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

ЭЛЕКТРОННЫЙ ПРАКТИКУМ «УЧЕБНАЯ ПРАКТИКА ПО ОБЕСПЕЧЕНИЮ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

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: 076

Екатеринбург 2019

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. Суслова
«____» _____ 2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ЭЛЕКТРОННЫЙ ПРАКТИКУМ «УЧЕБНАЯ ПРАКТИКА ПО ОБЕСПЕЧЕНИЮ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

Исполнитель:
обучающийся группы ЗИБ-401С В. А. Толстихина
Руководитель:
ст. преподаватель В. В. Мешков

Нормоконтролер: Н. В. Хохлова

Екатеринбург 2019

АННОТАЦИЯ[H1]

Выпускная квалификационная работа состоит из электронного практикума, содержащего теорию для изучения и повторения, лабораторные работы и блок самоконтроля, пояснительной записки на 50 страницах, содержащей 19 рисунков, 31 источник литературы, а также 2 приложения на 3 листах.

Ключевые слова: ЭЛЕКТРОННЫЙ ПРАКТИКУМ, УЧЕБНАЯ ПРАКТИКА ПО ОБЕСПЕЧЕНИЮ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ЗАЩИТА ИННФОРМАЦИИ.

Толстихина В.А., Электронный практикум «Учебная практика по обеспечению комплексной защиты информации»: выпускная квалификационная работа / В.А.Толстихина Рос. гос. проф-пед. ун-т, Ин-т инж-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2019. — 50 с.

Актуальность данной работы заключается в востребованности современного, структурированного методического обеспечения для проведения учебной практики у студентов специальности 09.02.02 «Компьютерные сети» в рамках среднего профессионального образования.

Таким образом, цель работы: разработать электронный практикум для учебной практики «Обеспечение комплексной защиты информации».

В соответствие с поставленной целью в данной работе определены следующие задачи:

1. Изучить особенности электронных учебных пособий и практикумов, ознакомиться с требованиями, которые к ним предъявляют.
2. Проанализировать литературу и электронные источники по эксплуатации объектов сетевой инфраструктуры.
3. Создать электронный практикум, для учебной практики «Обеспечение комплексной защиты информации»: подобрать материал, разработать задания для входного и итогового контроля обучающихся.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На сегодняшний день почти в каждом образовательном учреждении большое внимание уделяется компьютерному сопровождению профессиональной деятельности обучающихся.

В учебном процессе активно используются различного рода программы (тестирующие, эмуляция, обучающие) по различным дисциплинам и в разных специальностях.

Практика показывает, что применение электронных учебных пособий позволяет повысить успеваемость по изучаемым дисциплинам. Большинство людей воспринимают лучше информацию зрительно. Разнообразные электронные учебные пособия дают возможность каждому обучающемуся независимо от уровня подготовки активно участвовать в процессе образования, индивидуализировать свой процесс обучения, и даже осуществлять самоконтроль.

Почти каждым преподавателем ведется активный процесс по созданию электронных учебных пособий в самых разнообразных формах и их внедрения в учебный процесс.

Электронное пособие можно, например, определить, как совокупность графической, текстовой, цифровой, речевой, музыкальной, видео, фото и другой информации, а также печатной документации пользователя. Электронное издание может быть исполнено на любом электронном носителе, а также опубликовано в компьютерной сети.

Данная тема актуальна, потому что существует огромное количество средств, которыми может пользоваться преподаватель в своей работе, благодаря электронному практикуму преподаватель сможет систематизировать и упростить проведение лабораторных работ и учебных практик, таким образом:

Радиотехнический колледж им. А. С. Попова не исключение. В данном учебном заведении на высоком уровне реализуются специальности компьютер-

ных направлений, но проблема современного, актуального, методического обеспечения для проведения лабораторных работ и учебных практик, является актуальной всегда.

Объектом выпускной квалификационной работы является — процесс обучения студентов среднего профессионального образования (СПО) по специальности 09.02.02 «Компьютерные сети».

Предметом выпускной квалификационной работы являются учебные материалы по профессиональному модулю «Эксплуатация объектов сетевой инфраструктуры».

Цель работы [H2]— разработать электронный практикум для учебной практики УП.03.01 «Учебная практика по обеспечению комплексной защиты информации».

Для достижения поставленной цели необходимо решить следующие задачи:

1. Изучить особенности электронных учебных пособий и практикумов, ознакомиться с требованиями, которые к ним предъявляют.
2. Проанализировать литературу и электронные источники по эксплуатации объектов сетевой инфраструктуры.
3. Создать электронный практикум, для учебной практики «Обеспечение комплексной защиты информации»: подобрать материал, разработать задания для входного и итогового контроля обучающихся.[H3]

1 АНАЛИЗ ЛИТЕРАТУРЫ ПО ЭКСПЛУАТАЦИИ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

1.1 Анализ литературных источников

1.1.1 Анализ основной литературы

В учебнике Виктора и Натальи Олифер «Компьютерные сети. Принципы, технологии, протоколы» [14] описываются различные сетевые протоколы и те изменения, которые произошли за несколько последних лет в компьютерных сетях. Учебник состоит из 7 частей, включающих в себя 29 глав, описывающих основные понятия, историю создания и проектирования компьютерных сетей и их протоколов. Также последнее издание данного учебника подробно описывает безопасность компьютерных сетей и основы протокола IPv6.

Первая часть посвящена основам передачи данных по всем имеющимся сетям на сегодняшний день. Часть два описывает технологии физических подключений, таких как кабели, структуры кабельных систем и правила их прокладки. Часть три содержит в себе информацию о технологиях локальных сетей, их отказоустойчивости и масштабируемости. Часть четыре описывает современные протоколы построения сетей, их адресацию, построение маршрутов и современные используемые протоколы маршрутизации. Часть пять повествует об организации и услугах глобальных сетей. Часть шесть кратко излагает об организации сетевых служб, таких как веб-почта, протоколы HTTP (HyperText Transfer Protocol). Часть семь посвящена подробной безопасности компьютерных сетей.

