающих деятельность администраторов подсистемы защиты информации в составе: систем защиты СУБД, систем аутентификации,

систем сетевой безопасности, программно-технических средств защиты, биометрических средств защиты.

Применение лабораторного практикума целесообразно в теме «Системы сетевой безопасности». Изучение всех модулей рассчитано на 3 часа самостоятельной и 6 часов аудиторной работы. Лабораторные работы и контрольные задания выполняются в аудитории. Прохождение теоретической части и выполнение тестов целесообразно проходить самостоятельно, в силу ограниченности аудиторного времени.

В результате анализа рабочей программы, можно прийти к выводу, что созданный лабораторный практикум вполне может применяться в образовательном процессе РГППУ.

2 ОПИСАНИЕ ЛАБОРАТОРНОГО ПРАКТИКУМА

2.1 Педагогический адрес

Данный лабораторный практикум может изучаться в рамках дисциплины «Защита сетевых информационных систем», направление подготовки 44.03.04 «Профессиональное обучение (по отраслям)», профиль подготовки «Информационные технологии».

А также в рамках дополнительной программы кафедры информационных систем для более углубленного изучения технологий безопасности компьютерных сетей.

Знания и умения необходимые студентам для освоения лабораторного практикума:

- знать IPv4 и уметь его настраивать на ОС Windows;
- знать технологию Fast Ethernet;
- уметь работать со средами виртуализации Hyper-V, VMware Player;
- уметь работать в Брандмауэре Windows.

2.2 Структура лабораторного практикума

В качестве среды реализации лабораторного практикума была выбрана модульная объектно-ориентированная динамическая учебная среда (Moodle). Moodle — это свободная система управления обучением, ориентированная прежде всего на организацию взаимодействия между преподавателем и учениками, подходит для организации традиционных дистанционных курсов, а также для поддержки очного обучения.

Главным преимуществом системы является то, что она распространяется бесплатно. Moodle дает возможность проектировать, создавать и в дальнейшем управлять ресурсами информационно-образовательной среды. Си-

стема имеет удобный и понятный интерфейс, он изначально был создан для преподавателей, не обладающих глубокими знаниями в области программирования и администрирования сайтов. Используя только справочную систему, преподаватель самостоятельно может создать электронный курс и управлять его работой. Система поддерживает обмен файлами любых форматов, как между преподавателем и студентом, так и между самими студентами [14]. Преподаватели могут управлять крайним сроком сдачи работ. Количество обучаемых в системе неограниченно. Moodle имеет встроенные составляющие для курсов: «чат», «опрос», «форум», «глоссарий», «рабочая тетрадь», «урок», «тест», «анкета», «семинар», «ресурс», «задание» и другие. Это создает все необходимые условия для преподавательской деятельности.

На сегодняшний день, Moodle является самой распространенной системой дистанционного образования во всем мире и установлена более, чем в 54 тысячах учебных заведений и компаний в 212 странах. В том числе Moodle используется федеральным государственным автономным образовательным учреждением высшего образования РГППУ. В РГППУ существует институт непрерывного образования (ИНО), в состав которого входят: факультет повышения квалификации, центр дистанционных образовательных технологий и центр веб-технологий и программирования [13]. На данный момент институтом непрерывного образования реализуется около 70 дополнительных образовательных программ.

Средой реализации лабораторного практикума послужила учебная версия Moodle РГППУ [22]. Преимуществом использования является удобство применения, как студентами, так и преподавателями. У студентов появляется возможность изучать теоретический материал и выполнять тесты по пройдённому материалу дома. Это позволит выделить больше времени на выполнение лабораторных работ, а также очень удобно для тех, кто не присутствовал на занятии. Подготовка к занятию осуществляется дома в любое свободное время, а выполнение лабораторных работ осуществляется уже в аудитории на предоставленном оборудовании. Преподаватель может сразу отсле-

живать и оценивать выполнение заданий. Студентам нет необходимости искать информацию на разных источниках, все находится в одном месте, структурированно по модулям, задания размещены в последовательности выполнения, даны инструкции к выполнению заданий. Если преподаватель добавит какой-либо модуль или элемент студентам он будет сразу доступен. При возникновении вопросов можно задать его преподавателю с помощью обратной связи. Преподаватель может контролировать, как усвоен материал с помощью тестов созданных элементами Moodle, он автоматически посчитает количество баллов, набранных студентом. В любое время можно добавить, удалить или поменять какой-либо элемент курса. Так же можно отвечать на вопросы студентов, создавать групповые конференции и обсуждать там непонятные вопросы. При расположении всех заданий в Moodle нет необходимости в том, чтобы распространять учебный материал каждому студенту поотдельности, все находится в одном месте и всегда доступно. В лабораторном практикуме предусматривается возможность выставления баллов студентам за выполнение каждого элемента.

Перед изучением лабораторного практикума студентам дана инструкция по работе с лабораторным практикумом, а также описывается для кого он предназначен, сколько модулей в практикуме и из чего они состоят, что необходимо знать и уметь перед изучением модулей, а также перечислено оборудование, которое понадобится для выполнения лабораторных работ.

Лабораторный практикум разделен на модули, в каждом из которых есть свой набор материалов. В состав лабораторного практикума входят четыре модуля (рисунок 1):

- secure shell;
- access control list;
- IP-MAC-port binding;
- port security.

Каждый модуль состоит из:

1) теоретической части (представлена видео файлом);

2) теста по теории;

3) подготовки к выполнению лабораторной работы (представлена видео файлом);

4) настройки технологии (представлена видео файлом);

5) контрольных заданий по теме;

6) теста по лабораторной работе.

