

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

**ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО ДИСЦИПЛИНЕ
«БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ»**

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

Идентификационный номер ВКР: 558

Министерство науки и высшего образования 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

И.о. заведующего кафедрой ИС

_____ И. А. Сулова

« ____ » _____ 2019 г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО ДИСЦИПЛИНЕ
«БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ»**

Исполнитель:

обучающийся группы ЗИБ-401С

А. М. Атрощенко

Руководитель:

ст. преподаватель

Ю. А. Колесникова

Нормоконтролер:

Н. В. Хохлова

Екатеринбург 2019

АННОТАЦИЯ

Выпускная квалификационная работа состоит из лабораторного практикума содержащего учебные материалы по дисциплине «Безопасность компьютерных сетей» и пояснительной записки на 60 страницах, содержащей 27 рисунков, 30 источников литературы, а также 1 приложение на 2 страницах.

Ключевые слова: ЛАБОРАТОРНЫЙ ПРАКТИКУМ, БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

Атрощенко А.М., Лабораторный практикум по дисциплине «Безопасность компьютерных сетей»: выпускная квалификационная работа / А. М. Атрощенко; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2019. — 60 с.

В работе рассмотрены вопросы, связанные с безопасностью компьютерных сетей и разработкой лабораторного практикума.

Целью работы является разработка лабораторного практикума по дисциплине «Безопасность компьютерных сетей».

Для достижения цели были поставлены задачи: проанализировать учебную литературу и учебно-методическую документацию по дисциплине с целью отбора учебного материала; разработать структуру и интерфейс лабораторного практикума; наполнить лабораторный практикум учебными материалами.

Лабораторный практикум позволяет обучающимся самостоятельно освоить данную дисциплины и изучить оборудование.

СОДЕРЖАНИЕ

Введение.....	4
1 Анализ учебной литературы и учебно-методической документации по дисциплине «Безопасность компьютерных сетей»	6
1.1 Анализ литературных и интернет-источников по безопасности компьютерных сетей.....	6
1.2 Понятие лабораторный практикум.....	13
1.3 Анализ электронного учебного пособия по подобной тематике	14
1.4 Анализ рабочей программы дисциплины.....	17
2 Описание лабораторного практикума по безопасности компьютерных сетей.....	21
2.1 Педагогический адрес.....	21
2.2 Обзор средств реализации.....	21
2.3 Структура электронного лабораторного практикума	28
2.4 Интерфейс электронного учебного пособия	42
Заключение	54
Список использованных источников	56
Приложение	59

ВВЕДЕНИЕ

Важным и неотъемлемым аспектом любого информационного (ИТ) проекта являются вопросы информационной безопасности. Зачастую для крупных проектов требования по информационной безопасности бывают решающими для успешного проектирования и эксплуатации ИТ-систем и могут в значительной степени организационно влиять на способ реализации или содержательно влиять на выбор конкретных ИТ-решений в проекте.

В связи с этим появляется необходимость подготовки специалистов в данной области. В бюджетном учреждении (БУ) «Югорский политехнический колледж» при подготовке сетевых и системных администраторов отводится большая роль в изучении информационной безопасности в компьютерных сетях.

На сегодняшний день существует большое количество информации по безопасности компьютерных сетей.

Актуальность настоящей работы вытекает из противоречия между наличием образовательных ресурсов по дисциплине «Безопасность компьютерных сетей» и отсутствием упорядоченной информации в виде структурированного каталога, доступного всем преподавателям и студентам, единой базы электронных учебных материалов, организованных на уровне колледжа.

Таким образом, появляется проблема представления информации ученикам на занятиях в электронном виде.

В учебных заведениях такая проблема постепенно решается. Преподаватели ведут лекции с помощью электронных презентаций, предоставляют практический материал в электронном виде, создают электронные учебные пособия (ЭУП). Электронное учебное пособие — это целый комплекс учебного материала, предоставляющий возможность студенту в полном объеме изучить дисциплину посредством компьютера. В свою очередь преподава-

тель тратит меньше времени как на лекции, так и на практике на изложение материала.

В настоящее время существует несколько разновидностей электронных учебных пособий и одним из них является лабораторный практикум.

Лабораторный практикум — важная составляющая учебного процесса, в ходе которого обучающиеся сталкиваются с самостоятельной практической деятельностью [13].

Объектом выпускной квалификационной работы является процесс обучения студентов всех форм обучения, направления подготовки 09.02.06 Сетевое и системное администрирование базовой подготовки.

Предметом выпускной квалификационной работы является содержание учебного материала по дисциплине «Безопасность компьютерных сетей».

Таким образом, цель данной работы — разработать лабораторный практикум по дисциплине «Безопасность компьютерных сетей».

В соответствии с поставленной целью в работе определены следующие задачи:

- проанализировать учебную литературу и учебно-методическую документацию по дисциплине с целью отбора учебного материала;
- разработать структуру и интерфейс лабораторного практикума;
- наполнить лабораторный практикум учебными материалами.

1 АНАЛИЗ УЧЕБНОЙ ЛИТЕРАТУРЫ И УЧЕБНО-МЕТОДИЧЕСКОЙ ДОКУМЕНТАЦИИ ПО ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ»

1.1 Анализ литературных и интернет-источников по безопасности компьютерных сетей

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.

В учебном пособии В. В. Баринов, И. В. Баринов, А. В. Пролетарский, А. Н. Пылькин «Компьютерные сети» [2]. Изложены основные вопросы теории и практики построения компьютерных сетей и передачи данных. Рассмотрены определения, принципы построения, особенности архитектуры компьютерных сетей, приведены различные сетевые технологии (локальные, глобальные и региональные). Описаны физическая среда передачи, протоколы, функциональные группы устройств. Особое внимание уделено стандартам и технологиям беспроводных сетей, технологиям интернета и сервисам прикладного уровня.

Пособие состоит из восьми глав.

В главе 1 предоставлена эволюция компьютерных сетей, дано определение компьютерной сети, приведена классификация сетей, рассмотрены вопросы из топологии и продемонстрирована обобщенная схема компьютерной сети.

Глава 2 посвящена обзору основных стандартов в области компьютерных сетей.

В главе 3 рассмотрены теоретические основы передачи данных.

В главе 4 представлены определения протокола и межуровневого интерфейса, рассмотрены основные стеки протоколов.

Глава 5 посвящена вопросам изучения основных характеристик среды передачи данных, в ней рассмотрены основные линии передачи данных, используемые в компьютерных сетях.

В главе 6 раскрыты основные группы функциональных устройств, используемых в компьютерных сетях.

В главе 7 приведено полное описание основных топологий локальных и глобальных компьютерных сетей.

В главе 8 изложены вопросы современных технологий беспроводной передачи.

Вывод. Книга с обновлённым содержанием профессионального образования с учетом профессиональных стандартов, современных методик и технологий.

В книге А. А. Бирюков. «Информационная безопасность. Защита и нападение» [2]. Приведены как техническая информация, описывающая атаку и защиту от них, так и рекомендации по организации процесса обеспечения информационной безопасности.

Описаны современные решения по маршрутизации, беспроводной связи и другим направлениям развития информационных технологий. Рассмотрены практические примеры для организации защиты персональных данных в соответствии с Федеральным законом от 27 июля 2006г. № 152-ФЗ «О персональных данных».

Пособие состоит из восьми глав. Каждая глава разделена на параграфы. Каждый параграф подробно описывает рассматриваемую проблему, приводятся рисунки, так же приводятся примеры.

Вывод. В книге проведена актуализация технической информации, а также описано более глубокое погружение в практические аспекты, связанные с проведением аудитов по безопасности и тестов на проникновение для различных систем. Книга предназначена для системных администраторов и

пользователей малых и средних сетей, осуществляющих защиту корпоративных ресурсов.

В книге М. М. Котухов, А. Н. Кубанков, А. О. Калашников «Информационная безопасность» [9]. Рассмотрены основные классы способов и средств защиты информации, нормативные и правовые аспекты обеспечения информационной безопасности и ее организационно-техническое обеспечение, а также особенности структуры и управления корпоративных систем защиты информации, включая аудит.

Книга разбита на 3 главы, каждая глава разделена на параграфы из 6 частей, каждая часть поделена на темы. Каждая тема раскрыта достаточно полно, приводятся рисунки.

Вывод. Данный источник полно описывает нормативным и правовым аспектам обеспечения информационной безопасности. Книга предназначена для студентов.

В учебном пособии А. Н. Андрончик, «Сетевая защита на базе технологий фирмы Cisco Systems» [1]. Раскрывает вопросы практического применения методов и средств защиты информации в компьютерных сетях. В качестве платформы для построения защищенных сетей рассмотрены технологии и программно-аппаратные комплексы фирмы Cisco Systems.

В пособии рассмотрены основные команды операционной системы Cisco, вопросы администрирования маршрутизаторов и межсетевых экранов, способы обнаружения сетевых компьютерных атак на базе комплексов Cisco IDS Sensor и Cisco MARS.

Учебное пособие состоит из 5 разделов, каждый раздел содержит параграфы.

В основном разделы носят практический характер, в которых описаны: основы конфигурирования в командной строке, конфигурирование сетевых устройств фирмы Cisco, межсетевое экранирование с использованием технологий фирмы Cisco, обнаружение сетевых компьютерных атак.

После каждого раздела есть контрольные вопросы.

Вывод. Практическое пособие подробно описывает технологии и программно-аппаратные комплексы фирмы Cisco Systems. Предназначено для студентов и преподавателей, слушателей потоков повышения квалификации по направлению информационной безопасности, а также специалистов-практиков в области защиты компьютерной информации.

В книге Бен Пайпер «Администрирование сетей Cisco» [2]. Рассказывается в доступной форме рассказывает об администрировании сетей с применением оборудования Cisco. С помощью практических заданий вы сможете получить полное представление о том, как работают сети, получите знания, которые сможете использовать уже сегодня. Вы сможете не только усовершенствовать свои навыки, но так же будете в состоянии объяснить, почему сети работают так.

Книга состоит из 22 глав, далее разбиты на параграфы, которых рассматриваются основные темы: управление портами коммутатора, защита портов с помощью технологии port-security, обеспечение безопасности сети с помощью списка контроля доступа и т.д.

Вывод. Книга содержит множество примеров команд Cisco, размещенных рядом с обычным текстом. Решения практических заданий и рекомендации по настройке виртуальной лаборатории.

Книга предназначена для усовершенствования знаний о существующих сетях, усовершенствования навыков работы в сети, для выполнения практических заданий и применения их на практике.

В книге В. Ф. Мелехина, Е. Г. Павловского «Вычислительные машины, системы и сети» [28]. Рассмотрены современные компьютеры, микропроцессорные системы на базе микроконтроллеров, вычислительные системы параллельной обработки данных, основы построения компьютерных сетей, а также тенденции развития архитектур, обусловленные успехами микроэлектроники и развитием информационных технологий.

Книга состоит из 7 глав, каждая глава содержит темы.

Вывод. Книга предназначена для студентов как учебное пособие. В книге изложены основы организации, архитектура построения вычислительных машин, систем и сетей. Приведены основные характеристики различных классов систем обработки данных и способы их оценки.

В учебнике В. Г. Олифер, Н. А. Олифер «Безопасность компьютерных сетей» [14]. Рассмотрены меры обеспечения безопасности компьютерных систем как органической части общей информационной системы предприятия; методы защиты программного обеспечения компьютеров и обрабатываемой ими информации; сетевые аспекты передачи информации между узлами компьютерной сети (вопросы безопасности сетевых протоколов и сервисов); базовые технологии, используемые для защиты информации в компьютерной сети, такие как шифрование, аутентификация, авторизация, организация защищенного канала и другие, которые в той или иной мере являются основой всех методов обеспечения безопасности компьютерных сетей.

Учебник состоит из 4 частей, каждая часть содержит главы.

В первой части приводятся основы информационной безопасности.

Второй части рассматриваются базовые технологии компьютерной безопасности.

В третьей части подробно описываются защиты транспортной инфраструктуры сетей.

В четвертой части описана безопасность системного и прикладного программного обеспечения.

Вывод. Книга структурирована в виде учебного курса и отличается широким охватом затронутых тем, при этом авторы стремились сохранить достаточную глубину рассмотрения вопросов, позволяющую понять их суть. Все главы книги завершаются набором вопросов для проверки и самопроверки.

Дисциплина «Безопасность компьютерных сетей» не нова. Учебный материал содержит в себе различные формулы, графики, лабораторные работы.

Есть много электронных учебников и курсов по данной дисциплине. Основным можно считать сетевую академию Cisco [16], это закрытый интернет-ресурс, но в нём достаточно хорошо изложен материал и практические работы. Также есть и открытые интернет ресурсы.

Электронный учебник Б. А. Фороузан «Криптография и безопасность сетей» [23]. В данном учебнике используется подход обучению безопасности сети и криптографии по нарастающей сложности. Она не предполагает у читателя никаких особых и специальных знаний

Учебник состоит из 18 лекций: начиная от основ криптографии и заканчивая безопасностью на сетевых уровнях.

Вывод. Данный источник довольно полно рассматривает тему криптографии. В представленных лекциях студенты могут освоить необходимую математическую основу для изучения следующего за ним материала; эти математические лекции могут быть пропущены, если студенты обладают соответствующими знаниями. Данный источник открыт и может быть использован для самостоятельного изучения или в качестве учебного пособия.