Вывод. Данный учебник служит отличным руководством по изучению компьютерных сетей и их построения, также огромное значение имеет описание современных технологий, используемых в конвергентных сетях.

Книга «Безопасность компьютерных сетей» [13], написанная Виктором Олифером, является учебным курсом, охватывающим широкий спектр различных тем в области методов, способов и средств обеспечения безопасности компьютерных сетей. При этом затрагиваются как базовые технологии защиты, так и методы защиты различного программного обеспечения.

Данное пособие состоит из 4 частей. Первая часть описывает общие понятия информационной безопасности, виды и возможные результаты угроз и общие способы защиты от них. Вторая часть посвящена изучению базовых технологий компьютерной безопасности, таких как симметричные и ассиметричные алгоритмы шифрования, понятия аутентификации, авторизации и идентификации, их виды и примеры реализации. Также в данной части рассматриваются технологии защищенного канала, технологии анализа трафика и состояния сети. Третья часть повествует о защите самой сети, включая реализуемые протоколы, их уязвимости, возможные атаки на них и методы защиты при помощи фильтрации, мониторинга трафика и туннелирования. В четвертой части разобрана реализация безопасности различного программного обеспечения, включая в себя различные операционные системы, прикладное программное обеспечение (ПО) и веб-сервисы. Затрагиваются вредоносные программы, вирусы, ботнет-сети и методы защиты от них.

Вывод. Данный курс подходит любому, кто хочет систематизировать или углубить свои знания в области компьютерных сетей и их безопасности. Особую пользу данная книга принесет специалистам, работающим в области сетевого администрирования и информационной безопасности.

В практическом пособии «Безопасность сети» [12], написанном Эриком Мэйволдом, содержатся подробные пошаговые инструкции по установке, настройке и использованию межсетевых экранов. Сведения о биометрических методах аутентификации, безопасных беспроводных соединениях и других со-

временных способах защиты сети и информации. Описываются воздействия компьютерных атак на организации и политики безопасности, предотвращающие летальные исходы.

Книга разбита на 4 части. Первая часть, как в многих других книгах по безопасности описывает основы, такие как определения, атаки, законодательство. Вторая часть посвящена юридическим вопросам информационной безопасности. В данной части описаны управление рисками и рекомендации по обеспечению сетевой безопасности. Часть третья подробно повествует о различных видах межсетевых экранов, виртуальных частных сетях (Virtual Private Network — VPN), современных методах шифрования, таких как AES (Advanced Encryption Standard), RSA (Rivest, Shamir и Adleman), DES (Data Encryption Standard). Описываются разнообразные системы обнаружения вторжений и их классификации. Четвертая часть посвящена практическому развертыванию систем безопасности в различных операционных системах. А также обеспечению безопасности в сети Интернет.

Вывод. Данное пособие подойдет читателям среднего уровня и студентам, обучающимся по специальностям направления «Компьютерные сети» и «Информационная безопасность»

1.1.2 Анализ дополнительной литературы

В книге Андрея Бирюкова, «Информационная безопасность: защита и нападение» [4] приводится описание различных атак и способов защиты от них.

Данная книга пригодится как системным администраторам, так и обычным пользователям небольших сетей, которые хотят обезопасить своё информационное пространство. В 8 главах данного издания достаточно глубоко описаны практические аспекты, связанные с тестированием уязвимостей систем и проведением аудитов по безопасности.

Вывод. Для разработки учебных пособий данная книга является хорошим справочником об атаках и их последствиях, также в данной книге приведён примерный практикум на примере операционной системы Kali Linux.

Учебник под редакцией Александра Назарова, предназначен для освоения модуля ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» для специальности 09.02.02 «Компьютерные сети» учреждений среднего профессионального образования. В данном учебнике описаны вопросы организации и использования объектов сети. Рассматриваются безопасность функционирования информационных систем, место информационной безопасности в политике Российской Федерации (РФ)[Н4], приведены технологии аутентификации и шифрования информационных процессов.

Данный учебник поделен на 2 части. Первая часть посвящена обслуживанию сети и её конфигурации. Вторая часть описывает безопасность функционирования объектов сетевой инфраструктуры.

Вывод. Учебник может быть рекомендован студентам и преподавателям СПО специальности «Компьютерные сети».

В книге «Техника сетевых атак» Криса Касперского [9] ведется повествование о проблемах безопасности сетевых сообщений. Вся информация, использованная в книге, получена из открытых источников и личного опыта автора. Материал, изложенный в книге, рассчитан на неподготовленного читателя, поэтому большую часть книги занимают описание основных протоколов сетей, операционных систем и принципов их построения.

Книга содержит более 50 глав, которые описывают достаточно большое количество материала, начиная от определения «хакер» и заканчивая примерами атак на различные виды серверов.

Вывод. Данная книга будет полезна сетевым администраторам, студентам технических специальностей и просто любопытным пользователям, так как в ней затронуты актуальные темы, описанные простым языком понятным каждому.

1.1.3 Анализ интернет-источников

Разработчик оборудования и решений для отрасли телекоммуникаций — НАГ (shop.nag.ru) — предлагает различное сетевое оборудование, комплексную техническую поддержку и сервис. На данном сайте расположены различные базы знаний по настройке и обслуживанию сетевого и телекоммуникационного оборудования и руководства пользователей по каждой конкретной единице техники. Данный материал поможет пользователю в настройке оборудования, а также на тематическом форуме сайта найдутся технические специалисты, которые ответят на любой возникший вопрос.

Вывод. Данный сайт будет необходим студентам и преподавателям, работающим с этим практикумом. Помимо этого, сайт полезен организациям и пользователям, работающим с оборудованием SNR, Cisco и Juniper.

Информационный портал по безопасности SecurityLab.ru — на данном портале постоянно рассказывается о событиях в области информационной безопасности.

Портал содержит несколько разделов, каждый из которых отвечает за своё направление. Раздел «Аналитика» содержит большое количество авторских статей по технологиям. Статьи позволяют получить свежую информацию об атаках, технологиях нападения, антивирусной защите и новых технологиях. Раздел «Софт» описывает более двух тысяч самых разнообразных программ для Вашей информационной среды. На сайте имеется общедоступный форум, который является самым популярным форумом по информационной безопасности.