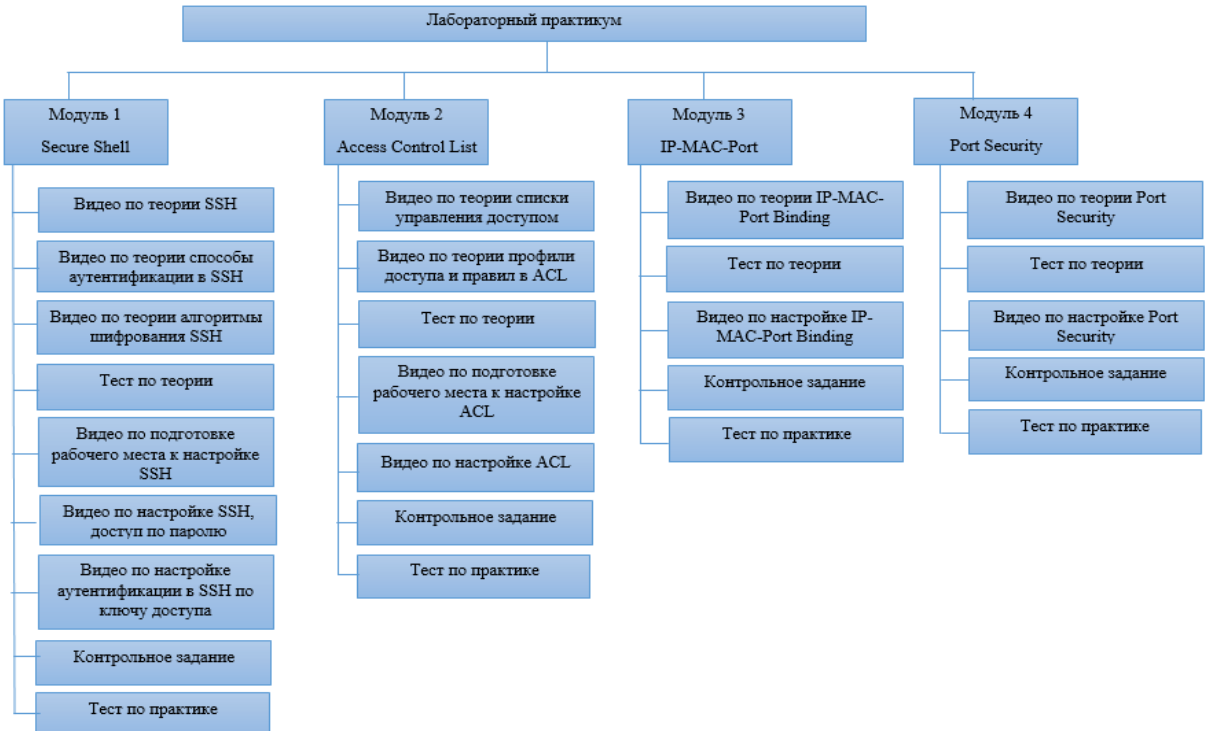

Рисунок 1 — Схема лабораторного практикума

Теоретический материал представлен в качестве коротких видеороликов. Данная технология была выбрана в связи с тем, что она привычна для большинства современных студентов они привыкли к просмотру видео в интернете, поэтому формат подачи информации в видеороликах им близок и понятен. Видео намного информативнее текста — можно не только описать, но еще и наглядно продемонстрировать этапы работы. Анимационное обучающее видео — это хорошее средство эффективно донести информацию в легкой и запоминающейся форме. Главная цель такого видео — обучить, объяснить, показать. Информация в видео представлена коротко и понятно, что сокращает время работы и повышает качество усвоения учебного материала.

При выборе средства для создания видеороликов были рассмотрены сервисы: GoAnimate, PowToon, Animaker.

Сервис для создания анимированных презентаций GoAnimate [31]. Он помогает превратить презентацию в полноценный мультипликационный фильм. С его помощью можно создать сюжетный рассказ или историю, которая будет происходить с героем. В программе есть множество анимированных персонажей. Вы можете сами задавать их поведение и действия. Для этого нужно использовать готовые шаблоны: герой может прыгать, бегать, говорить. Вы можете добавлять различные сцены из шаблонов или же использовать свои фотографии, текст, аудио, музыку, записать голос. Интерфейс достаточно простой, а для каждого действия есть подсказки. Для начала работы нужна регистрация. Готовый ролик можно встроить на сайт, скачать в высоком разрешении или опубликовать в социальных сетях.

Преимущество сервиса большая коллекция действий, с помощью которых можно оживить персонажей. Человечки хлопают глазами, танцуют, готовят пироги, оказывают медицинскую помощь и произносят любой текст, в том числе на русском языке.

Минус в том, что сервис англоязычный, но поддерживает ввод текста на русском языке. Базовая подписка стоит 39 долларов в месяц. За такую сумму можно делать неограниченное количество видео в разрешении 720 пикселей, однако в кадре останется водяной знак сервиса. Профессиональный и групповой тарифы составляют 79 и 250 долларов в месяц соответственно. В течение 14 дней сервисом можно пользоваться бесплатно.

Следующий сервис PowToon [29]. Он во многом похож на GoAnimate. Для создания анимированных видео используются слайды и готовые шаблоны. В отличие от GoAnimate интерфейс скорее напоминает приложения для создания презентаций — только с расширенным функционалом. Для начала работы нужна регистрация.

Рабочая область сервиса содержит кнопки управления, окно предварительного просмотра, список слайдов и переключатель выбора элементов.

Также этот сервис предлагает другие полезные ресурсы: музыку, анимированные таблицы и графики. Готовые ролики можно скачать в формате MP4 или загрузить на YouTube. Также есть возможность экспортировать контент в PDF и PPT.

В PowToon есть два режима: для создания анимированных презентаций и для создания самых разных клипов, например, маркетинговых видео или видео для лекций. Программа проста в использовании.

Бесплатная версия ставит на видео водяной знак и ограничивает длительность ролика 5 минутами. Платные тарифы, от 19 долларов в месяц при оплате за год, дают много преимуществ — снимают ограничения на объем ролика, использование библиотек и функционал экспорта.

К преимуществам определенно стоит отнести мгновенный доступ к просмотру ваших слайдов, интуитивный интерфейс и относительно недорогую подписку. Также огромное количество разнообразных готовых решений.

К недостаткам можно отнести не слишком большие возможности в анимации элементов и скудную библиотеку персонажей. На базовых тарифах количество персонажей и готовых визуальных элементов значительно меньше, чем у GoAnimate.

Ещё один простой сервис для создания анимированных роликов Animaker [27]. В нем более 40 шаблонов — готовых видео с эффектами, переходами и музыкой. Сервис создаёт с нуля горизонтальные и вертикальные видео, а также ролики специально для «Историй» в Инстаграме. Доступные шаблоны подойдут для любых индустрий: образование, путешествия, бизнес, здоровье, еда, спорт и многих других. С помощью Animaker можно создавать 2D и 3D анимацию, инфографику и видеоинфографику. Он не только позволяет перетаскивать элементы для создания анимации, но и обладает обширной библиотекой анимированных элементов. Каждый такой элемент имеет свой визуальный эффект и встроенные возможности движения, что дает возможность создавать качественную анимацию без предварительного обучения и опыта. К презентации легко добавить музыку или голосовую дорожку. Го-

товые видео из сервиса можно напрямую экспортировать в YouTube и Facebook или скачать. Для начала работы нужна регистрация.

К преимуществам сервиса относится наличие русскоязычной версии. У Animaker есть бесплатная версия с ограниченным функционалом. С его помощью можно создавать безлимитное количество роликов продолжительностью до двух минут в SD качестве, количество экспорта видео составляет 5 роликов в месяц. Данного функционала вполне хватает для создания небольших симпатичных роликов. Более широкие права можно получить за 19 долларов в месяц.

Для создания видеороликов был выбран сайт animaker.com [27]. Он отлично подходит для создания анимированных видеороликов. По сравнению с другими сервисами у Animaker более удобный интерфейс, дешевле тарифные планы и интереснее графика.