В электронном учебнике Криса Касперски «Компьютерные вирусы изнутри и снаружи» [10]. Рассматриваются темы: как происходит внедрение чужеродного кода в исполняемый файл, и по каким признакам его можно распознать; насколько надежны антивирусы и можно ли их обхитрить; как хакеры ломают программное обеспечение и как их остановить.

Учебник разделен на 4 части. Каждая часть содержит в себе как минимум 3 раздела.

Вывод. В данном источнике достаточно полно и иллюстративно представлен учебный материал. В учебном материале рассмотрены основы происхождения вирусов и общее понимание про них.

В электронном учебнике С. В. Гордейчика, В. В. Дубровина «Безопасность беспроводных сетей» [6]. Представлен подробный анализ причин возникновения уязвимостей и типичных ошибок, допускаемых при развертыва-

нии беспроводных сетей. Описываются этапы построения защищенной беспроводной сети — от создания политики безопасности до настройки систем обнаружения беспроводных атак и проведения тестов на проникновения.

Книга разбита на 3 главы, каждая глава разделена на параграфы. Каждый параграф подробно описывает рассматриваемую проблему.

Вывод. В данном источнике достаточно полно представлен учебный материал. В учебном материале рассмотрены основные причины уязвимости беспроводных сетей так и настройку безопасности в беспроводных сетях.

В учебнике А. А. Кузина «Компьютерные сети» [9]. Рассматриваются общие вопросы построения компьютерных сетей, такие как: сетевые архитектуры, аппаратные компоненты, «линии связи, сетевые модели, задачи и функции по уровням сетевой модели Open Systems Interconnection Basic Reference Mode (OSI), различия и особенности распространенных протоколов разных уровней, принципы адресации в сети, методы доступа к среде передачи данных.

Учебник состоит из 9 глав, каждая глава содержит параграфы.

Вывод. В книге приводятся особенности основных операционных систем, структура и информационные услуги территориальных сетей. Книга предназначена для студентов средних специальных учебных заведений.

Таким образом, проанализировав учебную литературу, пришли к следующему выводу, не смотря на то, что данные источники содержат актуальную информации необходимую для изучения дисциплины «Безопасность компьютерных сетей», они не в полной мерной соответствуют содержанию рабочей программы и поэтому данную литературу рекомендуется использоваться в качестве дополнительной литературы. В связи с этим возникла необходимость в создании лабораторного практикума, тематика которого полностью соответствует содержанию рабочей программы и может использоваться в качестве основано источника информации.

1.2 Понятие лабораторный практикум

Лабораторный практикум — важная составляющая учебного процесса, в ходе которого обучающиеся сталкиваются с самостоятельной практической деятельностью [13]. 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 в будущем специалисту, возможно, придется столкнуться в реальной жизни.

Эффективность лабораторного практикума 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 Анализ электронного учебного пособия по подобной тематике

Дисциплина «Безопасность компьютерных сетей» очень сложна в своей интерпретации. Учебный материал содержит как теоретические сведения, так и наглядное объяснение тех или иных аспектов компьютерной безопасности, демонстрацию объектов.

Перед тем, как начать разрабатывать интерфейс электронного учебного пособия, нужно было исследовать аналогичные продукты по данной тематике. В результате исследования данного вопроса, было выявлено очень много электронных пособий по данной дисциплине. Особый интерес для нас представляет сетевая академия Cisco, являющаяся закрытым интернет ресурс [12].

Программа Сетевой Академии Cisco предоставляет студентам комплексную среду обучения, которая позволяет получать навыки использования Интернет технологий, играющих важнейшую роль в условиях глобализации экономики. Она обеспечивает доступ к информационным Интернет ресурсам и включает в себя средства онлайн-тестирования и проверки успеваемости, практические лабораторные занятия, консультации и поддержку преподавателей, а также готовит студентов к получению сертификатов международного образца.

Для анализа были выбраны три характеристики ЭУП:

- удобство интерфейса;
- цветовое решение;
- навигация.

Удобство интерфейса

Интерфейс продукта заставляет пользователя обратить внимание на себя. Заставка на стартовой странице выполнена на рисунке 1.

Все пункты меню расположены горизонтально.

В целом, интерфейс достаточно интересен, так же есть возможность сменить задний фон.

ЭУП представлено на 9 языках: русский, английский, китайский, французский и т.д.

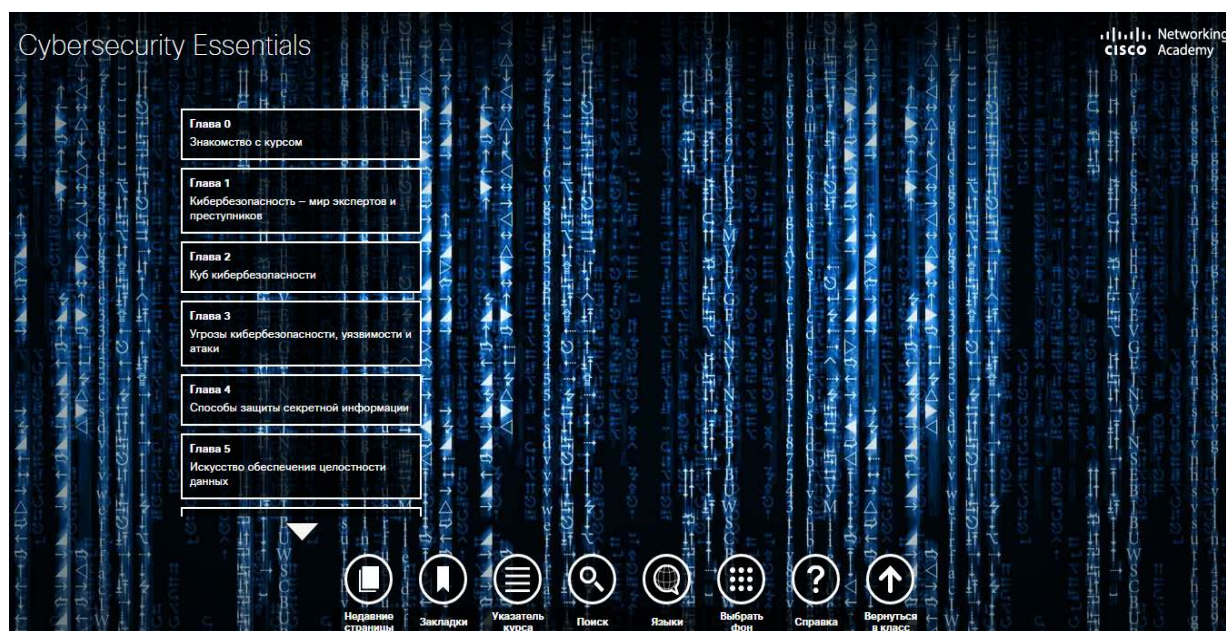


Рисунок 1 — Стартовая страница

Цветовое решение

Наиболее важными при выработке цветового решения экрана можно считать следующие принципы:

- при выборе цветов следует учитывать их психофизиологическое воздействие на человека;
- при использовании нескольких цветов большую роль играет их правильное сочетание.

В ЭУП можно менять фон как удобно пользователю, тема самым позволяю выбирать самое оптимальное и приятное цветоощущения для восприятия материала.

Навигация

Навигация в электронном учебном пособии интуитивно понятна пользователю. При наведении на название главу появляются выпадающий список разделов, при наведении на раздел, появляется выпадающий список (рисунок 2).

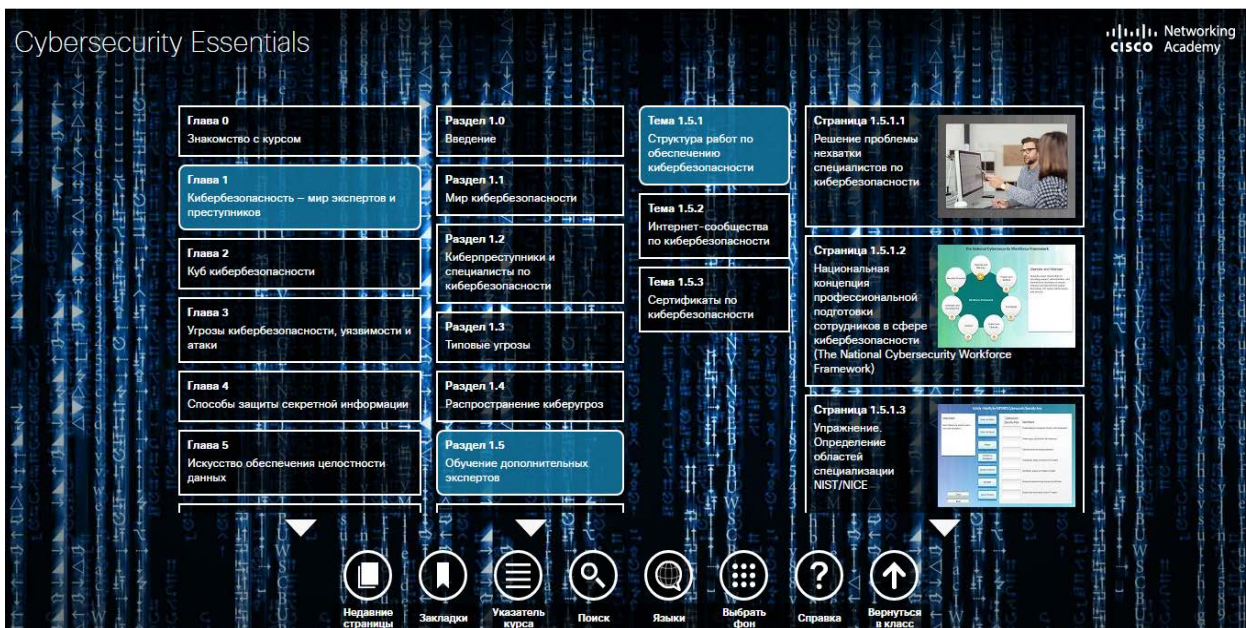


Рисунок 2 — Навигация по материалу

Есть удобное дополнительное меню (рисунок 3).

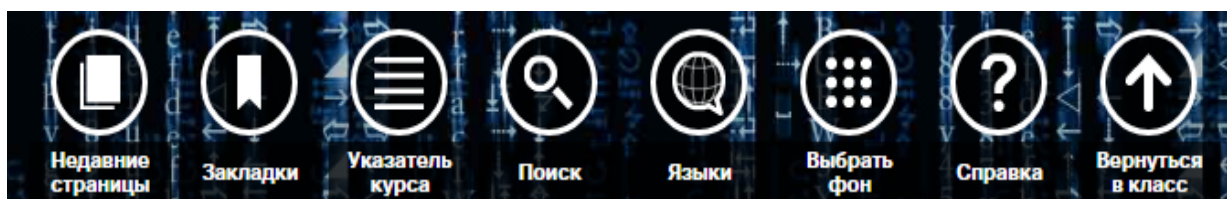


Рисунок 3 — Дополнительное меню

Для удобства предусмотрена кнопка «Вперед» «Назад», и вкладки «Закладка» «Запись» (рисунок 4).



Рисунок 4 — Кнопка управления страниц

Общий интерфейс и подача материала представлен на рисунке 5.

Вывод. Проанализировав данное ЭУП были выявлены такие достоинства как интуитивно-понятный интерфейс, удобная навигация, удобность кнопок перехода простота и понятность материала, наличие медиа — материала и практических работ.

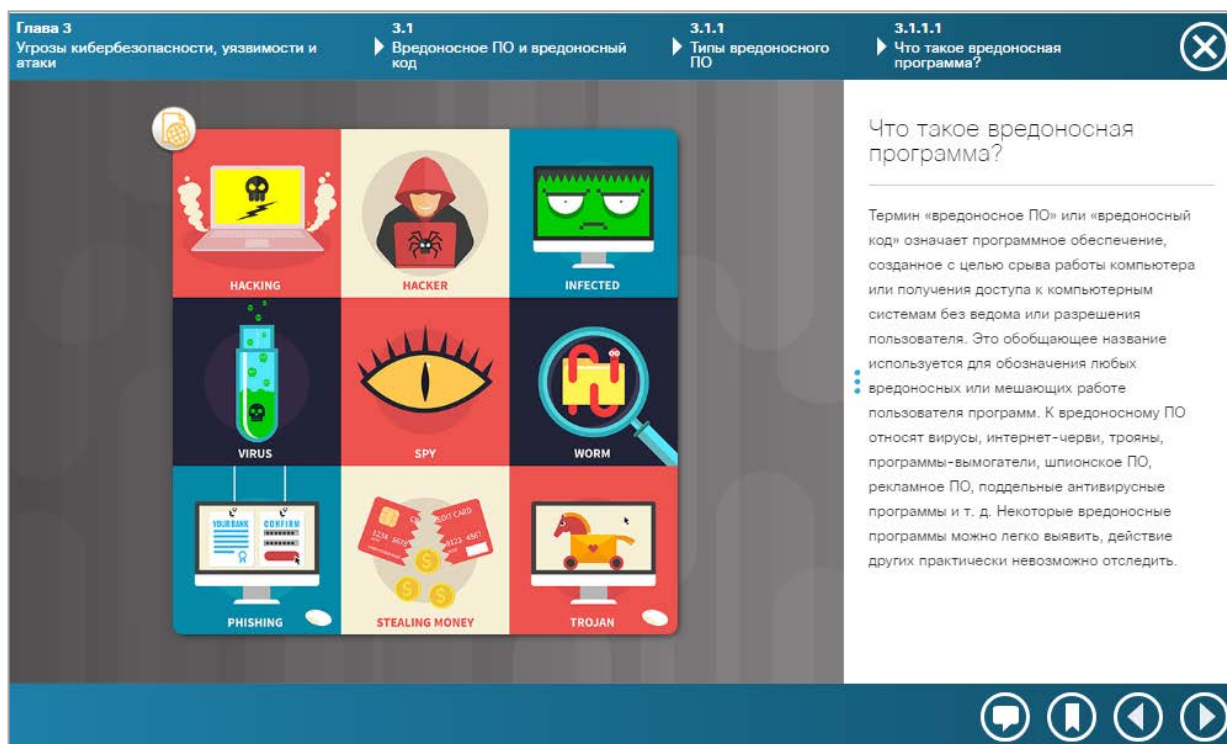


Рисунок 5 — Учебный материал

1.4 Анализ рабочей программы дисциплины

Анализ рабочей программы [22] показал место учебной дисциплины в структуре основной профессиональной образовательной программы.