Вывод. «SecurityLab» является единственным русскоязычным ресурсом, в котором можно найти полную информацию обо всех известных уязвимостях и рекомендациях по их устранению. Данный ресурс будет полезен всем, кто связан с областью информационных технологий и информационной безопасностью, не исключая обычных пользователей.

Habr.com — один из самых крупных ресурсов в Европе для IT-специалистов (IT — Information Technology), на котором можно найти разнообразные публикации и инструкции по таким направлениям информационной области, как разработка, дизайн, администрирование, программирование, информационная безопасность, разработка игр и прочие. Большим плюсом данного ресурса является то, что любой пользователь может предложить свою статью для публикации на сайте по любому из интересующих его направлений. Как и на многих других сайтах, «Habr» имеет собственный форум, на котором пользователи публикуют свои вопросы и варьируют их по уровню сложности.

Вывод. «Habr» будет полезен не только студентам IT-специальностей, но и опытным администраторам, дизайнерам, тестировщикам, программистам и всем тем, кто работает и развивается в сфере IT-технологий.

Сайт Xgu.ru — это ресурс обмена знаниями по различным системам с открытым кодом, компьютерным сетям, сетевой безопасности и прочей близкой к данным темам информации. Вся информация на данном сайте предоставляется свободно, каждую публикацию автор может выложить как открыто, так и с лицензией. Все статьи, публикации и инструкции представлены на русском языке.

Вывод. Данный сайт содержит в себе огромное количество информации по настройке сетевого оборудования, начиная от простых конфигураций и заканчивая сложными проектами. Тексты любой статьи являются простыми и будут понятны совершенно разным людям с различным уровнем образования и разнообразного рода деятельности.

Сетевая академия Cisco www.netacad.com является закрытым ресурсом профессионального обучения в сфере информационных технологий. Ресурсы академии используются зарегистрированными учебными заведениями и студентами по всему миру. Академия предлагает к изучению около 50 курсов по четырём направлениям с различной степенью сложности на нескольких языках. Направление компьютерных сетей подробно описывает базовые понятия технологий и настройки компьютерных сетей, всевозможные протоколы коммутации и маршрутизации и принципы построения локальных сетей для предприя-

тий. Направление сетевой и кибербезопасности глубоко затрагивает проблематику обеспечения информационной безопасности в сфере IT, не менее подробными и популярными являются направления программирования и Linux-подобных операционных систем.

Вывод. Знания и умения, которые могут получить обучающиеся данной сетевой академии, в будущем могут помочь построить карьеру в сфере сетевых технологий. Преподавателям академия помогает создавать учебные планы, позволяющие студентам приобрести необходимые навыки в сфере информационных технологий. После прохождения курсов данной академии студента можно считать квалифицированным специалистом, и это подтверждается квалификационными сертификатами.

1.2 Анализ нормативной и учебно-программной документации

Разрабатываемый электронный практикум предназначен для студентов среднего профессионального образования специальности 09.02.02 «Компьютерные сети», проходящих учебную практику, входящую в междисциплинарный курс «Эксплуатация объектов сетевой инфраструктуры».

Учебная практика (УП) «Обеспечение комплексной защиты информации» относится к части междисциплинарного курса, профессионального модуля образовательной программы [17].

Сроки прохождения учебной практики: УП.03.01 IV курс, VII семестр.

Максимальная учебная нагрузка по УП.03.01 — 36 часов.

Сроки изучения профессионального модуля: ПМ.03 IV курс, VII семестр.

Максимальная учебная нагрузка по ПМ.03 — 362 часа, из них 122 часа — самостоятельные работы, 172 часа выделены под теоретическое обучение и 68 часов на лабораторные и практические занятия. 36 — часов как описано выше выделены на прохождение учебной практики.

Задачами изучения профессионального модуля являются:

- уметь выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
- использовать схемы послеаварийного восстановления работоспособности сети эксплуатировать технические средства сетевой инфраструктуры;
- осуществлять диагностику и поиск неисправностей технических средств;
- выполнять действия по устранению неисправностей в части, касающейся полномочий техника; тестировать кабели и коммуникационные устройства;
- выполнять замену расходных материалов и мелкий ремонт периферийного оборудования;
- правильно оформлять техническую документацию; наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;
- устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту.

Целью изучения профессионального модуля «Эксплуатация объектов сетевой инфраструктуры» в учреждениях среднего профессионального образования являются [17]:

- формирование у студентов практического опыта обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;
- удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;
- организации бесперебойной работы системы по резервному копированию и восстановлению информации;
- поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры.

В результате изучения дисциплины студенты должны уметь:

1) выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;

2) использовать схемы послеаварийного восстановления работоспособности сети эксплуатировать технические средства сетевой инфраструктуры;

3) осуществлять диагностику и поиск неисправностей технических средств;

4) выполнять действия по устранению неисправностей в части, касающейся полномочий техника;

5) тестировать кабели и коммуникационные устройства;

6) выполнять замену расходных материалов и мелкий ремонт периферийного оборудования;

7) правильно оформлять техническую документацию;

8) наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;

9) устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту.

В результате изучения дисциплины, обучающиеся должны знать:

1) архитектуру и функции систем управления сетями, стандарты систем управления;

2) задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;

3) средства мониторинга и анализа локальных сетей;

4) классификацию регламентов, порядок технических осмотров, проверок и профилактических работ;

5) правила эксплуатации технических средств сетевой инфраструктуры;

6) расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;

7) методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;

8) основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем (ИС), требования к архитектуре информационных систем и их компонентам для

обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных;

9) основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.

В тематическом плане профессионального модуля «Эксплуатация объектов сетевой инфраструктуры» имеется 2 раздела [17]:

1) эксплуатация объектов сетевой инфраструктуры;

2) обеспечение безопасности функционирования информационных систем;

3) производственная практика (по профилю специальности).