Бесплатное использование ресурсов накладывает определенные ограничения на создание виде роликов, а именно: ограничение по времени, которое составляет две минуты; ограничение на экспорт видео, которое составляет пять роликов в месяц. В связи с этим для соединения нескольких видеороликов в один и записи видеороликов использовалась программа Camtasia Studio. Данная программа была использована в двух видеороликах по теоретической части.

Camtasia Studio — одна из самых популярных программ для захвата изображения с экрана. Несмотря на то, что программа только частично на русском языке, она обладает понятным интерфейсом. В программе содержится подробная документация, поэтому легко можно найти помощь при проблеме. Весь процесс создания видео разделен на три этапа: запись, редактирование и сохранение видео в нужном формате.

В теоретической части модулей в общем содержится 7 видеороликов, продолжительностью от 1 до 4 минут. Видеоролики занимают от 1 – 6 Мб. В них содержится информация о назначении изучаемой технологии, ее использование, какие возможности предоставляет и режимы работы. При создании

видеороликов были использованы различные переходы, анимации и объекты, задействованы разные персонажи.

Видеоролики содержат в себе теоретический материал, который представляется с помощью различных слайдов, переходов, объектов, а также персонажей (рисунок 2). Персонажи выражают только позитивные эмоции, их деловой стиль создает рабочую атмосферу.

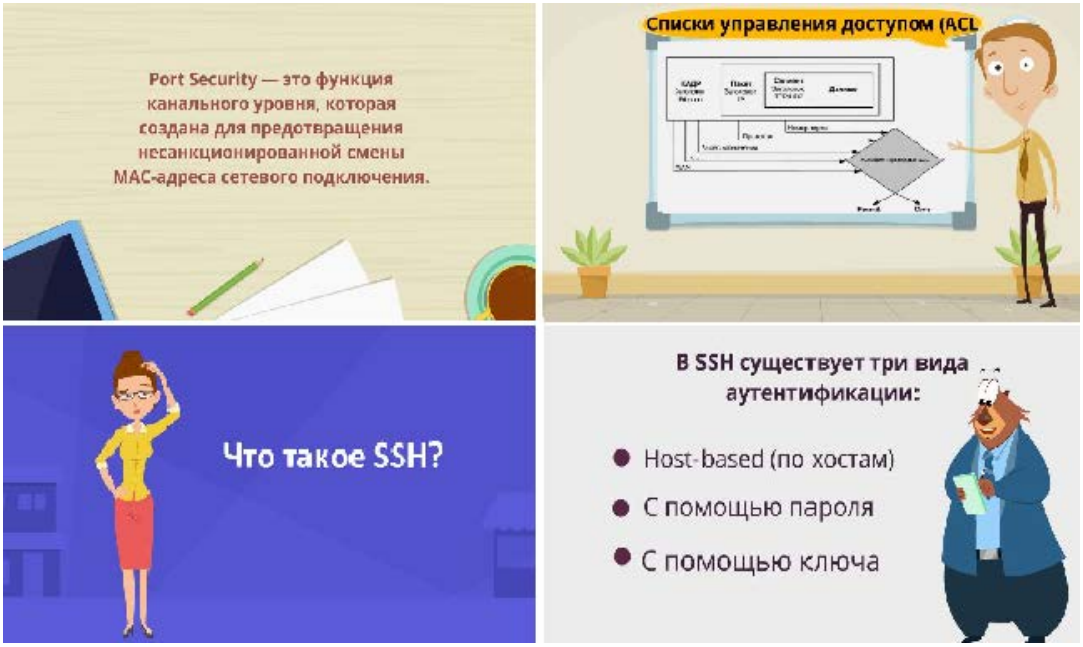

Рисунок 2 — Содержание теоретических видеороликов

При выборе фона учитывалось психофизиологическое воздействие цветов на человека. Глазу приятнее, если используется нечетное количество цветов — 3 или 5. Использование более 7 цветов одновременно не рекомендуется, так как это может утомить обучающегося, а один цвет выглядит скучно [2]. Подвижность показываемых кадров способствует усилению внимания, вызывает интерес и делает разнообразным процесс передачи информации. Поэтому в видеороликах были применены различные переходы и анимации. При выборе музыки для видеороликов учитывалось воздействие на эмоции человека. Прослушивание фоновой музыки оказывает воздействие на людей множеством способов: способствует концентрации внимания и запоминанию материала, избавляет от стресса, повышает силу и выносливость,

повышает иммунитет и другое. Была применена фоновая музыка, задающая темп к прочтению материала и обучению.

Видеоролики размещены в Moodle с помощью элемента «Задание», которое позволяет преподавателям добавлять коммуникативные задания, собирать студенческие работы, оценивать их и предоставлять отзывы. Видеоролик открывается в новой вкладке.

Для закрепления и проверки знаний по теоретическому материалу были разработаны тестовые задания по изученной теме. Тестирование в педагогике выполняет три основные взаимосвязанные функции [3]: диагностическую, обучающую и воспитательную. Диагностическая функция заключается в выявлении уровня знаний, умений, навыков обучающегося. Обучающая функция тестирования состоит в мотивировании обучающегося к активизации работы по усвоению учебного материала. Воспитательная функция проявляется в периодичности и неизбежности тестового контроля.

Тесты созданы с помощью элемента курса «Тест», который позволяет преподавателю создавать тесты, состоящие из вопросов разных типов: множественный выбор, верно/неверно, на соответствие, короткий ответ, числовой. Перед выполнением теста содержится небольшая инструкция с описанием критерия оценивания. Тест содержит в себе 10 вопросов закрытой формы с выбором одного или нескольких правильных ответов. Тестовое задание закрытой формы подразумевает тестовое задание, где есть готовые ответы, из которых тестируемый должен выбрать [4]. Под тестовым заданием с выбором одного правильного ответа понимают тестовые задание закрытой формы, в котором среди предложенных ответов лишь один правильный. Тестовое задание с выбором нескольких правильных ответов подразумевает задания в которых допускается выбор нескольких правильных ответов из числа предложений. Количество вопросов в тесте определялось некоторыми общими принципами отбора содержания теста [18]. По принципу репрезентативности была обеспечена оптимальная полнота и правильность пропорций содержания теста. По принципу значимости в тест были включены наиболее значи-

мые элементы содержания, относящиеся к опорным понятиям. Придерживать этим принципам в тестах было определенно оптимальное количество вопросов равное десяти. Такое количество вопросов не перегружает обучающегося и включает в себя основные знания для усвоения материала.

Подготовка к выполнению лабораторных работ так же представлена в виде видеороликов продолжительностью не более четырех минут, занимающих около 8 Мб. В них рассматривается оборудование, которое понадобится для выполнения лабораторных работ и подробно описывается инструкция предварительной настройки перед изучением технологии. При создании видеороликов анимации, музыка, переходы и персонажи применялись по тому же принципу, что и при создании теоретического материала. Дополнительно к ним были добавлены фотографии оборудования и действий при его настройке. Фон на протяжении всего видео использовался одного цвета, чтобы внимание обучающихся было сосредоточено только на самом процессе настройке. Видеоролики расположены в Moodle при помощи элемента «Задание». В начале каждого видеоролика представлены цели и задачи, которые они выполняют. Если обучающийся с первого раза не запомнил или не понял, как выполняется то или иное действие видеоролики предусматривают возвращение к началу этого шага и выполнение его заново (рисунок 3).