Обучения направления подготовки 09.02.06 Сетевое и системное администрирование базовой подготовки, по профилю «Сетевой и системный администратор» по дисциплине «Безопасность компьютерных сетей».

Целью дисциплины «Безопасность компьютерных сетей» является формирование у студентов знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств.

Задачи дисциплины — дать знания:

- о методах и средствах защиты информации в компьютерных сетях;
- о технологии межсетевое экранирования;
- о методах и средствах построения виртуальных частных сетей;
- о методах и средствах аудит уровня защищенности информационных систем.

Приобретенные знания и навыки позволят студентам работать в должностях администраторов компьютерных сетей и администраторов безопасности.

Распределение времени на освоение программы учебной дисциплины «Безопасность компьютерных сетей» представлено в таблице 1.

Таблица 1 — Количество часов, отведенных на изучение дисциплины «Безопасность компьютерных сетей»

Вид учебной работы	Объем часов
Общая трудоемкость дисциплины	84
Аудиторные занятия	36
Лекции	12
Лабораторные занятия	12
Практические занятия (ПЗ)	24
Самостоятельная работа	
внеаудиторная самостоятельная работа	14

В результате изучения дисциплины студенты должны:

знать:

- технологии обнаружения компьютерных атак и их возможности;
- основные уязвимости и типовые атаки на современных компьютерные системы;
- возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности;
- методы защиты компьютерных сетей;
- классификацию и общую характеристику сетевых программно аппаратных средств защиты информации;
- основные принципы администрирования защищенных компьютерных систем;
- особенности реализации методов защиты информации современными программно-аппаратными средствами;

уметь:

- выполнять функции администратора безопасности защищенных компьютерных систем;
- выполнять настройку защитных механизмов сетевых программно-аппаратных средств;
- настраивать политику безопасности средствами программно-аппаратных комплексов сетевой защиты информации;
- применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей;
- организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов;

владеть:

- средствами администрирования сетевых программно-аппаратных комплексов защиты информации;
- средствами администрирования систем обнаружения компьютерных атак;
- средствами и системами аудита информационной безопасности;
- методикой проведения аудита информационной безопасности средствами администрирования систем организации виртуальных частных сетей.

Тематический план дисциплины «Безопасность компьютерных сетей» предусматривает изучение следующих разделов:

1. Обнаружение компьютерных атак.
2. Технология межсетевого экранирования.
3. Организация виртуальных частных сетей.
4. Технологии защищенной обработки информации.
5. Аудит информационной безопасности в компьютерных сетях.

Цикл лабораторных работ по дисциплине «Безопасность в компьютерных сетях» реализуется в рамках аудиторных занятий, предусмотренных

учебным планом и выполняются в компьютерном классе и в лаборатории на специализированных стендах коммутаторов и маршрутизаторов Cisco.

Цикл практических работ реализуется в специальной программе Cisco Packet Tracer.

При разработке лабораторного практикума мы опирались на рабочую программу и методическим указанием.

В результате анализа рабочей программы, можно прийти к выводу, что созданный лабораторный практикум вполне может применяться в образовательном процессе в БУ «Югорский политехнический колледж» и содержание практикума полностью соответствует учебной программе дисциплине «Безопасности компьютерных сетей».

2 ОПИСАНИЕ ЛАБОРАТОРНОГО ПРАКТИКУМА ПО БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

2.1 Педагогический адрес

Данный лабораторный практикум предусмотрен для изучения в рамках дисциплины «Безопасность компьютерных сетей», направление подготовки 09.02.06 «Сетевое и системное администрирование» базовой подготовки, по профилю «Сетевой и системный администратор».

Изучение дисциплины «Безопасность компьютерных сетей» предусматривает предварительное зачисление студента в сетевую академию Cisco.

Знания и умения необходимые студентам для освоения лабораторного практикума:

- знать IPv4 и уметь его настраивать на операционной системе (ОС) Windows;
- знать технологию Fast Ethernet;
- уметь работать со средами виртуализации Hyper-V, VMware.

2.2 Обзор средств реализации

В настоящее время можно выделить основные требования к современным учебным пособиям, которые должны быть ориентированы на увеличение самостоятельной работы студента, а, следовательно, должны быть более простыми в использовании, информативными, наглядными, усиливающими мотивацию к освоению предмета; быть доступными для всех желающих получить полноценное образование; обеспечивать подготовку специалистов высокого класса; широко использовать современные средства телекоммуникации и новейшие информационные технологии.

Многие из перечисленных требований противоречивы и трудно совместимы, поэтому разработка электронного учебника представляет собой сложную задачу, решаемую коллективом специалистов разного профиля, и требует обоснованного выбора подходящего программного обеспечения.

Средства создания электронных пособий можно разделить на группы используя комплексный критерий, включающий такие показатели, как назначение и выполняемые функции, требования к техническому обеспечению, особенности применения. В соответствии с указанным критерием возможна следующая классификация:

- языки программирования;
- средства мультимедиа;
- специальные программные средства создания электронных учебников.

Языки программирования. Современные визуальные среды программирования (Visual Basic, C# и др.) позволяют создавать достаточно универсальные программы, в том числе и электронные учебники. К явным недостаткам электронных пособий, созданных средствами языков программирования можно отнести:

- сложность модификации и сопровождения;
- большую стоимость вследствие трудоемкости разработки.

К достоинствам:

- разнообразие стилей реализации (цветовая палитра, интерфейс, структура электронных пособий, способы подачи материала);
- отсутствие аппаратных ограничений, то есть возможность создания электронных пособий, ориентированного на имеющуюся в наличии техническую базу.

Следует отметить, что учитывая современное состояние технической базы в образовательных учреждениях, использование языков программирования для создания электронных пособий становится неактуальным. Данное программное средство, как правило, используют для написания отдельных

модулей пособий с элементами интерактивности (модули проверки знаний, тренировочные задания, виртуальные эксперименты и др.).

Средства мультимедиа. Технологии мультимедиа объединяют несколько способов подачи информации: текст, неподвижные изображения, движущиеся изображения и звук в интерактивный продукт.

Средства мультимедиа позволяют значительно обогатить учебный материал за счет активизации всех способов восприятия. Таким образом, к достоинствам электронных пособий, созданных с помощью данного программного средства относят:

- возможность комбинированного представления учебного материала в графическом, текстовом, звуковом виде;
- возможность автоматического просмотра всего содержания продукта («слайд-шоу»).

К недостаткам:

- большой вес электронных пособий на диске;
- преобладает линейная структура представления учебного материала.

Рассмотрим несколько специальных программ для создания электронных пособий.

eBooksWriter LITE. Простая в эксплуатации программа с достаточным количеством функций. С её помощью создают книги не только для персональных компьютеров, но и для мобильных устройств. eBooksWriter LITE имеет простой визуальный редактор, подходящий как для начинающего, так и для продвинутого пользователя. Продукт даёт возможность не только создавать пособия с нуля, но и импортировать уже готовые книги в формате *.rtf или *.doc. Кроме текстовых данных, книга, созданная с помощью eBooksWriter LITE, может содержать аудио и видео файлы и таблицы [26].

Достоинства:

- электронное пособие, созданный с помощью данного продукта, представляет собой самораспаковывающийся файл небольшого размера;

- можно защитить паролем отдельные части книги или всё пособие целиком;

- есть возможность защиты от копирования или печати;
- книги сохраняются в форматах *.exe или *.aep;
- есть подключаемые модули.

Недостаток:

- бесплатная версия LITE может создавать электронных пособий только размером до 1 Мб, что соответствует примерно 20 страницам. В версиях PRO и GOLD допустимый размер книг гораздо больший: до 260000 страниц.

eBook Maestro. Универсальное средство создания электронных журналов, пособий, отчётов, презентаций, опросников, книг и т.п. С помощью данного продукта в пособие могут быть включены файлы разных типов: HyperText Markup Language (HTML) страницы, Java скрипты, звуковые, графические и видео файлы и многие другие.

С помощью eBook Maestro можно вставлять в книгу ссылки на ресурс в Интернете, публиковать адрес электронной почты, а также создавать иконки. Элементами окна книги могут быть такие кнопки, как «Домашняя страница», «Поиск» и другие. Можно задавать им свои названия на русском и английском языках. Все файлы книги, имеющей сложную структуру, хранятся в разных директориях [25].

Достоинства:

- поддержка HTML;
- обработка и сохранение данных, введённых пользователем в проект;
- преобразование текста в речь;
- быстрый и удобный поиск.

Недостатки:

- максимальное число файлов для одной книги в версии FREE — 500, в то время как в версиях STANDARD и PRO их неограниченное количество.

ChmBookCreator — это простой в использовании продукт, который из обычных файлов *.html, *.txt, *.doc и *.rtf создаст электронное пособие, которое будет выглядеть как обычная раскрытая книга на бумажном носителе. С помощью ChmBookCreator можно создать хорошо структурированный электронный учебник [24].

Достоинства:

- можно не только создавать электронных пособий, но и конвертировать их из других форматов;
- есть возможность создавать собственный уникальный дизайн для пособия;
- удобен для неопытного пользователя;
- наличие подробной встроенной справки.

Недостатки:

- медленная обработка файлов *.doc.

TurboSite. Бесплатная программа для создания сайтов и электронных пособий. Можно создать HTML-сайт или электронное пособие с поддержкой комментариев, формы обратной связи, вставки видео-файлов и JavaScript — тестов и другими возможностями. Программа очень проста в обращении, не требует знания языков программирования и разметки текста [30].

Достоинства:

- программа проста в освоении и предлагает множество готовых шаблонов, которые в процессе работы можно изменять;
- работа осуществляется через веб-браузер с поддержкой стандарта HTML5;
- результат получается быстро и его можно редактировать в процессе работы.

Недостатки:

- возможность некорректного отображения материала в разных браузерах;

- в структуре создаваемого электронного учебника все разделы будут одного уровня.

Learning Content Development System. Система управления обучением, совместимые с форматом Sharable Content Object Reference Model (SCORM), который описывает техническую структуру электронного пособия, с помощью некоторых основных принципов, спецификаций, и стандартов, основанных на работе других уже созданных спецификаций и стандартов электронного и дистанционного образования.

Система предназначена для создания электронных пособий с интерактивными тестами, демонстрационными роликами, экзаменами и анимацией. Использование среды не требуется никаких особых навыков программирования или дизайна. Интерактивные курсы строятся путем создания и настройки различных модулей на основе готовых шаблонов с использованием созданных автором аудио и видео клипов и других мультимедийных файлов.

Достоинства:

- создание веб-материалов, соответствующих набору стандартов SCORM и пригодных к использованию в системах для управления обучением;
- выбор форм из широкого многообразия форм для создания эффективных электронных курсов и интерактивных компонентов на основе технологии Silverlight.

Также к неоспоримым преимуществам программы Learning Content Development System является поддержка технологии Windows Presentation Foundation (WPF). Данная технология представляет собой набор инструментальных средств для построения приложений, сочетающих в себе графический пользовательский интерфейс, возможности работы с документами и мультимедиа. WPF является развитием предыдущих технологий Microsoft для создания пользовательского интерфейса (Windows Forms, Direct 3D, технологии, применяемые в Windows Media Player). WPF включает в себя большую часть возможностей предшествовавших технологий и добавляет новые средства для создания более сложных пользовательских интерфейсов [27].

Недостатки:

- необходимость установки плагинов для корректного отображения учебных материалов.

В целом, при выборе средств разработки электронных учебников необходима оценка наличия:

- аппаратных средств определенной конфигурации;
- сертифицированных программных систем;
- специалистов требуемого уровня.

Таким образом, рассмотрев несколько средств реализации современных электронных пособий, мы пришли к выводу, что, не смотря на ряд преимуществ рассматриваемых сред, они в большинстве своем имеют ряд ограничений, например на объем предоставляемой памяти, недостаточный функционал бесплатных версий и необходимость установки дополнительного программного обеспечения.

Кроме того, необходимо учитывать назначение разрабатываемого электронных пособий необходимость модификации дополнения новыми данными, ограничение на объем памяти и др. Все это привело к тому, что в качестве среды реализации лабораторного практикума был выбран формат HTML с использованием таблицы стилей Cascading Style Sheets (CSS). Для автоматизации набора HTML-кода был использован редактор «Notepad++».