Объём предлагаемого к изучению материала предназначен для реализации государственных требований к содержанию и уровню подготовки выпускников, и соответствует требованиям к знаниям. Является единым для всех форм обучения.

Кратко опишем содержание каждого из разделов.

Первый раздел содержит в себе шесть тем:

1) организация технического обслуживания средств вычислительной техники (СВТ);

2) мониторинг и анализ сетевых компонентов локальной вычислительной сети (ЛВС)[Н5];

3) средства восстановления данных;

4) создание точек восстановления для возобновления работы сети;

5) сетевые мониторы;

6) виртуальные частные сети.

Второй раздел содержит следующие темы:

1) угрозы сетевой безопасности;

2) безопасность на канальном уровне модели open systems interconnection (OSI)[Н6];

3) межсетевое экранирование;

4) трансляция сетевых адресов;

5) виртуальные частные сети.

Так же к данному разделу относиться учебная практика по обеспечению комплексной защиты информации.

Третий подраздел является производственной практикой по профилю.

Для качественного изучения и освоения материала, в программе используются лабораторные и практические работы большинству тем и разделов модуля.

Как и в любой рабочей программе предусмотрена самостоятельная работа студента в виде подготовки докладов, рефератов по разнообразным темам, подготовки к контрольным и практическим работам, и выполнения профессиональных заданий.

В ходе изучения модуля предусмотрен входной, промежуточный и итоговый контроль.

Изучение разделов и прохождение практик заканчивается дифференцированным зачетом, а изучение модуля в целом, заканчивается квалификационным экзаменом, который является завершающим для изучения модуля.

Тематический план рабочей программы приведен в приложении Б.

1.3 Проектирование электронных учебных пособий

1.3.1 Понятия лабораторного практикума и электронного учебного пособия

Лабораторный практикум — это потенциально наиболее значимый и результативный компонент естественно-научной, общей профессиональной и специальной подготовки в области техники и технологий, предназначенный для приобретения навыков работы на реальном оборудовании, с аналогами которого будущему специалисту, возможно, придется иметь дело в своей практической деятельности.

Электронное учебное пособие (ЭУП) — современный программно-методический обучающий комплекс, соответствующий времени, потребностям студента и запросам практики. При создании электронных учебных пособий необходимо наличие программного обеспечения, которое разработчик в состоянии грамотно использовать. В настоящее время создаются программные среды для разработки ЭУП и документации различного вида.

Электронное учебное пособие представляет собой интегрированное средство, включающее теорию, справочники, задачники, лабораторные практикумы, системы диагностики и другие компоненты.

Основное назначение учебного пособия — систематизация знаний, получаемых обучающимися при изучении дисциплины.

Преимуществами ЭУП можно назвать следующие аспекты:

1) возможность компактного хранения большого объема информации;
2) легко актуализируется (дополняется и расширяется);
3) широкие возможности поиска;
4) возможность выполнения интерактивных упражнений и тестов;
5) наглядность: широкие возможности построения визуальных моделей, представления графической и аудио информации;
6) хорошая структурированность (гипертекстовая организация информации).

1.3.2 Особенности электронных учебных пособий

Самым простым электронным учебником или пособием может быть конспект лекций преподавателя, хранимый как электронный документ и размещенный на учебном сервере образовательного учреждения или на любом общедоступном электронном ресурсе, но такой учебник, по факту, ничем не отличается от печатного конспекта и в нем никак не могут быть использованы специфические возможности электронного пособия. К главным таким особенностям можно причислить [8]:

1) возможность построения удобного и простого механизма навигации в пределах электронного учебника;

2) поисковый механизм в пределах электронного учебника, в частности, при использовании гипертекстового формата;

3) возможность встроенного автоматизированного контроля уровня знаний;

4) возможность адаптации изучаемого материала учебника к уровню знаний обучаемого, следствием чего является резкий рост уровня мотивации обучаемого;

5) возможность адаптации и оптимизации пользовательского интерфейса под индивидуальные запросы обучаемого.

К дополнительным особенностям электронного учебного пособия по сравнению с печатным следует отнести [8]:

1) возможность включения специальных фрагментов, моделирующих течение многих физических и технологических процессов;

2) возможность включения в состав учебника фрагментов видеофильмов для иллюстрации определенных положений учебника;

3) возможность включения в учебник аудиофайлов, в частности, для сближения процесса работы с учебником и прослушивания лекций этого же преподавателя;

4) включение в состав пособия интерактивных фрагментов для обеспечения оперативного диалога с обучаемым;

5) полномасштабное мультимедийное оформление учебника, включающее в себя диалог на естественном языке, организацию по запросу обучаемого видеоконференции с автором (авторами) и консультантами и пр.

Отсюда можно выделить что, электронное учебное пособие имеет следующие отличия от печатного учебника, эти отличия состоят в следующем:

1) любой печатный учебник рассчитан на определенный уровень подготовки обучающихся и предполагает конечный уровень обучения. Наглядность в электронном учебнике значительно выше, чем в печатном учебнике;

2) электронный учебник обеспечивает многовариантность, проверочных заданий, и разнообразного контроля;

3) наглядность обеспечивается использованием при создании электронных учебников мультимедийных технологий: анимации, звукового сопровождения, гиперссылок, видеосюжетов и т.п.;

4) электронные учебные пособия являются по своей структуре в большинстве случаев открытыми системами. Их можно корректировать, модифицировать дополнять в процессе использования;

5) электронное учебное пособие является мобильным: при его создании и распространении выпадают стадии типографской работы;

6) доступность электронного учебника выше, чем у печатных. При спросе на электронный учебник легко можно увеличить его тираж, можно переслать по сети.

Исходя из вышеописанного, к отличительным характеристикам электронных пособий можно отнести:

- возможность мультимедиа;
- определенная степень использования интерактивности;
- возможность индивидуального подхода к студенту;
- обеспечение виртуальной реальности.

1.3.3 Общие требования по созданию электронного учебного пособия

При разработке электронного учебного пособия выделяют ряд следующих требований:

1. Общие требования.
2. Дидактические требования.
3. Методические требования.
4. Требования к содержанию.
5. Требования к оформлению.