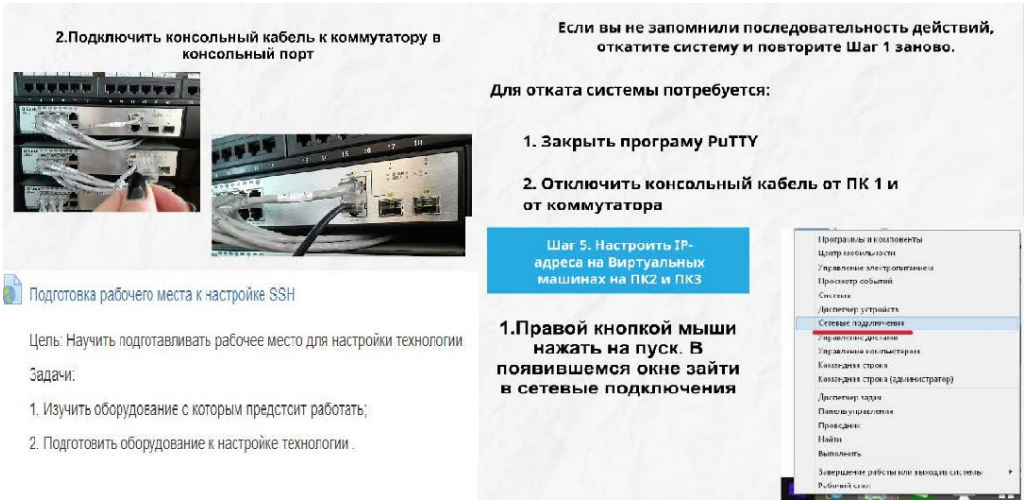

Рисунок 3 — Содержание видеороликов по подготовке к выполнению лабораторных работ

Настройка технологий безопасности также представлена посредством видеороликов. Положительность, которых составляет от 1 – 2 минут, занимающих от 2 – 7 Мб. В них дана пошаговая инструкция по настройке технологий, которая сопровождается соответствующими иллюстрациями. Расположен в Moodle элементом «Задание». Для оценки выполнения лабораторных работ студенты отправляют преподавателю заполненный файл-отчет, прикрепленный совместно с видеороликом. Перед просмотром видеороликов поставлены цели и задачи (рисунок 4).

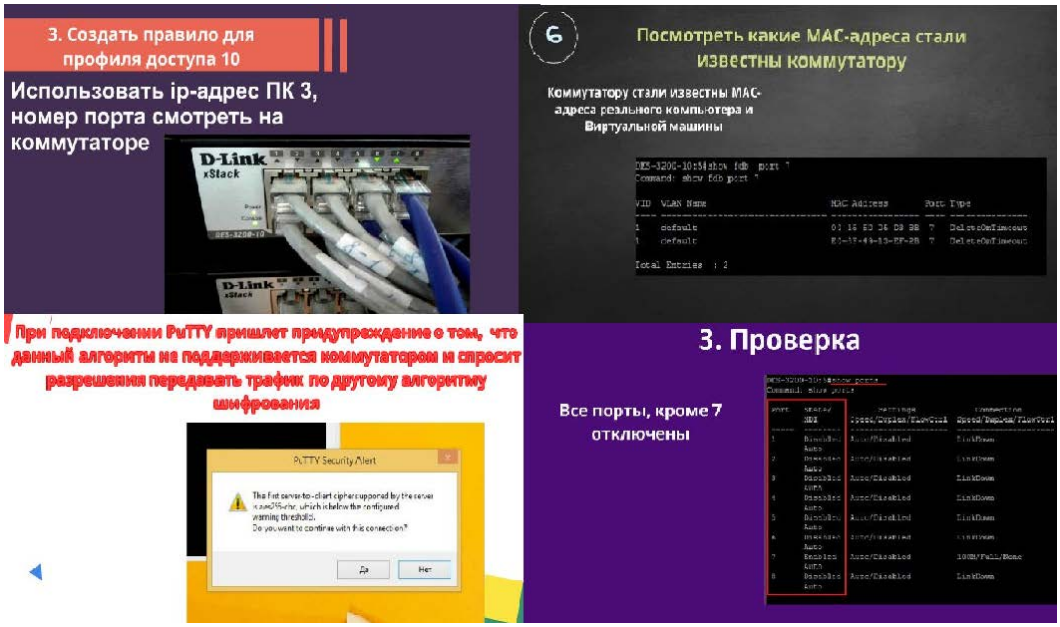

Рисунок 4 — Содержание видеороликов по настройке технологий

Проверка навыков, полученных в ходе выполнения лабораторных работ осуществляется при помощи контрольных заданий. Контрольные задания расположены в Moodle с помощью учебного элемента «Задание». Задание добавляется в форме любого выбранного вами файла. Перед контрольным заданием содержится небольшая инструкция к его выполнению. Задания содержат в себе различных 10 вариантов. Именно на такое количество одновременной работы студентов рассчитано оборудование учебной аудитории. Контрольные задания студенты выполняют самостоятельно. После выполнения работы студенты отправляют преподавателю файл-отчет, прикрепленный совместно с файлом задания. Задание считается выполненным при соответствии результата с критериями оценивания для преподавателя.

Закрепление знаний, полученных на практике осуществляется с помощью тестов. Тесты созданы с помощью элемента курса «Тест». Перед его выполнением содержится описание с критериями оценивания. Тест содержит 10 вопросов закрытой формы с выбором одного или нескольких правильных ответов и открытой формы на дополнение. Заданиями открытой формы называют задания без указания возможных вариантов ответа. Такие задания требует от учащихся самостоятельно сформулировать ответ, а не выбрать готовый. Достоинством заданий закрытой формы можно считать то, что они не допускают возможности угадывания [4]. С помощью заданий открытой формы проверяется точное знание изученных команд. Количество вопросов в тесте определялось значимостью и оптимальной полнотой полученных знаний.

Изучение каждого из модулей завершается на тесте по лабораторным работам. В ходе изучения модулей, обучающиеся усваивают теоретический материал, формируют умение применять полученные знания на практике, подтверждают знание изученного материала.

Преподавателю предоставляются файлы, в которых даны критерии оценивания практических работ и указания к подготовке учебной аудитории к их выполнению. Преподаватель может модифицировать курс по своему личному усмотрению: настроить журнал оценок, чтобы оценивать все работы студентов; установить необходимое количество баллов за выполнение каждого задания; наблюдать за активностью выполнения заданий студентами; назначать крайние сроки сдачи работ; добавлять, удалять, изменять сами модули или их содержание; самостоятельно записывать обучающихся на курс; открыть или закрыть доступ к курсу. Moodle предусматривает создание резервной копии всего лабораторного практикума. Эта возможность позволит при необходимости «откатить» лабораторный практикум к изначальному состоянию, всегда можно восстановить свои материалы, а также легко перенести часть информации из одного курса в другой. Файл резервной копии можно удалить, скачать, перенести в любое удобное для вас место.