Notepad++ — популярный текстовый редактор, поддерживающий огромное количество языков программирования

Текстовый редактор Notepad++, несмотря на свою простату, обладает богатым функционалом. Текст, разделяется на блоки, а слова, относящиеся к языкам программирования, подсвечиваются. Следует отметить, что в одном документе можно создать несколько вкладок [28].

Так же редактор позволяет пользователю изменять, а также преобразовывать кодировку. Подобная возможность позволяет переписывать код с применением кириллицы. При необходимости можно установить кодировку UTF-8. К тому же эта функция позволяет редактировать bat-файлы.

Среди всех редакторов кода Notepad++ определенно является одним из самых лучших программ. Под его довольно простой внешностью скрывается мощный, настраиваемый редактор кода с большим полезным функционалом, и поддерживающий множество языков программирования.

2.3 Структура электронного лабораторного практикума

Структуре лабораторного практикума выделяют 6 разделов (рисунок 6):

1. Введение.
2. Блок теоретического материала.
3. Блок практического материала.
4. Итоговый контроль.
5. Литература.
6. Оборудования.

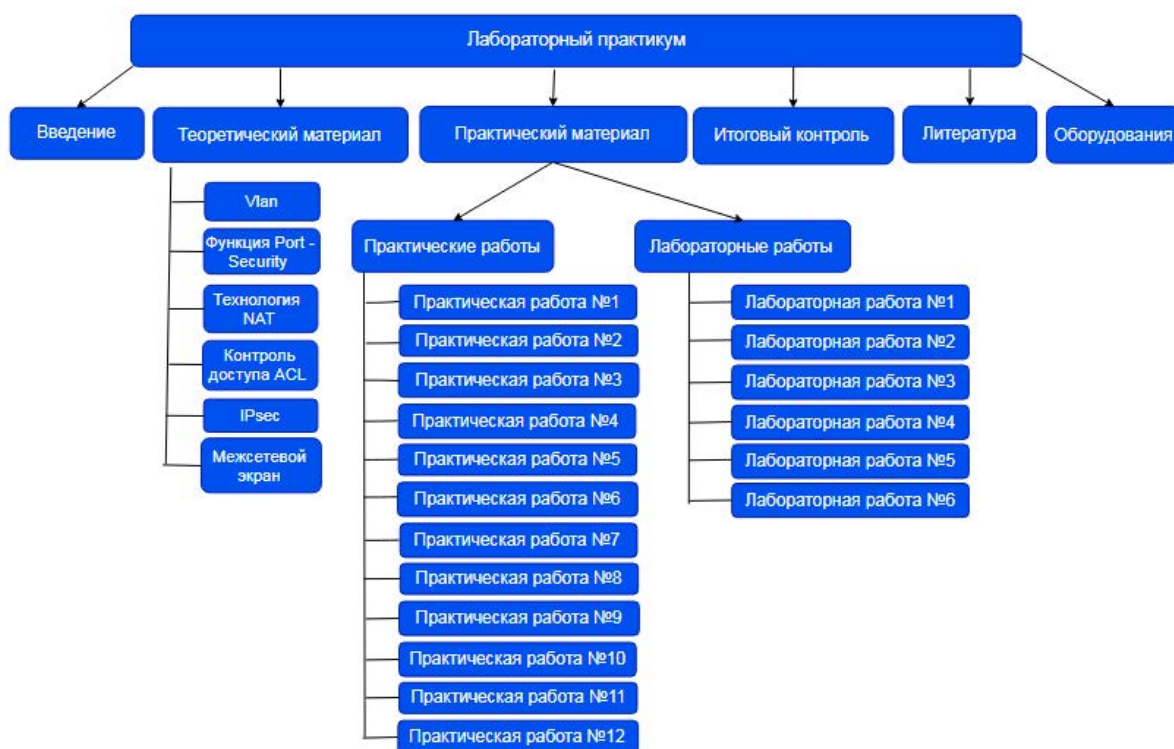


Рисунок 6 — Схема структуры электронного учебного пособия

Раздел «Введение» содержит информацию о дисциплине в обучении, педагогический адрес, а также знания, умения и навыки, необходимые для изучения дисциплины.

В разделе «Теоретического материала» в соответствии с рабочей программой по дисциплине «Безопасность компьютерных сетей» содержится теоретический материал из нескольких тем:

1. VLAN. Описывается технология VLAN, для чего нужен VLAN. Рассмотрены примеры использования VLAN.

2. Функция Port-Security. Рассмотрены основные определения, способы введения ограничений на MAC адреса, и для чего она используется.

3. Технология преобразования сетевых адресов (NAT). Дано определение NAT, показаны диапазоны адресов. Описано использование для NAT специфической терминологии для узлов в Intranet.

4. Контроль доступа Access List Control (ACL). Дано определение, описан функционал ACL, типы ACL. Рассмотрены виды ACL и настройка.

5. IPsec. Приведено определения IPsec, особенности протокола IPsec и какие важные функции выполняет протокол IPsec.

6. Межсетевой экран. Описаны основные задачи, какие имеет названия межсетевой экран. Свойства экрана, преимущества и недостатки межсетевого экрана.

В разделе «Практический материал» содержится практические и лабораторные работы в соответствии с рабочей программой по дисциплине «Безопасность компьютерных сетей» в лабораторном практикуме были включены 12 практических работ и 6 лабораторных работ. Первые 6 предусматривают пошаговое выполнения задания, работы с 7 по 12 предполагают самостоятельное выполнения заданий, также содержат контрольные задания необходимые для допуска к итоговому контролю. К практическим работам прилагаются методические указания, в которых описывается цель выполнения работ. Описание практических работ представлено ниже.

Практическая работа № 1 «Изучение функции коммутатора port-security». Целью практической работы является изучение функции коммутатора port-security. Практическая работа предполагает изучение функции port-security, позволяющая указать MAC-адреса хостов, которым разрешено передавать данные через порт и обезопасить сеть от атак направленных на переполнение таблицы коммутации. Задание на практическую работу: Требуется построить соответствующий проект в Cisco Packet Tracer, по приведённой топологии сети. Настроить пошагово функцию на коммутаторах.

Практическая работа № 2 «Изучение технологии виртуальных локальных сетей VLAN».

Целью практической работы является изучить основы работы механизма VLAN и отработать навык его конфигурирования.

В практической работе нужно продемонстрировать конфигурацию механизма VLAN и основы работы с коммутаторами.

Задание на практическую работу: Требуется построить соответствующий проект в Cisco Packet Tracer, по приведённой топологии, а в таблице указана схема адресация и схема назначения портов. Произвести настройку VLAN'ы.

Практическая работа № 3 «Списки управления доступом ACL».

Целью практической работы является изучить основы работы списка управления доступом ACL и отработать навык его конфигурирования.

В практической работе необходимо построить соответствующий проект в Cisco Packet Tracer, по приведённой топологии сети. Произвести настройку стандартного списка доступа ACL.

Практическая работа № 4 «Преобразование сетевых адресов NAT».

Целью практической работы является изучить основы работы списка управления доступом ACL и отработать навык его конфигурирования.

В ходе практической работы: требуется построить соответствующий проект в Cisco Packet Tracer, по приведенной топологии сети. Настроить стандартный список доступом ACL.

Практическая работа № 5 «Конфигурирование и проверка IPsec VPN между двумя пунктами с помощью интерфейса командной строки».

В ходе практической работы: требуется построить соответствующий проект в Cisco Packet Tracer, топология сети включает три маршрутизатора. Ваша задача заключается в том, чтобы настроить маршрутизаторы R1 и R3 для поддержки сети site-to-site IPsec VPN (при передаче трафика между соответствующими локальными сетями). Туннель IPsec VPN проходит от маршрутизатора R1 к маршрутизатору R3 через R2. Маршрутизатор R2 играет роль транзитного узла и не имеет информации о VPN. IPSec обеспечивает безопасную передачу конфиденциальной информации по незащищенным сетям.

Практическая работа № 6 «Настройка межсетевого экрана Cisco ASA 5505».

Целью практической работы является изучение основ работы межсетевого экрана Cisco ASA 5505 и отработать навык его конфигурирования.

Работа предполагает построение соответствующего проекта в Cisco Packet Tracer. Дан внешний статический IP адрес, используются интерфейс Ethernet0/0 для Wide Area Network (WAN). Физический интерфейс Ethernet0/1 будет использован для подключения всех внутренних сетевых устройств. Устройства сети будут находиться в VLAN 5. Настроить Cisco ASA так, чтобы она автоматически выдавала IP-адреса рабочим станциям по протоколу DHCP. Настроим NAT (PAT) в направлении внутренняя сеть — внешняя сеть.

Практическая работа № 7 «Изучение функции коммутатора port-security».

Работа предполагает изучение функции коммутатора port-security, позволяющие обезопасить сеть от атак.

В ходе практической работы нужно установить порты на всех switch (SW) с fa0/1 — fa0/2 в режим access. Активировать port-security на всех портах SW, смотрящие в сторону конечных устройств. Установить максималь-

ное количество secure-mac на портах равное двум. Установить динамическое определение secure-mac. Показать результат о проделанной работе.

Практическая работа № 8 «Изучение технологии виртуальных локальных сетей VLAN».

Целью практической работы является изучение основы работы механизма VLAN. В ходе практической работы необходимо настроить пользовательские порты в режиме access в соответствии со схемой. Произвести настройку Ethernet интерфейсов персональных компьютеров. Настроить VLAN'ы на коммутаторах. Проверить наличие связи в сети. Результаты о проделанной работе показать преподавателю.

Практическая работа № 9 «Преобразование сетевых адресов NAT».

Работа предполагает изучение преобразование сетевых адресов NAT. В ходе практической работы необходимо активировать пользовательские порты на S1 и S2 и на R1 и R2. Произвести настройку Ethernet интерфейсов персональных компьютеров и IP-адресов для интерфейсов управления на S1 и S2. Настроить статический NAT между R1 и R2. Результаты о проделанной работе показать преподавателю.

Практическая работа № 10 «Списки управления доступом ACL».

Работа предполагает изучение работы списка управления доступом ACL. В ходе практической работы необходимо активировать пользовательские порты на router (R1) и R2 и на S2 и S3. Произвести базовую настройку Ethernet интерфейсов персональных компьютеров и интерфейсов управления на S2 и S3. Создать список, который разрешает трафик от локальной сети компьютеров PC4 и PC5 в локальную сеть компьютера PC1 и запрещает трафик от локальной сети компьютеров PC2 и PC3 в локальную сеть компьютера PC1.

Выполнить проверку с помощью команды ping с PC1 на PC5 и PC4 и с PC1 на PC2 и PC3. Результаты о проделанной работе показать преподавателю.

Практическая работа № 11 «Конфигурирование и проверка IPsec VPN между двумя пунктами с помощью интерфейса командной строки».

В ходе практической работы: требуется построить соответствующий проект в Cisco Packet Tracer, топология сети включает три маршрутизатора. Ваша задача заключается в том, чтобы настроить маршрутизаторы R1 и R3 для поддержки сети site-to-site IPsec VPN (при передаче трафика между соответствующими локальными сетями. Туннель IPsec VPN проходит от маршрутизатора R1 к маршрутизатору R3 через R2. Маршрутизатор R2 играет роль транзитного узла и не имеет информации о VPN. IPsec обеспечивает безопасную передачу конфиденциальной информации по незащищенным сетям.

Практическая работа № 12 «Настройка межсетевого экрана Cisco ASA 5505».

Целью практической работы является изучение работы межсетевого экрана Cisco ASA 5505 и конфигурации. В ходе практической работы необходимо активировать пользовательские порты на R1 и S1. Настроить Ethernet интерфейсы персональных компьютеров. Настроить сетевые интерфейсы PC1, PC2, PC3, PC4. Создать VLAN'ы согласно топологии сети.

Произвести базовую настройку межсетевого экрана Cisco ASA 5505. Результаты о проделанной работе показать преподавателю.

Как уже говорилось выше, в разделе практический материал содержится 6 лабораторных работ. Выполнение лабораторной работы начинается с ознакомления с оборудованием, на котором будет выполняться работа.

Лабораторная работа № 1 «Изучение функции коммутатора port-security».

Работа предполагает изучение функции коммутатора port-security, позволяющие обезопасить сеть от атак.

В ходе лабораторной работы нужно установить порты на всех SW с fa0/1 — fa0/2 в режим access. Активировать port-security на всех портах SW, смотрящие в сторону конечных устройств. Установить макс. количество

secure-mac на портах равное двум. Установить динамическое определение secure-mac. Показать результат о проделанной работе.

Лабораторная работа № 2 «Изучение технологии виртуальных локальных сетей VLAN».

Целью лабораторной работы является изучение основы работы механизма VLAN. В ходе лабораторной работы необходимо настроить пользовательские порты в режиме access в соответствии со схемой. Произвести настройку Ethernet интерфейсов персональных компьютеров. Настроить VLAN'ы на коммутаторах. Проверить наличие связи в сети. Результаты о проделанной работе показать преподавателю.

Лабораторная работа № 3 «Преобразование сетевых адресов NAT».

Работа предполагает изучение преобразование сетевых адресов NAT.

В ходе лабораторной работы необходимо активировать пользовательские порты на S1 и S2 и на R1 и R2. Произвести настройку Ethernet интерфейсов персональных компьютеров и IP-адресов для интерфейсов управления на S1 и S2. Настроить статический NAT между R1 и R2. Результаты о проделанной работе показать преподавателю.