К общим требованиям можно отнести педагогическую целесообразность

и сочетаемость традиционной и информационной технологий в изучении конкретных учебных дисциплин.

Дидактические требования включают в себя:

- требование научности обучения — обеспечение достаточной глубины и корректности изложения учебного материала с учетом последних достижений науки;
- требование доступности обучения — обеспечение соответствия степени теоретической сложности и глубины изучения возрастным и индивидуальным особенностям учащихся, не допущение чрезмерной усложненности и перегруженности учебного материала;
- требование систематичности и последовательности обучения — обеспечение формирования знаний, умений и навыков, учащихся в определенной логически связанной последовательности с обеспечением преемственности;
- требование наглядности обучения — обеспечение чувственного восприятия учащимися объектов, процессов, явлений;
- требование сознательности и активности обучения — обеспечение самостоятельных и активных действий учащихся по извлечению учебной информации;
- требование прочности усвоения знаний — обеспечение закрепления знаний.

Основные методические требования к электронным учебным пособия сводятся к следующим:

- электронное учебное пособие должно отвечать требованию полноты содержания, позволяющему в полной мере реализовать методические цели обучения;
- электронное учебное пособие должно разрабатываться на основе педагогического сценария — целенаправленной последовательности педагогических методов и технологий, обеспечивающих достижение целей обучения.

При построении электронного учебного пособия необходимо обеспечить следующее:

1) учебный материал должен иметь завершенный смысл, но в тоже время не быть перегружен информацией;

2) текстовый материал, располагающийся в пособии должен сопровождаться иллюстративным материалом (статические и динамические иллюстрации);

3) в блоке должны присутствовать только те иллюстрации, которые связаны с текстом;

4) текстовый материал электронного учебного пособия не должен полностью повторять тексты бумажных учебников;

5) по ходу изучения учебного материала должны вводиться задания, стимулирующие самостоятельность и развивающие мышление;

6) электронное учебное пособие должно содержать встроенный раздел с контрольными вопросами, упражнениями и задачами, содержание которых определяется спецификой конкретной учебной дисциплины;

7) электронное учебное пособие должно включать в себя встроенный справочник (глоссарий), позволяющий в любой момент оперативно получать справочную информацию об основных понятиях, терминах, определениях и т.п., используемых в учебном материале. Вход в справочник (глоссарий) должен обеспечиваться с любой страницы электронного учебника;

8) электронное учебное пособие должно иметь встроенную тестирующую систему, предназначенную в первую очередь для самоконтроля учащегося в рамках текущего и итогового контроля;

При разработке внешнего вида (интерфейса) следует принимать во внимание требования, определяемые стандартами в области создания интерактивных приложений и определяемые психофизиологическими особенностями человека.

Существуют некоторые общие требования к программным продуктам [2]:

1. Принцип пропорции требующий, чтобы различные объекты не были хаотично разбросаны по экрану.

2. Порядок. Объекты должны располагаться от верхнего левого угла

экрана слева направо к нижнему правому углу экрана. Имеет смысл применять одни и те же цвета для различных блоков приложения.

3. Акцент. Выделение наиболее важного, которое должно быть воспринято в первую очередь.

4. Принцип равновесия. Равномерное расположение по экрану оптической тяжести изображения.

5. Принцип единства. Элементы изображения должны выглядеть взаимосвязано, правильно соотноситься по размеру, форме, цвету. Идентичные данные должны быть представлены однотипно.

6. Яркостные характеристики. Острота зрения при восприятии светлых объектов в 3–4 раза ниже, чем для тёмных. Светлые объекты на тёмном фоне обнаруживаются легче, чем тёмные на светлом.

7. Цветовые характеристики. Наиболее важными при выборе цветового решения можно считать следующие принципы:

- следует учитывать психофизиологическое воздействие на человека;
- глазу приятнее, если при оформлении используется нечётное число цветов — 3 или 5 (1 — уныло, 7 — слишком пестро);
- при использовании нескольких цветов большую роль играет их правильное сочетание.

Вывод. В результате анализа литературных источников можно сделать вывод о том, что создание электронного учебного пособия для изучения дисциплины «Основы теории информации» вполне оправдано и обосновано.

2 ЭЛЕКТРОННЫЙ ПРАКТИКУМ «ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

2.1 Педагогический адрес

Данный электронный практикум предназначен для прохождения учебной практики УП.03.01 «Обеспечение комплексной защиты информации» входящей в профессиональный модуль ПМ.03 «Эксплуатация объектов сетевой инфраструктуры», для студентов специальности 09.02.02 «Компьютерные сети» среднего профессионального образования.

2.2 Сравнительный анализ инструментов создания электронных пособий

Сегодня в образовании все чаще используются информационные технологии. С их помощью реализуются и используются различные средства наглядности (видео-уроки, мультимедийные презентации), разнообразные способы контроля (тестовые задания, практические задачи) и электронные учебные пособия (электронные учебники, лабораторные практикумы, тренажеры).

Не смотря на удобство электронных пособий, разработка подобных средств представляет собой сложную и трудоемкую задачу, требующую основательного подхода к выбору подходящего программного обеспечения.

Так как одной из задач данной работы является разработка электронного лабораторного практикума, то проведем сравнительный анализ средств и инструментов при помощи, которых можно создать электронное учебное пособие.

Исходя из различных требований к электронным пособиям, средства создания можно классифицировать следующим образом:

1. Средства мультимедиа.
2. Языки программирования.

3. Гипертекстовые средства.

Средства мультимедиа. Такие средства имеют возможность предоставлять информацию несколькими способами: текст, простые изображения, анимированные изображения и звук.

Мультимедийные средства обогащают и делают более интересным материал учебный материал за счет активизации всех способов восприятия. Отсюда, к плюсам электронных пособий, созданных при помощи данных средств можно отнести:

- возможность представления учебного материала в графическом, текстовом, звуковом виде одновременно;
- возможность автоматического просмотра содержания продукта, например слайд-шоу.