2.3 Методика работы с лабораторным практикумом для обучающихся

Перед изучением лабораторного практикума необходимо ознакомиться с требованиями для его выполнения.

Первым модулем изучается secure shell, он является основой всех последующих модулей.

Обучающийся начинает изучение модуля с теоретической части. Теоретический материал лекций представлен видеороликами и рассчитан на самостоятельное обучение. После просмотра каждого видеоролика обучающийся отправляет отчет о прохождении задания преподавателю. Отчетом является слово «Выполнено».

После изучения теоретической части выполняется тест по изученному материалу. В тесте содержится 10 вопросов, в которых нужно выбрать один или несколько правильных ответов. Время для прохождения и количество попыток не ограниченно. После прохождения теста, тестовая система покажет результат прохождения в виде процента. За выполнение теста можно максимум набрать 5 баллов, проходной балл составляет 4 балла.

После прохождения теста нужно просмотреть видеоролики по подготовке рабочего места к настройке технологии, следуя инструкциям выполнения подготовить оборудование к настройке технологии. Отчетом также является слово «Выполнено».

Затем следует посмотреть видеоролик по настройке технологии безопасности. После просмотра соответствуя инструкциям настроить изучаемую технологию на оборудовании. Результаты работы отправить преподавателю в форме файла-отчета, прикрепленного совместно с видеороликом.

Следующим шагом необходимо самостоятельно выполнить контрольные задания по теме в соответствии со своим вариантом. Результат выполненной отправить преподавателю в форме файла-отчета, прикрепленного совместно с видеороликом.

Завершающим этапом в изучении модуля является тест по выполненным лабораторным работам. Тест содержит 10 вопросов с выбором вариантов ответа или вопросов открытого типа. Время для прохождения и количество попыток не ограниченно. После прохождения теста, тестовая система покажет результат прохождения в виде процента. За выполнение теста можно максимум набрать 5 баллов, проходной балл составляет 4 балла.

Последующие модули выполняются в той же последовательности. Если в ходе выполнения лабораторных работ у вас возникли вопросы обратитесь к преподавателю лично или свяжитесь с ним любым удобным для преподавателя способом. За выполнение всего курса можно получить максимум 100 баллов, проходная оценка составляет 77 баллов.

2.4 Методика применения лабораторного практикума для преподавателя

Перед выполнением лабораторных работ преподавателю необходимо:

1. Заблаговременно узнать у студентов наличие учетных записей в Moodle. Если их нет, создать учетные записи в Moodle самостоятельно.
2. Проверить наличие у компьютеров консольного порта. Если порт отсутствует, необходимо заменить системные блоки компьютеров на те, у которых есть консольный порт.
3. Проверить работу интернет соединения.
4. Проверить связь виртуальных машин с коммутаторами.
5. Проверить работу портов на коммутаторах D-Link DES 3200-10.
6. Проверить наличие оборудования с расчетом на 1 студента:
    - коммутатор D-Link DES 3200-10 – 1 штука;
    - консольный кабель – 1 штука;
    - кабель Ethernet – 3 штуки.
7. Проверить работу интернет соединения.

8. Учесть, что коммутаторов в аудитории 10 штук, а в аудитории может максимум находиться 12 студентов. Если в аудитории более 10 студентов, тогда следует разделить их по парам. В паре студенты выполняют роли «Организатора» и «Исполнителя». Роль «Организатора» выполняет студент, который чувствует себя более уверенно, роль «Исполнителя» выполняет студент, который не уверен в своих знаниях. В роль «Организатора» входит объяснение «Исполнителю», для чего используются команды, как подключается оборудование. За эту работу преподаватель оценивает контрольные задания у «Организатора» по результату «Исполнителя», если «Исполнитель» выполнил все правильно, то «Организатор» может не выполнять контрольные задания. В роль «Исполнителя» входит задавать вопросы «Организатору». «Организатор» говорит «Исполнителю», что нужно сделать, «Исполнитель» выполняет указания. Если «Исполнителю» что-то не понятно, «Организатор» ему поясняет. При затруднении у обоих обратиться к преподавателю. «Организатор» разбирается в командах и оборудовании, объясняя при этом ход работы «Исполнителю». «Исполнитель» подключает оборудование и вводит команды, по указанию «Организатора».

9. После настройки технологии SSH, ваша задача сохранить конфигурацию коммутаторов.

Модули следует выполнять в следующем порядке:

1) secure shell;
2) access control list;
3) IP-MAC-port binding;
4) port security.

Изучение модуля начинается с теоретической части. После просмотра видеороликов необходимо пройти тест по пройденному материалу, который содержит в себе пять вопросов. Необходимо ответить правильно на все вопросы.

Затем следует выполнить лабораторные работы по подготовке рабочего места к настройке технологии и настройке технологии. И подтвердить полу-

ченные знания путем выполнения контрольного задания и тестовых вопросов по практической части.

Видеоролики по теоретическому материалу и тесты выполняются дома самостоятельно. Лабораторные работы и контрольные задания выполняются только в аудитории на соответствующем оборудовании.

Студенты, которые отсутствовали или не успели выполнить лабораторные работы приходят на дополнительное занятие вместе с другой группой. Если у студентов возникли вопросы, они могут обратиться лично к преподавателю или связаться с ним любым удобным для преподавателя способом.

Выполнение лабораторных работ оценивается при помощи отчета. Студенты заполняют файл-отчет и отправляют его преподавателю. В лабораторном практикуме предусматривается возможность выставления баллов за проделанную работу. За выполнение всего курса можно получить максимум 100 баллов, проходная оценка составляет 77 баллов.

В файле-отчете студентам необходимо прикрепить скриншоты результата работы. В связи с этим для преподавателя составлен лист оценивания, в котором присутствуют подобные результаты, которые должны получится у студентов.

Лабораторная работа № 1. Настройка SSH, доступ по паролю.