Лабораторная работа № 4 «Списки управления доступом ACL».

Работа предполагает изучение работы списка управления доступом ACL.

В ходе лабораторной работы необходимо активировать пользовательские порты на R1 и R2 и на S2 и S3. Произвести базовую настройку Ethernet интерфейсов персональных компьютеров и интерфейсов управления на S2 и S3. Создать список, который разрешает трафик от локальной сети компьютеров PC4 и PC5 в локальную сеть компьютера PC1 и запрещает трафик от локальной сети компьютеров PC2 и PC3 в локальную сеть компьютера PC1.

Выполнить проверку с помощью команды ping с PC1 на PC5 и PC4 и с PC1 на PC2 и PC3. Результаты о проделанной работе показать преподавателю.

Лабораторная работа №5 «Конфигурирование и проверка IPsec VPN между двумя пунктами с помощью интерфейса командной строки».

В ходе лабораторной работы: требуется построить соответствующий проект в Cisco Packet Tracer, топология сети включает три маршрутизатора. Ваша задача заключается в том, чтобы настроить маршрутизаторы R1 и R3 для поддержки сети site-to-site IPsec VPN (при передаче трафика между соответствующими локальными сетями. Туннель IPsec VPN проходит от маршрутизатора R1 к маршрутизатору R3 через R2. Маршрутизатор R2 играет роль транзитного узла и не имеет информации о VPN. IPsec обеспечивает безопасную передачу конфиденциальной информации по незащищенным сетям.

Практическая работа № 6 «Настройка межсетевого экрана Cisco ASA 5505».

Целью лабораторной работы является изучение работы межсетевого экрана Cisco ASA 5505 и конфигурации.

В ходе выполнения лабораторной работы необходимо активировать пользовательские порты на R1 и S1. Настроить Ethernet интерфейсы персональных компьютеров. Настроить сетевые интерфейсы PC1, PC2, PC3, PC4. Создать VLAN'ы согласно топологии сети. Произвести базовую настройку межсетевого экрана Cisco ASA 5505. Результаты о проделанной работе показать преподавателю.

Раздел «Итоговый контроль» представляет собой самостоятельное выполнения заданий по вариантам. Каждый вариант содержит по 3 задания, и дана общая топология сети для всех вариантов.

В разделе «Литература» написаны учебные пособия и книги по дисциплине «Безопасность компьютерных сетей», которые помогут освоить дисциплину.

Раздел «Оборудование». Описывается лаборатория, компьютерный класс, и весь технический парк на котором будет производиться работы по обучению студентов и подготовки их к WorldSkills Russia.

Технопарк оснащён следующим оборудованием:

- маршрутизаторы Cisco 2911 (количество 6);
- маршрутизаторы Cisco 2811 (количество 9);
- коммутаторы Cisco Catalyst 2960 (количество 9);
- межсетевые экраны Cisco ASA 5505 (количество 6);
- блейд-система HP c7000;
- сервер HP ProLiant BL 460c G7 2x 5675;
- консольный сервер;
- 12 рабочих мест;
- IP-телефоны Cisco CP-7961G (количество 6).

Маршрутизатор Cisco 2911/K9 — это устройство нового поколения, относящееся к семейству ISR G2. Модель позволяет создавать безопасное широкополосное подключение к сети, производить передачу мультимедийных данных, видео, осуществлять беспроводную связь, а также применять множество дополнительных функций при минимальном уровне затрат на приобретение и содержание.

Маршрутизатор Cisco 2911/K9 со встроенными сетевыми сервисами на 3 порта идеально подходит для создания сетей малых и средних организаций и предприятий. Модель имеет 512 Мб встроенной и 526 Мб флеш-памяти, возможность поддержки PoE на портах 10/100/1000 Ethernet, а также поддержку протокола VPN и туннелирования для осуществления надежной и безопасной передачи при построении удаленных VPN сетей.

Маршрутизатор Cisco 2811 — маршрутизатор с интеграцией сервисов, обеспечивающий все потребности небольших офисов и филиалов (до 36 рабочих мест) в современных коммуникациях.

Может выполнять функции:

- маршрутизатора доступа и маршрутизатора локальной сети;
- центра IP-телефонии и голосовой почты (в вариантах Voice bundle и Voice Security bundle);

- интегрированного решения для обеспечения безопасности (в вариантах Security bundle и Voice Security bundle);
- межсетевого экрана;
- систему предотвращения вторжений;
- шифрования и создания VPN-туннелей;
- система Cisco NAC и фильтрация по Uniform Resource Locator (URL);

Коммутатор Cisco Catalyst 2960 — линейка ведущих продуктов среди коммутаторов второго уровня. Эти коммутаторы позволяют снизить совокупную стоимость владения при развертываниях с использованием IP-телефонов Cisco, точек доступа к беспроводной сети (WLAN) Cisco Aironet или других устройств, совместимых с IEEE 802.3af. Технология PoE позволяет устранить потребность в обеспечении питания устройств с поддержкой PoE от сети электропитания и исключить затраты на дополнительные электрические кабели, которые в противном случае необходимы при развертываниях IP-телефонов и сетей WLAN. Их использование позволяет упростить эксплуатацию ИТ-инфраструктуры, повысить уровень безопасности бизнес-процессов, обеспечить устойчивую работу сети, а также предоставить пользователям возможность работы в «сетях без границ».

Каждый спаренный порт каскадирования состоит из одного порта Ethernet RJ-45 и одного порта GE для подключения SFP, при этом активен может быть только один из двух портов, возможность подключения настольных компьютеров к 24 портам Fast Ethernet, широкий набор программных средств, обеспечивающих простоту эксплуатации, защиту бизнес-процессов, устойчивость и работу в «сетях без границ».

Межсетевой экран Cisco ASA 5505 — современное многофункциональное устройство для защиты локальных сетей от внешних атак и вторжений. Основная функция межсетевого экрана Cisco (файрвол) — защита сети от вторжений, вирусов, спама, шпионских программ, контентная фильтрация трафика пользователей. Построенные на базе аппаратной платформы сетевые

экраны Cisco ASA обеспечивают высокую надежность, производительность в задаче обеспечения безопасности локальной сети от внешних атак. Брандмауэр Cisco ASA 5505 — это производительный файрвол, обеспечивающий до 150 Мбит/с транзитного трафика. Он работает на скорости до 100 Мбит/с при организации VPN доступа. В первую очередь устройство ориентировано на обеспечение сетевой безопасности пользователей сегмента малого бизнеса в силу простоты эксплуатации и низкой цены. Помимо функций межсетевого экрана ASA 5505 выполняет NAT трансляцию для совместного доступа пользователей к сети Интернет, является IPSec VPN сервером для безопасного удаленного доступа к локальным ресурсам. Огромным преимуществом является наличие встроенного 8-и портового коммутатора, при этом 2 порта имеют поддержку PoE, что обеспечивает простоту подключения IP камеры, WI-FI точки доступа или IP-телефона.

IP-телефон Cisco — это полнофункциональный телефон, который предоставляет возможность голосовой связи с использованием тех же сетей для передачи данных, которые используются компьютерами. Этот телефон по своим функциональным возможностям похож на обычный аналоговый телефон и позволяет выполнять и получать телефонные вызовы. Кроме того, он поддерживает функции, которыми должен обладать телефон, например: быстрый набор, повторный набор, перевод вызова, вызов в режиме конференцсвязи, и др.

HP BladeSystem c7000 — это самое вместительное шасси для развертывания блейд-серверов от Hewlett Packard. Его высота составляет 10 юнитов, что позволяет развертывать до 8 четырехпроцессорных или до 16 двухпроцессорных серверов со всеми необходимыми модулями питания и охлаждения. Среди совместимых блейд-серверов имеются как доступные по цене варианты, так и высокопроизводительные решения на базе новейших процессоров Intel Xeon/AMD Opteron.

Питание осуществляется 6 источниками электроэнергии, при мощности каждого 2250 Вт. Поддерживается 8 коммуникационных модулей стандарта

FC (4 Гб Fiber Channel), Ethernet (Gigabit и 10 Гб Ethernet) и Infiniband (4x DDR InfiniBand).

Удаленное управление осуществляется с помощью Insight Display и/или двух Onboard Administrator (в стандартную комплектацию входит только один).

Для эффективного управления HP BladeSystem c7000 в состав блейд-системы включены специальные средства, с помощью которых системный администратор может визуальнo контролировать систему, получая наглядное представление о текущем положении дел для наиболее точной настройки параметров электропитания и системы охлаждения.

При разработке HP BladeSystem c7000 было уделено особое внимание надежности. На аппаратном уровне это выражается в дублировании критически важных компонент и возможности их горячей замены. На программном же уровне количество решений куда больше и варьируется в зависимости от используемых блейд-серверов

Сервер HP ProLiant BL460c G7 выполнен в конструктиве половинной высоты. В него может быть установлено до 2-х процессоров Intel Xeon 5500 или 5600Series. Сервер использует до двух жестких дисков с возможностью горячей замены. Объем памяти до 384 Гб, 12 слотов DIMM. HP ProLiant BL460c G7 имеет интегрированный двухпортовый адаптер FlexFabric 10 Гб/с. Сервер гибко управляется благодаря включенному в поставку Advanced iLO 3-й версии, со значительно увеличенной в сравнении с предыдущей версией производительностью.

Консольный сервер — это специализированный сетевой компьютер, имеющий один сетевой Ethernet порт и большое количество последовательных портов, для обеспечения управления с одного центрального компьютера, использующего TCP/IP сеть, возможности последовательного доступа к консольным портам различных устройств [8]. Централизованный консольный контроль достигается с использованием Telnet через Ethernet LAN/WAN соединение. Как запасной вариант управления, когда прямое управление через

Ethernet сеть невозможно, используется модемное соединение. В этом случае управляющий компьютер связывается через модем с модемом, подключенным к консольному порту устройства.

Лаборатория БУ «Югорский политехнический колледж» оснащена монтажной стойкой (рисунок 7) со следующим оборудованием:

- маршрутизатор Cisco 2911 (количество 6);
- маршрутизатор Cisco 2811 (количество 9);
- коммутатор Cisco Catalyst 2960 (количество 9);
- межсетевой экран Cisco ASA 5505 (количество 6).

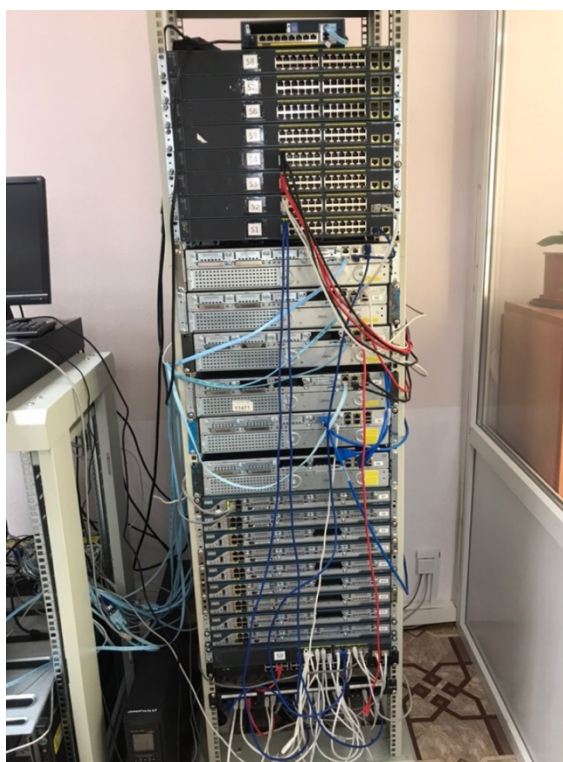


Рисунок 7 — Монтажная стойка

Так же лаборатория оснащена блейд-системой HP c7000, с одним сервером HP ProLiant BL 460c G7 2x 5675 и консольным сервером для подключения по СОМ-портам.

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 [13].

В лабораторном стенде БУ «Югорский политехнический колледж» используется Unshielded twisted pair (UTP) кабель Ethernet для технологии 100 Base-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 [7]. 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 15 кабеля используются коннекторы. Для витой пары пятой категории используют коннекторы типа RJ-45 (24AWG). В его разьеме 8 позиций, в которые вставляется 8 проводников [19].

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

2.4 Интерфейс электронного учебного пособия

Лабораторный практикум реализовано в формате HTML и открывается запуском файла index.html. Стартовая страницу, представлена на рисунке 8.