Минусами являются:

- большой объем данных занимаемых подобным пособием;
- линейная структура представления учебного материала.

В пример мультимедиа средств для создания электронных учебных пособий можно привести: Macromedia Flash — инструмент для создания анимированных объектов на основе векторной графики со встроенной поддержкой интерактивности. Данная программа активно используется дизайнерами и веб-художники, так как она очень проста в использовании, но при этом позволяет создавать разнообразные проекты со звуковой анимацией.

Adobe Flash — мультимедиа платформа от компании Adobe Systems для создания веб-приложений или мультимедийных презентаций.

Система ToolBook — является очень обширной, разно профильной, гибкой и мощной средой разработки приложений с возможностью вставлять в программу статический текст, графические изображения, анимацию, управляющие объекты — кнопки, списки.

Редактор электронных курсов Courselab — эффективный инструмент быстрой разработки мультимедийных учебных курсов, позволяющий создавать интерактивные учебные материалы в графическом режиме. Созданные на дан-

ном ресурсе курсы могут быть использованы для просмотра через Интернет, и для просмотра с любого съемного носителя.

Языки программирования. Современные среды программирования (C++, Delphi, Python, C# и др.) позволяют пользователю создавать универсальные программы, не исключены и электронные пособия. К основным недостаткам электронных пособий, созданных на языках программирования можно отнести:

- сложность изменения и сопровождения;
- дороговизну из-за трудоемкости разработки.

К достоинствам:

- разнообразие стилей реализации;
- отсутствие аппаратных ограничений, то есть возможность создания пособия, на необходимую программную и техническую базу.

Отметим, что, учитывая современное состояние технической базы в образовательных учреждениях, использование языков программирования для создания электронных учебных пособий становится неактуальным, так как на сегодняшний день в открытом доступе можно найти бесплатные и простые средства по разработке электронных пособий.

Гипертекстовые средства. Гипертекст — это способ нелинейной подачи материала. Данный способ позволяет легко сочетать различные виды информации — обычный текст, рисунок, звук, изображение, при котором в тексте имеются каким-либо образом выделенные слова, имеющие привязку к определенным текстовым фрагментам. Отсюда, пользователь не просто листает по порядку страницы текста, он может сам управлять процессом получения необходимой информации.

Использование гипертекстовой технологии удовлетворяет таким предъявляемым к электронным пособиям требованиям, как структурированность, удобство в обращении. При необходимости такой учебник можно опубликовать в сети Интернет и его можно легко корректировать. В настоящее время существует множество различных гипертекстовых форматов (HTML, DHTML, PHP и др.)

Hypertext Markup Language (HTML) [H7]— это язык разметки гипертекста с помощью которого создаются веб-страниц, а для того что бы придать эстетичный вид созданным страницам используют каскадные таблицы стилей cascading style sheets (CSS).

Язык разметки гипертекста имеет следующие плюсы:

1. Сайты и страницы, написанные на HTML, имеют малый вес.
2. Сайты на HTML работают и загружаются намного быстрее.
3. Простота создания простых и резервных копий.
4. Простота создания макета страниц и проектов.
5. Простота поддержки, т.к. обслуживанием проектов может заниматься любой более или менее знающий [H8]HTML-язык человек.

К минусам HTML можно отнести несколько пунктов, которые могут быть решающими при выборе средств создания электронных ресурсов:

- сложность внесения повторяющихся изменений на всех страницах (или на большинстве). Сложность заключается в том, что эти данные необходимо «вручную» заменить на каждой странице. И если сайт состоит из нескольких сотен страниц, кому-то этот процесс может показаться весьма затруднительным;
- отсутствие админ-панели, в которой более простым и понятным способом выводится информация о сайте и упрощен способ наполнения сайта контентом;
- для поддержки и наполнения сайта, необходимо обладать базовыми знаниями HTML.[H9]

PHP (Hypertext Preprocessor — препроцессор гипертекста) — это широко используемый язык сценариев общего назначения с открытым исходным кодом.

Это язык программирования, специально разработанный для написания web-приложений (скриптов, сценариев), исполняющихся на web-сервере. Одним из достоинств данного языка является то, что он способен генерировать и преобразовывать не только HTML документы, но и изображения разных фор-

матов, файлы PDF и FLASH. PHP способен формировать данные в любом текстовом формате, включая XHTML и XML.

В итоге к достоинствам электронных пособий, созданных средствами гипертекстовых технологий, относят:

- полную совместимость с web-технологиями и возможность опубликования электронного пособия в сети Интернет;
- малый вес за счет применения специальных алгоритмов сжатия информации.

К недостаткам:

- отсутствие единого стандарта представления материала;
- зависимость отображения учебного материала от расширения монитора и от конкретного браузера.

Проанализировав некоторые из средств создания электронных учебных пособий, был выбран язык разметки гипертекста HTML с применением каскадных таблиц стиля.

Данное средство было выбрано так как продукт созданный на HTML не требует дополнительной установки, достаточно просто запустить файл с необходимой страницей. Продукт созданный при помощи данных средств не будет привязан к конкретным операционным системам, единственным требованием будет наличие web-браузера.

Так же стоит отметить что продукт созданный средствами HTML будет занимать совсем не большое количество дискового пространства. В отличие от большинства других средств пособие, созданное на HTML, легко редактируется без специальных средств, и для разработки и пользования пособия не нужен доступ в сеть Интернет.

Для создания страниц практикума был использован текстовый редактор Notepad++, так как он прост в использовании, имеет поддержку большого количества языков программирования, упрощает работу с кодом подсветкой синтаксиса и является бесплатным. При необходимости к данному редактору возможно подключить различные дополнения и компиляторы.

2.3 Проект учебного пособия

Электронный практикум предназначен для прохождения учебной практики «Обеспечение комплексной защиты информации» входящей в профессиональный модуль ПМ.03 «Эксплуатация объектов сетевой инфраструктуры».

Пособие представляет собой программный продукт, написанный на стандартном языке разметки гипертекстовых страниц в Интернете — HTML5 (HyperText Markup Language) и языка для формирования внешнего вида документа — CSS (Cascading Style Sheets).