- IP-адрес виртуальной машины (рисунок 5);

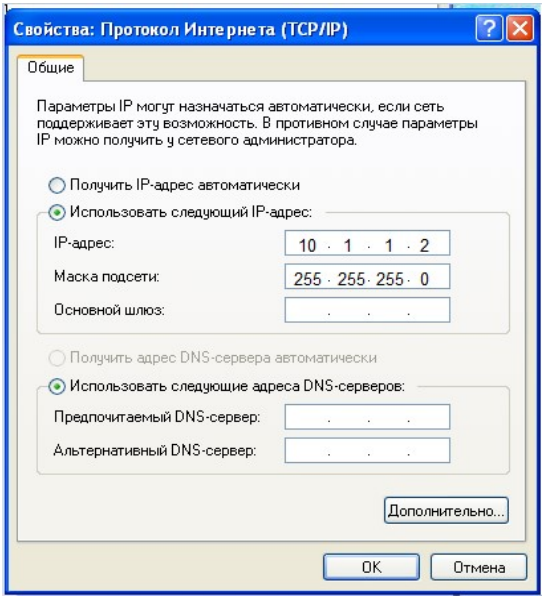

Рисунок 5 — IP-адрес виртуальной машины

- консоль управления, с введенными логином и паролем (рисунок 6).

Рисунок 6 — Консольное окно после успешного прохождения аутентификации

Лабораторная работа № 2. Настройка аутентификации в SSH по ключу доступа.

- IP-адрес виртуальной машины (рисунок 5);
- загрузка ключа в программу PuTTY (рисунок 7);

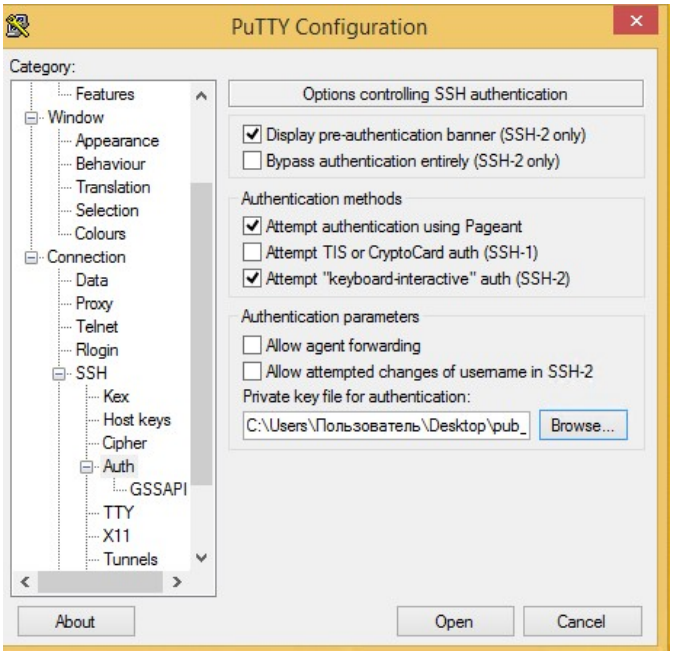

Рисунок 7 — Загрузка ключа в программу PuTTY

- запрос логина и пароля в консоли управления (рисунок 6);
- ошибка при подключении без ключа (рисунок 8);

Рисунок 8 — Ошибка при подключении без ключа

- разрешение передавать трафик по другому алгоритму (рисунок 9).

Рисунок 9 — Разрешение

Лабораторная работа № 3. Настройка ACL.

- IP-адрес компьютера (рисунок 5);
- команда правила для профиля доступа разрешающую прохождение трафика (рисунок 10);

```
DES-3200-10:5#config access_profile profile_id 10 add access_id 11 ip source_ip
10.1.1.3 port 6 permit
Command: config access_profile profile_id 10 add access_id 11 ip source_ip 10.1.1
.3 port 6 permit

Success.
```

Рисунок 10 — Правило для профиля доступа разрешающего прохожение трафика

- команда правила для профиля доступа запрещающую прохождение трафика (рисунок 11);

```
DES-3200-10:config access_profile profile_id 10 add access_id 11 ip source_ip 10.
1.1.3 port 5 deny
Command: config access_profile profile_id 10 add access_id 11 ip source_ip 10.1.1
.3 port 5 deny

Success.
```

Рисунок 11 — Правило для профиля доступа запрещающего прохожение трафика

- консоль управления при пинге в разрешенный порт (рисунок 12);

```
C:\Users\Пользователь>ping 10.1.1.1

Обмен пакетами с 10.1.1.1 по с 32 байтами данных:
Ответ от 10.1.1.1: число байт=32 время=4мс TTL=30
Ответ от 10.1.1.1: число байт=32 время=3мс TTL=30
Ответ от 10.1.1.1: число байт=32 время=3мс TTL=30
Ответ от 10.1.1.1: число байт=32 время=3мс TTL=30

Статистика Ping для 10.1.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 4 мсек, Среднее = 3 мсек
```

Рисунок 12 — Ответ коммутатора

- консоль управления при пинге в запрещенный порт (рисунок 13).

```
C:\Users\Пользователь>ping 10.1.1.1

Обмен пакетами с 10.1.1.1 по с 32 байтами данных:
Ответ от 10.1.1.7: Заданный узел недоступен.
Ответ от 10.1.1.7: Заданный узел недоступен.
Ответ от 10.1.1.7: Заданный узел недоступен.
Ответ от 10.1.1.7: Заданный узел недоступен.

Статистика Ping для 10.1.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
```

Рисунок 13 — Ответ коммутатора

Лабораторная работа № 4. Настройка IP-MAC-Port Binding.

- созданные записи IP-MAC-Port Binding (рисунок 14);

```
DES-3200-10:5#show address_binding ip_mac all
Command: show address_binding ip_mac all

M(Mode) - D:DHCP, N:ND P:DHCP-PD, S:Static ACL - A:Active I:Inactive

IP Address                              MAC Address       M  ACL Ports
--------------------------------------- ----------------- -- -- ---------------
10.1.1.2                                00-15-5D-05-D3-3B S  I  7

Total Entries : 1
```

Рисунок 14 — Созданные записи

- состояние портов (рисунок 15).

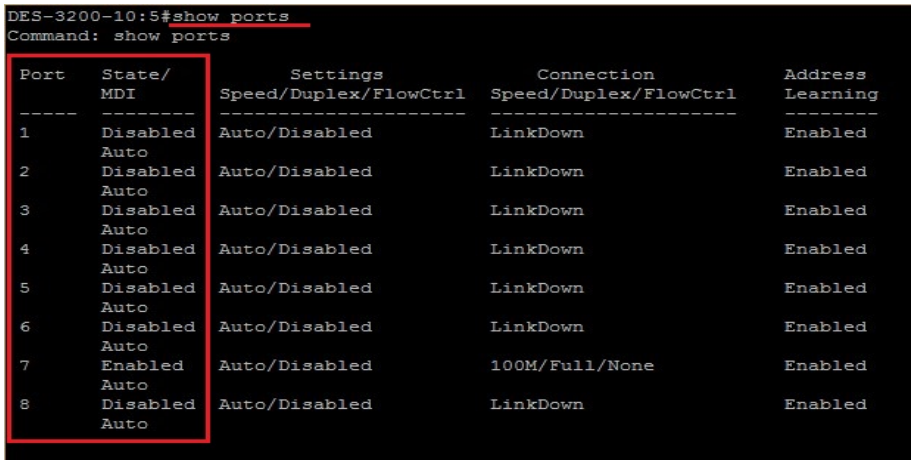

Рисунок 15 — Состояние портов

Лабораторная работа № 5. Настройка Port Security.