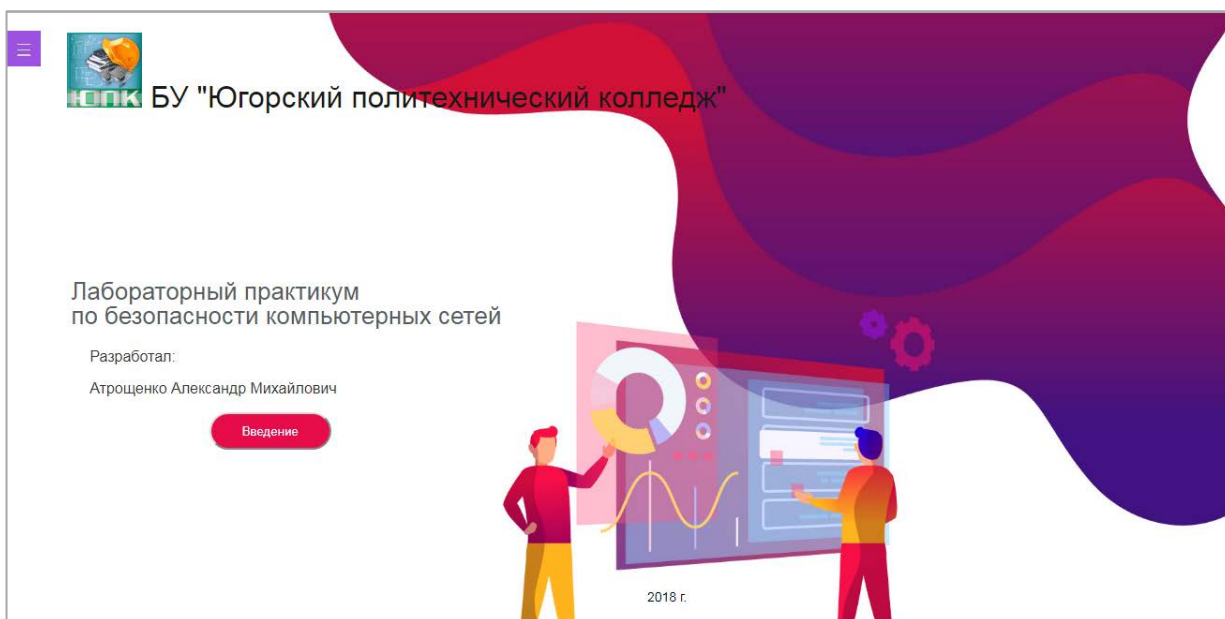


Рисунок 8 — Стартовая страница

На странице располагается название дисциплины, сверху слева кнопка меню, которая присутствует во всех разделах. При нажатие кнопки меню, выпадает список с разделами которые содержатся в практикуме, а также кнопка «Введение», при нажатие на которую начинается работа в лабораторном практикуме.

При выборе фона практикума 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.

Навигация по разделам практикума осуществляется с помощью меню, которая располагается в левом верхнем углу (рисунок 9).

Все переходы по разделам осуществляются непосредственно из главного меню.

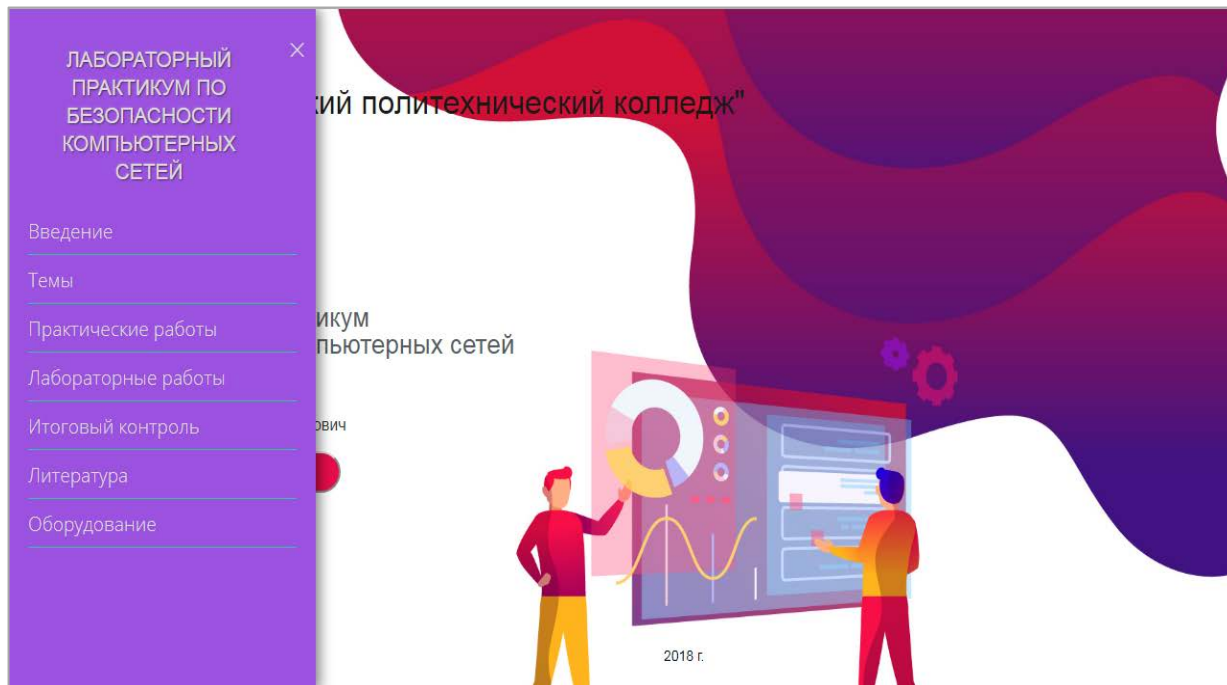


Рисунок 9 — Меню

Меню лабораторного практикума содержит 7 разделов:

1. Введение.
2. Темы.
3. Практические работы.
4. Лабораторные работы.
5. Литература.
6. Итоговый контроль.
7. Оборудование.

Раздел «Введение» носит информационный характер, в нем описывается для чего нужен лабораторный практикум, требования к студентам и краткое содержание практикума на рисунке 10.

Для удобства пользования практикума предусмотрены кнопки навигации «Назад», «Далее», «В начало». Помимо этого переход между

лабораторными работами, как с помощью меню, так и при использовании вспомогательных кнопок (рисунок 11).

Введение:

Вы начали работать в лабораторном практикуме по дисциплине "Безопасность компьютерных сетей"

Лабораторный практикум предназначен для:

Студентов всех форм обучения по направлению подготовки 09.02.06 «Сетевое и системное администрирование» базовой подготовки, по профилю «Сетевой и системный администратор» в бюджетном учреждении «Югорского политехнического колледжа»

Требования к студентам для освоения лабораторного практикума:

- быть зачисленным в сетевой академии Cisco;
- знать базовые знания о локальных сетях;
- знать IPv4 и уметь его настраивать на ОС Windows;
- знать технологию Fast Ethernet;
- уметь работать со средами виртуализации Hyper-V, VMware.

В лабораторном практикуме изложен материал по следующим темам:

- VLAN;
- функция Port Security;
- технология преобразования сетевых адресов (NAT);
- контроль доступа ACL (Access List Control);
- IPsec;
- межсетевой экран.

Рисунок 10 — Введение



Рисунок 11 — Кнопки навигации

В разделе «Темы» при наведении на интересующую тему раскрывается выпадающий список (рисунок 12) состоящий из перечня практических и лабораторных работ относящихся к данной теме, а при нажатии на определённую тему, переходим на страницу с кратким теоретическим материалом по данной теме, там раскрываются основные понятия и примеры использования (рисунок 13).



Рисунок 12 — Раскрытое меню

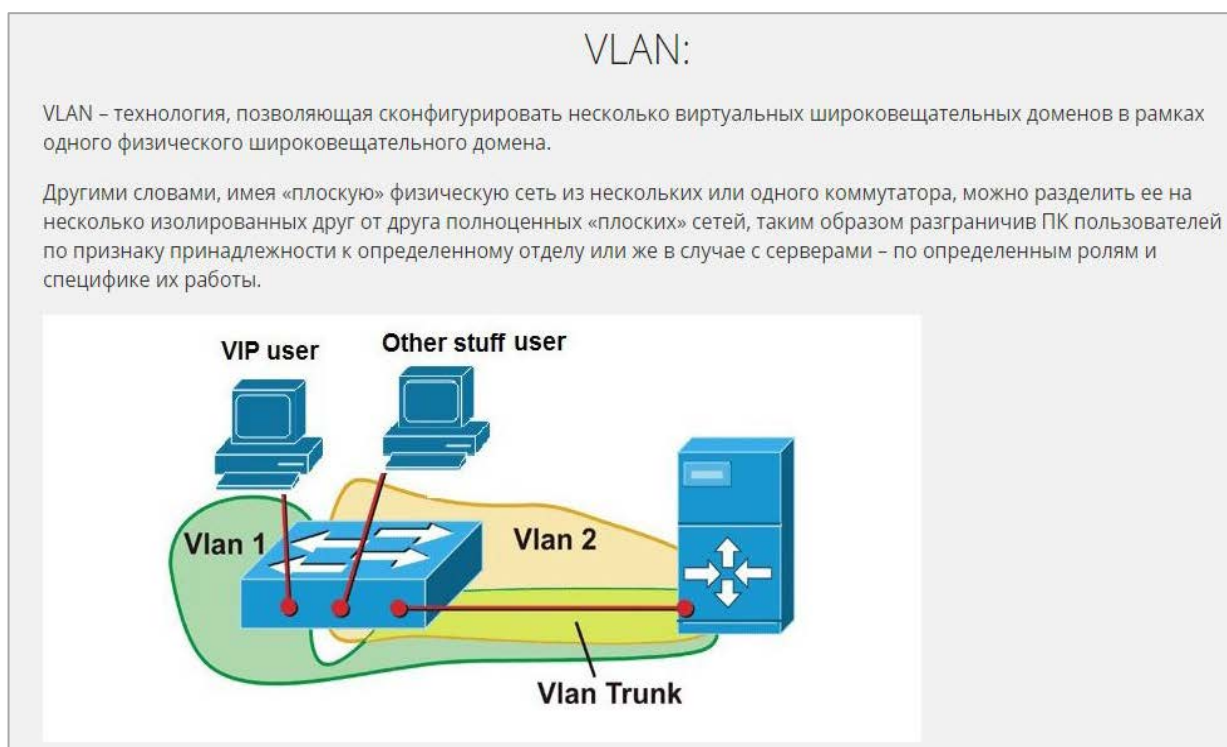


Рисунок 13 — Теоретический материал

Для удобства в конце кратких теоритических сведений располагаются кнопки перехода к практической работе и к возвращению в раздел «Темы» (рисунок 14).

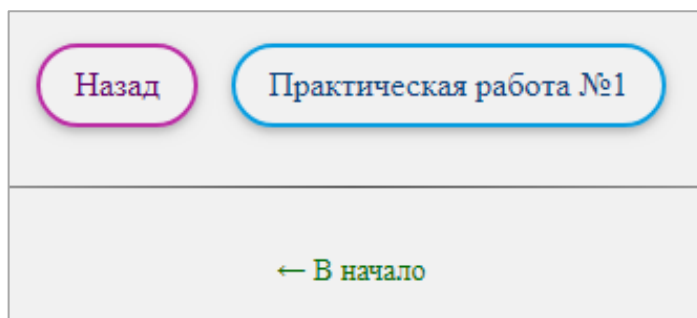


Рисунок 14 — Кнопки перехода

В разделе «Практические работы» содержится 12 практических работ (рисунок 15), которые условно можно разделить на два блока. Первый блок содержит работы с пошаговой инструкцией (работы с 1 по 6). Примеры практической представлены на рисунках 16 и 17. Во втором блоке работы, предполагающие самостоятельное выполнение, в которых есть контрольные задания для самостоятельного выполнения (работы 7 по 12). Пример работы представлен на рисунках 18 и 19.

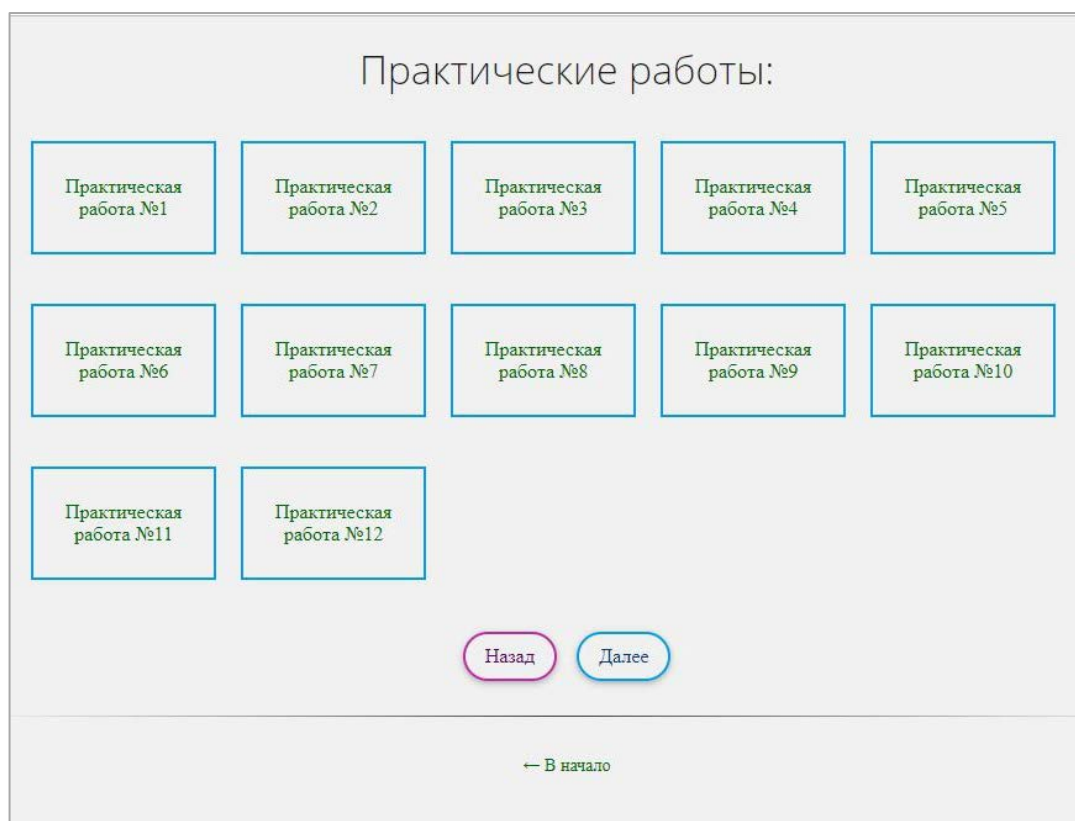


Рисунок 15 — Практические работы

Практическая работа №2:

Изучение технологии виртуальных локальных сетей VLAN

Цель работы:

Изучить основы работы механизма VLAN и отработать навык его конфигурирования.