Теоретический материал лабораторного практикума описывает основные определения и понятия угроз применимых к коммутаторам, предлагая студенту структурированный материал по данной тематике и помогает решить поставленные задачи в лабораторных работах.

Целью теоретического материала является упрощение и напоминание студентам информации об основных атаках и способах зашиты от них.

Для реализации данной цели были изучены:

- источники литературы по теме исследования;
- принципы создания электронных учебных пособий;
- требования к электронному учебному пособию.

Контроль знаний в электронном учебном пособии организован с использованием теоретических вопросов, на которые студентам необходимо ответить до начала выполнения практических заданий и итогового задания в виде комплексной задачи по всему пройденному материалу за время практики.

Целью лабораторной части является применение теоретических знаний студента на полученных на практике.

При создании электронного лабораторного практикума были учтены требования к проектированию таких средств, перечисленными в первой главе:

- содержание должно быть структурированным, информация хорошо и тщательно подобрана, оформление должно быть эстетичным;

- контраст приложения не должен утомлять глаза, учебный материал должен располагаться в центре окна;
- визуально должны выделяться зона заголовка, навигации и информационного блока, а также должна быть понятна система навигации.

В состав документации к продукту необходимо включать:

1) описание электронного пособия, включающее общие сведения о продукте, описание программного обеспечения для работы с ним;

2) инструкцию для пользователей, содержащую все сведения об электронном пособии, его структуре, и правилах работы.

Разработка лабораторного практикума выполнялась следующим образом:

1) сбор и структурирование материала по профессиональному модулю «Эксплуатация объектов сетевой инфраструктуры»;
2) разработка оформления;
3) оформление текстового материала;
4) разработка вводного и итогового контроля;
5) разработка практических и лабораторных работ;
6) проверка работоспособности продукта и внесение коррективов.

Во время реализации и наполнения лабораторного практикума вносились корректировки и поправки в его структуру и оформление.

2.4 Описание продукта

2.4.1 Общая характеристика

Полное наименование данной программной разработки: «Электронный практикум учебной практики УП 03.01 «Обеспечение комплексной защиты информации», в дальнейшем именуется как «практикум».

Главная страница практикума представлена на рисунке 1.

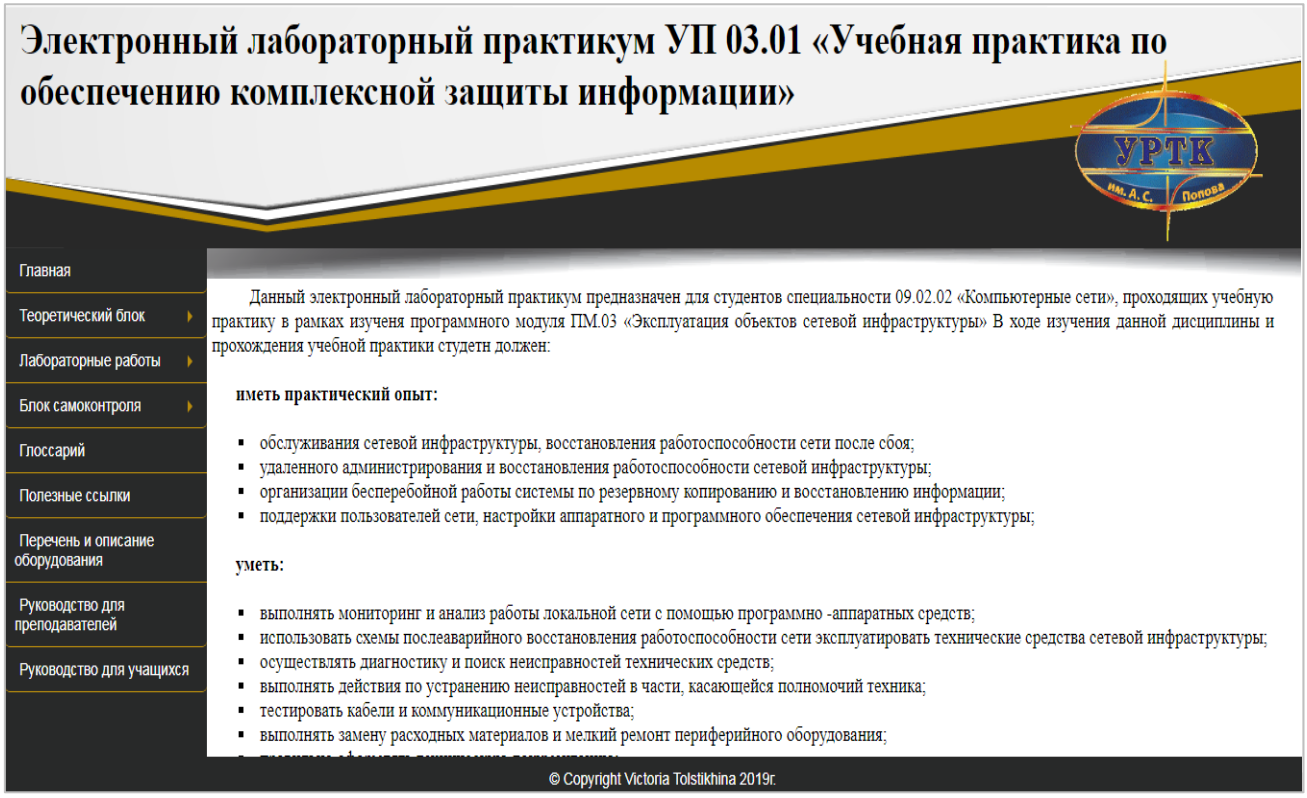

Рисунок 1 — Главная страница

Практикум включает в себя следующие разделы:

1) «Главная» — раздел содержит общую информацию о требованиях федерального государственного образовательного стандарта, предъявляемых к обучающимся, изучающим данную дисциплину;