- созданные статические записи в таблице коммутации (рисунок 16);

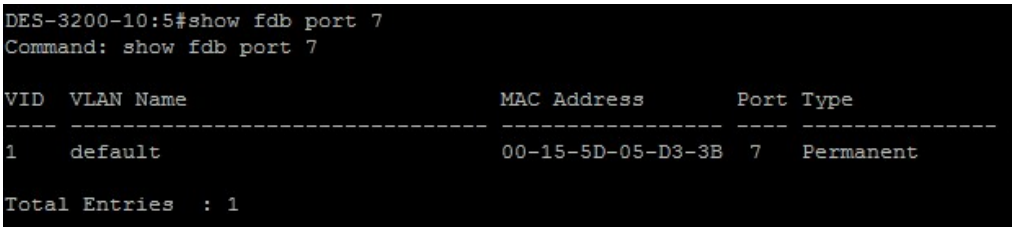

Рисунок 16 — Созданные записи в таблице коммутации

- информация о настройках Port Security на портах коммутатора (рисунок 17);

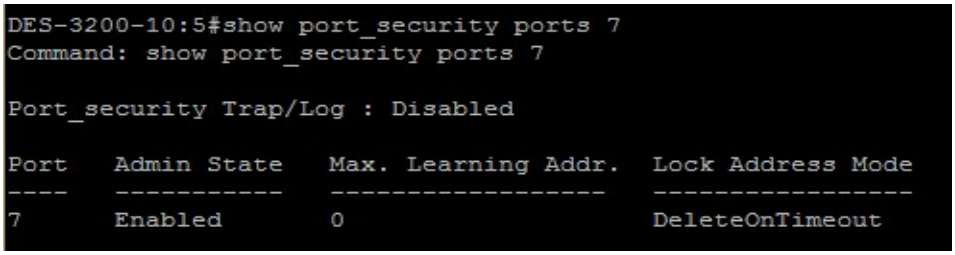

Рисунок 17 — Информация о настройке port security на коммутаторе

- MAC-адреса известные коммутатору после пинга коммутатора с виртуальной машины (рисунок 18).

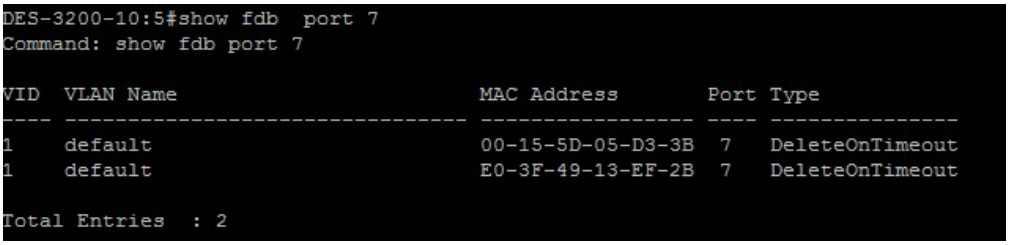

Рисунок 18 — MAC-адеса известные коммутатору

ЗАКЛЮЧЕНИЕ

В результате выпускной квалификационной работы был создан лабораторный практикум «Основы безопасности компьютерных сетей».

В ходе проделанной работы были проанализированы интернет-источники, которые показали, что в печатных изданиях содержится не достаточное количество информации по выполнению практических работ. Информация интернет-источников не дает четких руководств по настройке технологий и сложна для понимания новичками. Ни один из рассмотренных источников не предусматривает настройку технологии «с чистого листа» и не рассчитан на аудиторию сетевых технологий РГППУ.

Анализ учебной документации показал, что лабораторный практикум «Основы безопасности компьютерных сетей» вполне может применяться в рамках дисциплины «Защита сетевых информационных систем», направление подготовки 44.03.04 «Профессиональное обучение (по отраслям)», профиль подготовки «Информационные технологии».

В ходе определения содержания лабораторного практикума было выделено 4 модуля, включающих в себя: видеоролики и тесты по теоретической части, видеоролики по подготовке рабочего места к настройке технологий и настройки технологий, контрольные задания и тесты по закреплению изученного практического материала.

При разработке контента были созданы видеоролики в количестве 14 штук, тестовые задания в количестве 80 штук и контрольные задания в количестве 4 штук.

Лабораторный практикум был реализован в учебной версии модульной объектно-ориентированной динамической учебной среды (Moodle) РГППУ.

Таким образом, поставленные задачи можно считать полностью выполненными, а цель достигнутой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Базовая настройка свитчей D-Link серии xStack DES 3200 [Электронный ресурс]. — Режим доступа: http://sysadm.pp.ua/internet/des-3200-basic.html (дата обращения: 19.04.2018).

2. Влияние цвета на психику человека [Электронный ресурс]. — Режим доступа: http://psytheater.com/vliyanie-cveta-na-psixiku-cheloveka.html (дата обращения: 12.05.2018).

3. Желнин М.Э. Преимущества и недостатки тестирования в сравнении с другими методами контроля знаний / М.Э. Желнин, В.А. Кудинов, Е.С. Белоус // Ученые записки: электронный научный журнал Курского государственного университета. – 2012. –No1 (21) [Электронный ресурс]. — Режим доступа: http://scientific-notes.ru/pdf/023–030.pdf (дата обращения: 03.05.2018)

4. Жунусакунова А. Д. Разновидности заданий в тестовой форме [Текст] // Актуальные вопросы современной педагогики: материалы II Междунар. науч. конф. (г. Уфа, июль 2012 г.). — Уфа: Лето, 2012. — URL https://moluch.ru/conf/ped/archive/60/2572/ (дата обращения: 03.05.2018).

5. Категории кабеля витых пар, применяемых в компьютерных сетях [Электронный ресурс]. — Режим доступа: http://www.vadzhra.ru/version_twisted_utp_vapors_types_of_a_cable_applied_in_networks.html (дата обращения: 12.05.2018).

6. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding [Электронный ресурс]. — Режим доступа: https://www.intuit.ru/studies/courses/3591/833/lecture/14278 (дата обращения: 13.05.2018).

7. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding [Электронный ресурс]. — Режим доступа: https://www.intuit.ru/studies/courses/3591/833/lecture/14278?page=2 (дата обращения: 13.05.2018).

8. Контроль над подключением узлов к портам коммутатора. Функция Port Security [Электронный ресурс]. — Режим доступа: https://www.intuit.ru/studies/courses/3591/833/lecture/14277%3Fpage%3D2 (дата обращения: 12.05.2018).

9. Начальная настройка коммутатора [Электронный ресурс]. — Режим доступа: https://www.intuit.ru/studies/courses/3591/833/lecture/14253 (дата обращения: 12.05.2018).

10. Официальный сайт D-Link [Электронный ресурс]. — Режим доступа: http://www.dlink.ru (дата обращения: 15.04.2018).