Задачи:

Требуется соединить физическую сеть в соответствии со схемой сети или построить соответствующий проект в Cisco Packet Tracer. приведена топология сети, а в таблице указана схема адресация и схема назначения портов

Топология сети

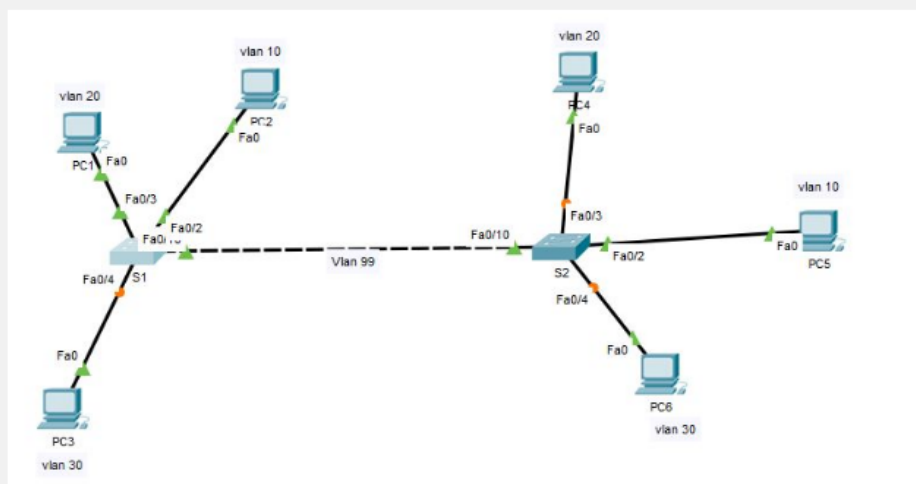


Рисунок 16 — Задачи и топология сети практические работы

Шаг 1: Защита комплексным паролем

Заходим на S1 и S2 открываем CLI

Вводим команды:

```
Switch>enable
Switch#configure terminal
Switch(config)#enable secret Pa$$w0rd
Switch(config)#line console 0
Switch(config-line)#password Pa$$w0rd
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line vty 0 15
Switch(config-line)#password Pa$$w0rd
Switch(config-line)#login
Switch(config-line)#exit
```

Рисунок 17 — Пошаговая инструкция

Практическая работа №7:

Изучение функции коммутатора port - security

Цель работы:

Изучить функцию коммутатора port - security, позволяющую обезопасить сеть от атак направленных на переполнение таблицы коммутации.

Задачи:

1. Установить порты на всех SW с fa0/1 – fa0/2 в режим access.
2. Активировать port-security на всех портах SW, смотрящие в сторону конечных устройств.
3. Установить макс. количество secure-mac на портах равное двум.
4. Установить динамическое определение secure-mac.
5. Проверить результат.
6. Результаты о проделанной работе показать преподавателю и обосновать результаты.

Топология сети

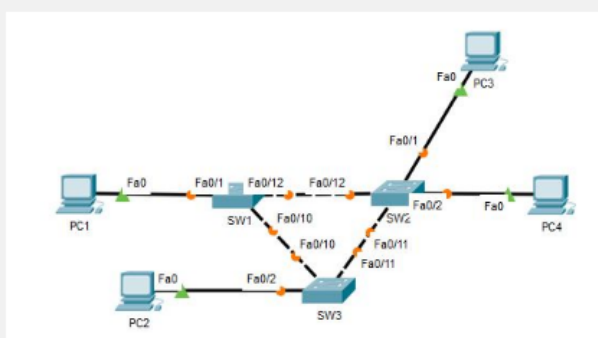


Рисунок 18 — Практическая работа без инструкции

Задания для самостоятельной работы

Для организации «название организации выбираем сами» технического парка, который состоит из 5 ПК, 1 коммутаторов (Cisco Catalyst WS-C2960-24PC-L) и Роутера (Router Cisco 2811). Необходимо построить сеть с отделами Бухгалтерия (1ПК), Директорат(1ПК), Отдел продаж (2ПК)и отдел логистики (1пк).Необходимо организовать VLAN для каждого отдела.

[Назад](#)

[Лабораторная работа №1](#)

Рисунок 19 — Задания для самостоятельной работы

Каждая тема практикума содержит одну практическую работу из первого блока и одну практическую работу из второго блока, помимо этого в тему так же входит и лабораторная работа. Для осуществления перехода от простой практической работы к сложной, и от сложной к лабораторной работе, в конце каждой практической работы расположена кнопка позволяющая осуществлять переход (рисунки 20 и 21).

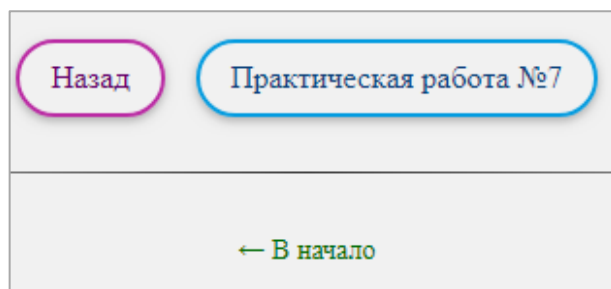


Рисунок 20 — Кнопка перехода от простой практической работы к сложной

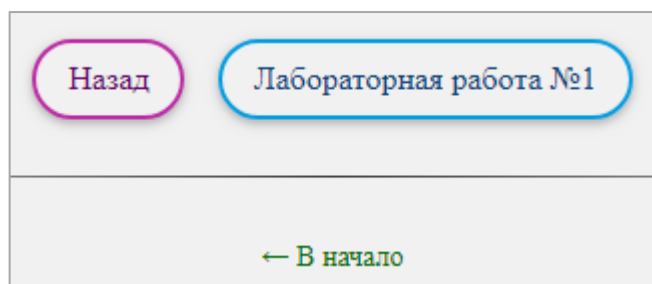


Рисунок 21 — Кнопка перехода с практической работы к лабораторной работе

Раздел «Лабораторные работы» содержит в себе 6 работ (рисунок 22).

Все работы выполняются на лабораторных стендах на реальном оборудовании, под руководством преподавателя, дана только топология сети и поставлены задачи (рисунок 23).

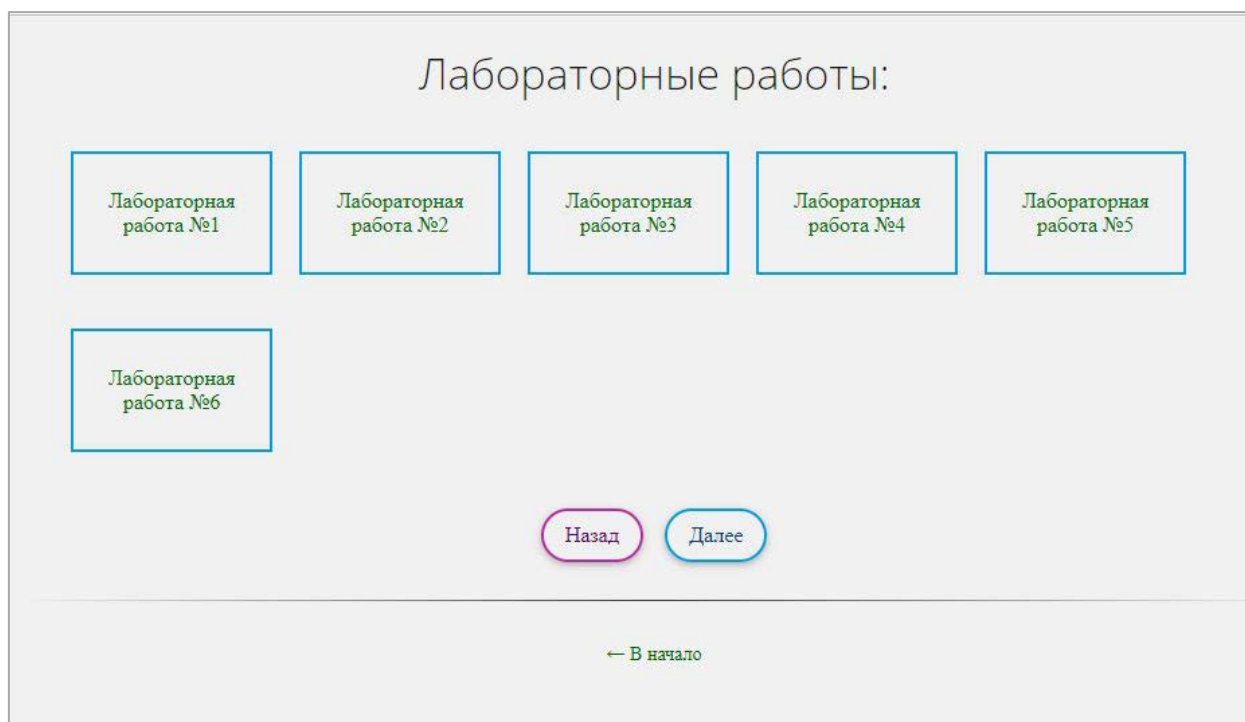


Рисунок 22 — Лабораторные работы

Лабораторная работа №1: Изучение функции коммутатора port - security

Цель работы:

Изучить функцию коммутатора port - security, позволяющую обезопасить сеть от атак направленных на переполнение таблицы коммутации.

Задачи:

1. Требуется построить соответствующий проект в лаборатории на данном оборудовании.
2. Установить порты на всех SW с fa0/1 – fa0/2 в режим access.
3. Активировать port-security на всех портах SW, смотрящие в сторону конечных устройств.
4. Установить макс. количество secure-mac на портах равное двум.
5. Установить динамическое определение secure-mac.
6. Проверить результат.
7. Результаты о проделанной работе показать преподавателю и обосновать результаты.

Топология сети

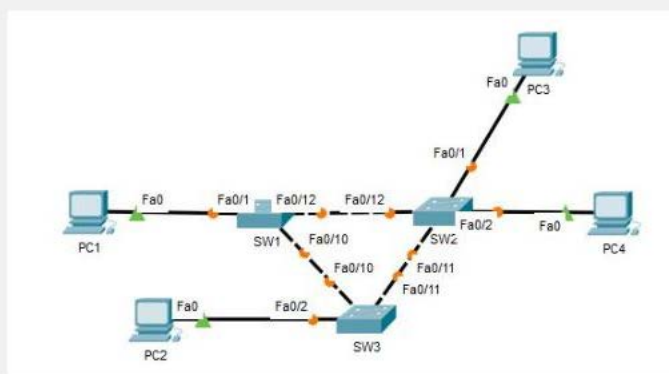


Рисунок 23 — Лабораторная работа

Раздел «Итоговый контроль». Суть данного раздела заключается в проверке знаний обучающихся по лабораторному практикуму (рисунок 24). В раздел содержится 6 различных вариантов задания отличавшихся по уровню сложности (рисунок 25). Каждый вариант содержит в себе 3 задания. Сделана общая топология сети для всех вариантов. Все задания выполняются в специализированной программе Cisco Packet Tracer. По окончании выполнения задания, обучающиеся сдают работу преподавателю для проверки.

Итоговый контроль:

Итоговый контроль представляет собой самостоятельное выполнения заданий по вариантам. Каждый вариант содержит в себе по 3 задания и общую топологию сети.

Топология сети

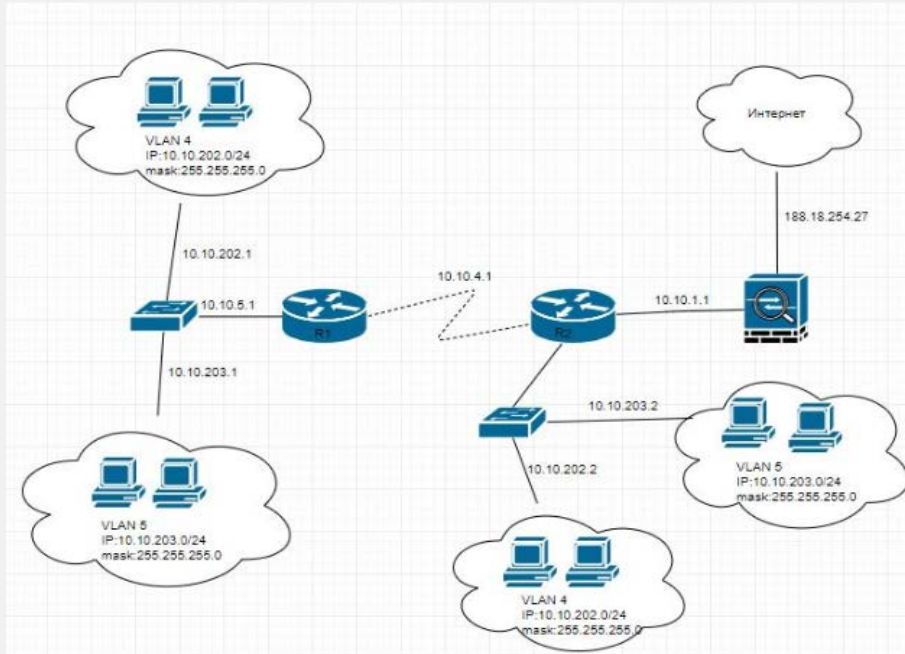


Рисунок 24 — Топология сети итогового контроля

Вариант 1

1. На всех устройствах настроить сетевую адресацию ,предварительно рассчитав сеть по классу С на 8 ПК(кроме межсетевого экрана ASA)
2. Создать VLAN (согласно схеме)
3. Задать имя VLAN

Вариант 2

1. На всех устройствах настроить сетевую адресацию ,предварительно рассчитав сеть по классу А на 8 ПК(кроме межсетевого экрана ASA)
2. Провести базовую настройку коммутаторов
3. Настроить для коммутаторов SW1 и SW2 функцию Port Security

Вариант 3

1. На всех устройствах настроить сетевую адресацию ,предварительно рассчитав сеть по классу В на 8 ПК(кроме межсетевого экрана ASA)
2. Провести базовую настройку роутеров
3. Настроить статический NAT между R1 и R2

Вариант 4

1. На всех устройствах настроить сетевую адресацию ,предварительно рассчитав сеть по классу А на 8 ПК(кроме межсетевого экрана ASA)
2. Создать VLAN (согласно схеме)
3. Задать имя VLAN

Рисунок 25 — Варианты с заданиями

В лабораторном практикуме для удобства бы включен раздел «Литература», состоит из двух видов литературы (рисунок 26).

Целью данного раздела является информирования обучающихся об основной литературе, по которой проходят лекционные занятия по дисциплин «Безопасность компьютерных сетей» и дополнительной литературы, по которой они могут учиться самостоятельно, для получения дополнительных знаний.

В разделе содержится информация об трех учебных пособиях и 4 книгах по данной тематике.

Литература:

Основная литература:

Учебное пособие В. В. Баринов, И. В. Баринов, А. В. Пролетарский, А. Н. Пылькин «Компьютерные сети»;
книга Бирюков А.А. «Информационная безопасность. Защита и нападение. 2-е изд.»;
книга Котухов М. М., Кубанков А. Н., Калашников А. О. «Информационная безопасность».

Дополнительная литература:

Учебное пособие Андрончик, А. Н. «Сетевая защита на базе технологий фирмы Cisco Systems»;
книга Бен Пайпер «Администрирование сетей Cisco»;
книга Мелехина В.Ф., Павловского Е.Г. «Вычислительные машины, системы и сети»;
учебник Олифер В.Г., Олифер Н.А.« Безопасность компьютерных сетей».

[Назад](#)

[← В начало](#)

Рисунок 26 — Раздел литература

Раздел «Оборудование». В начале раздела для ознакомления представлены подтверждающие сертификаты БУ «Югорский политехнический колледж» (рисунок 27), Далее по разделу обучающиеся могут ознакомиться с полным описанием оборудованием, которое есть в лаборатории, с которым обучающиеся столкнутся при выполнении лабораторных работ.

Оборудования:

Технопарк оснащён следующим оборудованием:

- маршрутизаторы Cisco 2911 (количество 6);
- маршрутизаторы Cisco 2811 (количество 9);
- коммутаторы Cisco Catalyst 2960 (количество 9);
- межсетевые экраны Cisco ASA 5505 (количество 6);
- блейд-система HP c7000;
- сервер HP ProLiant BL 460c G7 2x 5675;
- консольный сервер;
- 12 рабочих мест;
- IP-телефоны Cisco CP-7961G (количество 6).

Маршрутизатор Cisco 2911/K9 — это устройство нового поколения, относящееся к семейству ISR G2. Модель позволяет создавать безопасное широкополосное подключение к сети, производить передачу мультимедийных данных, видео, осуществлять беспроводную связь, а также применять множество дополнительных функций при минимальном уровне затрат на приобретение и содержание.



Рисунок 27 — Раздел оборудование

Очень удобный раздел для полного понимания, с каким оборудованием предстоит работать, и в большинстве лабораторных практикумах он отсутствует.

ЗАКЛЮЧЕНИЕ

В результате выпускной квалификационной работы был создан лабораторный практикум «Безопасность компьютерных сетей», который включает в себя теоретический и практический материал.

В ходе проделанной работы были проанализированы 12 учебников, которые показали, что в печатных изданиях содержится не достаточное количество информации по выполнению практических работ.

Таким образом, проанализировав учебную литературу, пришли к следующему выводу — не смотря на то, что данные источники содержат актуальную информации необходимую для изучения дисциплины «Безопасность компьютерных сетей», они не в полной мерной соответствуют содержанию рабочей программы и поэтому данную литературу рекомендуется использоваться в качестве дополнительной литературы. В связи с этим возникла необходимость в создании лабораторного практикума, тематика которого полностью соответствует содержанию рабочей программы и может использоваться в качестве основанного источника информации.

Так же была проанализирована учебная программа по дисциплине «Безопасность компьютерных сетей». В результате анализа была определена структура, содержание и последовательность изучения разделов данной дисциплины. Данная структура легла в основу лабораторного практикума, так же был определен объем часов на изучения каждого раздела дисциплины.

Были рассмотрены средства реализации, приведены примеры шести программ, описаны их достоинства и недостатки, и был выбран самый оптимальный вариант для реализации лабораторного практикума. Наиболее оптимальным вариантом реализации практикума явился формат HTML с использованием таблицы стилей CSS. Для автоматизации набора HTML-кода был использован редактор «Notepad++».

В структуре лабораторного практикума было выделено 6 разделов:

- введение;
- блок теоретического материала;
- блок практического материала;
- итоговый контроль;
- литература;
- оборудования.

В блок теоретического материала входит шесть тем: Vlan, функция port-security, технология преобразования сетевых адресов (NAT), контроль доступа ACL (Access List Control), IPsec, межсетевой экран.

Данные темы полностью соответствуют учебной программе дисциплины.

Блок практического материала вошли 12 практических работ и 6 лабораторных работ, что так же соответствует учебной программе.

Итоговый контроль содержит в себе 6 вариантов заданий отличающихся по уровню сложности.

Таким образом, все задачи решены, цель выпускной квалификационной работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Андрончик А. Н. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс [Текст]: учебное пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков. — Екатеринбург: Урал. ун-т, 2014. — 180 с.
2. Баринов В. В. Компьютерные сети [Текст]: учебник для студ. сред. проф. образования / В. В. Баринов, А. В. Пролетарский, А. Н. Пылькин. — Москва: Академия, 2018. — 192 с.
3. Бирюков А. А. Информационная безопасность защита и нападение. 2-е издание [Текст] / А. А. Бирюков. — Москва: ДМК Пресс, 2017. — 434 с.
4. Википедия [Электронный ресурс]. — Режим доступа — <http://ru.wikipedia.org> (дата обращения: 20.12.2018).
5. Гаврилов М. В. Информатика и информационные технологии [Текст]: учебник / М. В. Гаврилов, В. А. Климов. — 4-е изд., — Москва: Юрайт, 2016. — 383 с.
6. Гордейчик С. В. Безопасность беспроводных сетей [Текст]: учебное пособие / С. В. Гордейчик, В. В. Дубровин. — Москва: ДМК Пресс, 2017. — 288 с.
7. 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: 22.12.2018).
8. Консольный сервер [Электронный ресурс]. — Режим доступа: <http://ru.wikipedia.org> (дата обращения: 25.12.2018).
9. Котухов М. М. Информационная безопасность [Текст]: учебное пособие / М. М. Котухов, А. Н. Кубанков. — Москва: Академия ИБС: МФТИ, 2009. — 195 с.

10. Касперский Крис Компьютерные вирусы изнутри и снаружи [Текст] / Крис Касперский. — Санкт-Петербург: Питер, 2006. — 527 с.
11. Кузин А. А. Компьютерные сети. Практический курс [Текст]: учебное пособие / А. А. Кузин. — Москва: Инфра-М, 2011. — 192 с.
12. Мелехин В. Ф. Вычислительные машины, системы и сети [Текст]: учебник для студ. выш. учеб. заведений / В. Ф. Мелехин, Е. Г. Павловловский. — 3-е изд., стер. — Москва: Академия, 2010. — 560 с.
13. Начальная настройка коммутатора [Электронный ресурс]. — Режим доступа: <https://www.intuit.ru/studies/courses/3591/833/lecture/14253> (дата обращения: 08.01.2019).
14. Олифер В. Г. Безопасность компьютерных сетей [Текст]: учебный курс / В. Г. Олифер, Н. А. Олифер. — Москва: Академия ИБС, 2017. — 643 с.
15. Олифер В. Г. Компьютерные сети: Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. — 4-е изд. — Санкт-Петербург: Питер, 2013. — 944 с.
16. Сетевая академия Cisco [Электронный ресурс]. — Режим доступа: <http://www.netcad.com> (дата обращения: 07.12.2018).
17. Смирнова Е. В. Построение коммутируемых компьютерных сетей [Текст]: учебное пособие / Е. В. Смирнова, А. В. Пролетарский, И. В. Баскаков, Р. А. Федотов. — Москва: Национальный Открытый Университет «ИНТУИТ»: БИНОМ. Лаборатория знаний, 2011. — 367 с.
18. Советов Б. Я. Информационные технологии [Текст]: учебник / Б. Я. Советов, В. В. Цехановский. — 6-е изд., — Москва: Юрайт, 2017. — 261 с.
19. 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: 07.01.2019).
20. Трофимов В. В. Информационные технологии [Текст]: учебник / В. В. Трофимов, О. П. Ильина, В. И. Кияев, Е. В. Трофимова. — Москва: Юрайт, 2016. — 390 с.

21. Таненбаум Э. Компьютерные сети [Текст]: научное издание / Э. Таненбаум, Д. Уэзеролл. — 5-е изд. — Санкт-Петербург: Питер, 2013. — 960 с.
22. Учебная программа по дисциплине «Безопасность компьютерных сетей» [Электронный ресурс]. — Режим доступа: <http://www.yugorskpk.ru/inf/dokumenty> (дата обращения: 03.12.2018).
23. Фороузан Б. А. Криптография и безопасность сетей [Текст]: учебное пособие / А. Н. Берлина. — Москва: Университет Информационных технологий, 2010. — 784 с.
24. ChmBookCreator [Электронный ресурс]. — Режим доступа: https://studwood.ru/1698115/informatika/analiz_programmnogo_obespecheniya_s_ozdaniya_elektronnogo_posobiya (дата обращения: 07.12.2018).
25. eBook Maestro [Электронный ресурс]. — Режим доступа: <http://www.ebookmaestro.com/ru/> (дата обращения: 07.12.2018).
26. eBooksWriter LITE [Электронный ресурс]. — Режим доступа: <https://www.ebookswriter.com> (дата обращения: 07.12.2018).
27. Learning Content Development System [Электронный ресурс]. — Режим доступа: <https://www.microsoft.com/ru-ru/learning/lcds-tool.aspx> (дата обращения: 07.12.2018).
28. Notepad++ [Электронный ресурс]. — Режим доступа: <https://notepad-plus-plus.org/> (дата обращения: 07.12.2018).
29. Profile-edu [Электронный ресурс]. — Режим доступа: <http://www.profile-edu.ru/laboratornyj-praktikum-kakraznovidnostprakticheskogo-zanyatiya.html> (дата обращения: 07.12.2018).
30. TurboSite [Электронный ресурс]. — Режим доступа: <http://turbosite.do-info.ru/page2.html> (дата обращения: 07.12.2018).

ПРИЛОЖЕНИЕ

**Министерство науки и высшего образования 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

И.о. заведующего кафедрой

_____ И. А. Сулова

« ____ » _____ 2018 г.

ЗАДАНИЕ

на выполнение выпускной квалификационной работы бакалавра

студентки 4 курса, группы ЗИБ Атрощенко Александр Михайлович

1. Тема Лабораторный практикум по дисциплине «Безопасность компьютерных сетей» утверждена распоряжением по институту от « ____ » _____ 20 ____ г. № ____.
2. Руководитель Колесникова Юлия Алексеевна, старший преподаватель
3. Место преддипломной практики БУ «Югорский политехнический колледж»
4. Исходные данные к ВКР учебное пособие В. В. Баринов, И. В. Баринов, А. В. Пролетарский, А. Н. Пылькин «Компьютерные сети», книга Бен Пайпер «Администрирование сетей Cisco»
5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов)
 - проанализировать учебно-методическую документацию по дисциплине;
 - проанализировать учебную литературу по дисциплине с целью отбора учебного материала;
 - разработать структуру лабораторного практикума;
 - спроектировать интерфейс лабораторного практикума;
 - наполнить лабораторный практикум учебными материалами.
6. Перечень демонстрационных материалов
Мультимедийная презентация в Microsoft PowerPoint, лабораторный практикум по дисциплине «Безопасность компьютерных сетей»