11. Официальный сайт D-Link коммутатор DES-3200-10 [Электронный ресурс]. — Режим доступа: http://www.dlink.ru/ru/products/1/1719.html (дата обращения: 23.04.2018).

12. Официальный сайт D-Link коммутатор DES-3810-28 [Электронный ресурс]. — Режим доступа: http://www.dlink.ru/r/products/1/1359.html (дата обращения: 23.04.2018).

13. Официальный сайт института непрерывного образования РГППУ [Электронный ресурс]. — Режим доступа: http://ino.rsvpu.ru (дата обращения: 20.05.2018).

14. Преимущества и недостатки системы дистанционного образования Moodle типы [Электронный ресурс]. — Режим доступа: http://www.eduros.ru/konf/infor/9.html (дата обращения: 20.05.2018).

15. Рабочая программа дисциплины «Защита сетевых информационных систем» [Электронный ресурс]. — Режим доступа: https://vk.com/doc18589904_466916591?hash=f0a3dde73d77da2b94&dl=253ebbd6b87125c5c3 (дата обращения: 27.05.2018).

16. Рабочая программа дисциплины «Компьютерные коммуникации и сети» [Электронный ресурс]. — Режим доступа: https://vk.com/doc18589904_466916593?hash=edffe8d2620d17a7ff&dl=4007e60f774edf73d9 (дата обращения: 27.05.2018).

17. Смирнова Е.В. Построение коммутируемых компьютерных сетей: учебное пособие [Текст] / Е.В. Смирнова, А.В. Пролетарский, И.В. Баскаков, Р.А. Федотов. — Москва: Национальный Открытый Университет «ИНТУИТ»: БИНОМ. Лаборатория знаний, 2011. — 367 с.

18. Содержание педагогического теста [Электронный ресурс]. — Режим доступа: http://koi.tspu.ru/koi_books/samolyuk/lek9.htm (дата обращения: 03.05.2018).

19. Списки контроля доступа ACL [Электронный ресурс]. — Режим доступа: https://easy-network.ru/67-urok-39.html (дата обращения: 26.03.2018).

20. Списки управления доступом (Access Control List) [Электронный ресурс]. — Режим доступа: https://www.intuit.ru/studies/courses/3591/833/lecture/14276 (дата обращения: 26.03.2018).

21. Стандарты разъемов Rj и их типы [Электронный ресурс]. — Режим доступа: http://www.avs-el.ru/blogs/blog/standarty-razemov-rj-i-ih-tipy (дата обращения: 06.05.2018).

22. Учебная версия Moodle РГППУ http://lms-study.rsvpu.ru (дата обращения: 01.05.2018).

23. Функция IP-MAC-Port Binding [Электронный ресурс]. — Режим доступа: https://studopedia.ru/5_96780_funktsiya-IP-MAC-Port-Binding.html (дата обращения: 13.05.2018).

24. Что такое ACL и как его настраивать [Электронный ресурс]. — Режим доступа: http://ciscotips.ru/acl (дата обращения: 26.03.2018).

25. Что такое SSH [Электронный ресурс]. — Режим доступа: https://guides.hexlet.io/ssh/ (дата обращения: 21.04.2018).

26. Что такое SSH [Электронный ресурс]. — Режим доступа: https://www.hostinger.ru/rukovodstva/chto-takoe-ssh (дата обращения: 27.04.2018).

27. Animaker [Электронный ресурс]. — Режим доступа: https://www.animaker.com (дата обращения: 20.04.2018).

28. Profile-edu [Электронный ресурс]. — Режим доступа: http://www.profile-edu.ru/laboratornyj-praktikum-kak-raznovidnost-prakticheskogo-zanyatiya.html (дата обращения: 20.04.2018).

29. Powtoon [Электронный ресурс]. — Режим доступа: https://www.powtoon.com (дата обращения: 20.04.2018).

30. Port Security [Электронный ресурс]. — Режим доступа: http://telecombook.ru/archive/network/cisco/directory/63-port-security (дата обращения: 13.05.2018).

31. GoAnimate [Электронный ресурс]. — Режим доступа: https://www.vyond.com (дата обращения: 20.04.2018).

ПРИЛОЖЕНИЕ

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

Институт инженерно-педагогического образования
Кафедра информационных систем и технологий
направление 44.03.04 Профессиональное обучение (по отраслям)
профиль «Информатика и вычислительная техника»
профилизация «Информационная безопасность»

УТВЕРЖДАЮ
Заведующий кафедрой
_____Н. С. Толстова
«_____»_____2018 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра

студентки 4 курса, группы ИБ-401 Кашаповой Александры Анатольевны

1. Тема Лабораторный практикум «Основы безопасности компьютерных сетей» утверждена распоряжением по институту от 25.12.2017 г. № 82.

2. Руководитель Венков Сергей Сергеевич, старший преподаватель

3. Место преддипломной практики ФГАОУ ВО «Российский государственный профессионально-педагогический университет»

4. Исходные данные к ВКР

Смирнова Е.В. Построение коммутируемых компьютерных сетей: учебное пособие [Текст] / Е.В. Смирнова, А.В. Пролетарский, И.В. Баскаков, Р.А. Федотов. — Москва: Национальный Открытый Университет «ИНТУИТ»: БИНОМ. Лаборатория знаний, 2011. — 367 с.

Официальный сайт D-Link [Электронный ресурс]. — Режим доступа: http://www.dlink.ru (дата обращения: 15.04.2018).

5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов)
Проанализировать интернет-источники и учебную документацию
Определить содержание лабораторного практикума
Разработать контент
Создать лабораторный практикум
6. Перечень демонстрационных материалов
Презентация, разработанная в PowerPoint 2010, видеоролики.

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа ВКР	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной работе и сдача зачета по преддипломной практике	21.05.2018	15	
2	Выполнение работ по разрабатываемым вопросам их изложение в выпускной работе:		65	
	Определение содержания лабораторного практикума	01.05.2018	15	
	Разработка контента	08.05.2018	30	
	Создание лабораторного практикума	16.05.2018	20	
3	Оформление текстовой части ВКР	05.06.2018	5	
4	Выполнение демонстрационных материалов к ВКР	10.06.2018	5	
5	Нормоконтроль	11.06.2018	5	
6	Подготовка доклада к защите в ГЭК	13.06.2018	5	

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

Руководитель _____ *Задание получил* _____
подпись дата подпись студента дата

9. Выпускная квалификационная работа и все материалы проанализированы.
Считаю возможным допустить Кашапову Александру Анатольевну к защите выпускной квалификационной работы в государственной экзаменационной комиссии.

Руководитель _____ _____
подпись дата

10. Допустить Кашапову Александру Анатольевну к защите выпускной квалификационной работы
в государственной экзаменационной комиссии (протокол заседания кафедры
от 14.06.2018 №12)

Заведующий кафедрой _____ _____
подпись дата