2) «Теоретический блок» — содержит теоретический материал профессионального модуля, относящийся к учебной практике «Обеспечение комплексной защиты информации»», содержащие ссылки на подразделы с материалом для выполнения каждой лабораторной работы. Всего в разделе расположено одиннадцать тем:

- taking over the root bridge;
- dos using a flood of config bpdu’s;
- simulating a dual-homed switch;
- switch spoofing;
- double tagging;
- private vlan attack;

- random frame stress attack;
- уязвимости mac-spoofing;
- уязвимости arp-spoofing;
- уязвимости протокола dhcp;
- эксплуатация уязвимости;[H10]

3) «Лабораторные работы» — раздел содержит методические указания к выполнению лабораторных заданий практики. На основной странице данного блока расположена таблица с темами каждой лабораторной работы. Всего в практикуме представлено 9 лабораторных работ;

4) «Блок самоконтроля» — содержит подразделы с вводным контролем и итоговым контролем данной практики;

5) «Глоссарий» — содержатся основные определения и термины, используемые в лабораторных работах и теоретическом материале;

6) «Полезные ссылки» — раздел содержит ссылки на дополнительный материал, который может пригодиться в ходе прохождения практики и подготовки к итоговому контролю;

7) «Перечень и описание оборудования» — в разделе содержится перечень используемого в ходе лабораторных работ оборудования, и его описание по всем возможным характеристикам;

8) «Руководство для преподавателей» — в разделе содержатся требования к проведению практики, включающие в себя: методические указания, перечень оборудования, количество выделенных часов, а также ссылки на документы с инструкцией проверки;

9) «Руководство для учащихся» — содержит требования к ранее изученному материалу и уровню знаний студентов, а также ссылку на вводный контроль, необходимый для допуска к практике.

По левому краю практикума, располагается панель навигации со ссылками на все имеющиеся разделы (рисунок 2).

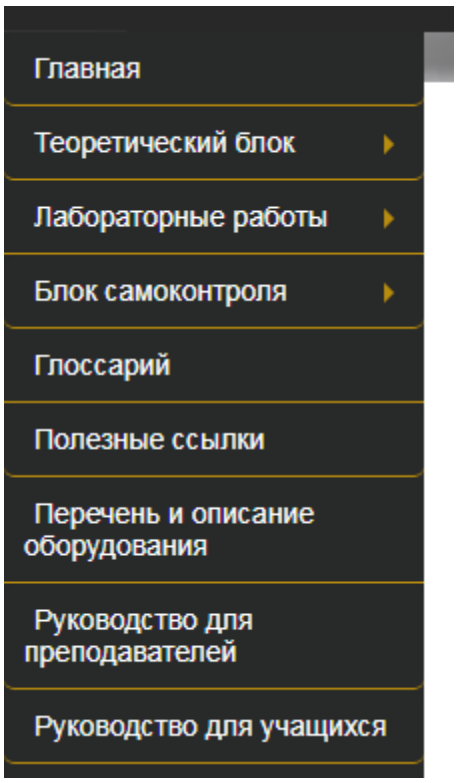

Рисунок 2 — Панель навигации

Раздел с лабораторными работами включает в себя краткое описание самих лабораторных работ (рисунок 3). Включенные в этот раздел, подразделы представляют собой методические указания по выполнению практических заданий (рисунок 4). Переходы выполняются кликабельными ссылками (рисунок 5).

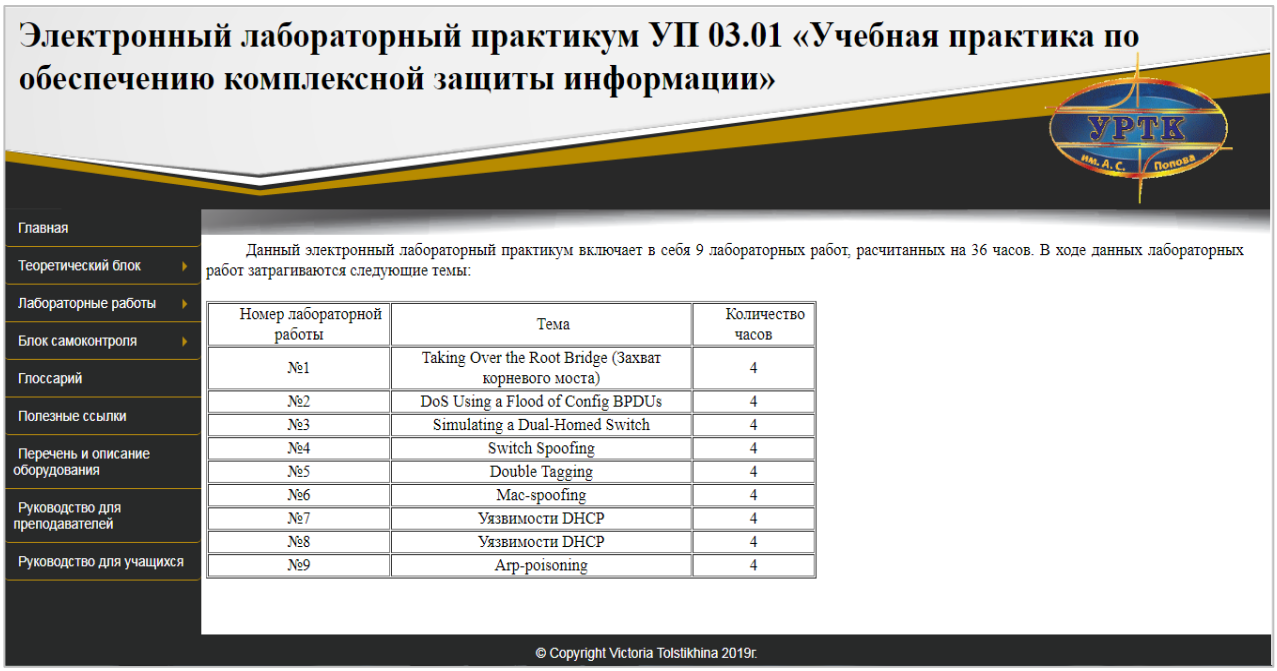

Рисунок 3 — Блок описания лабораторных работ

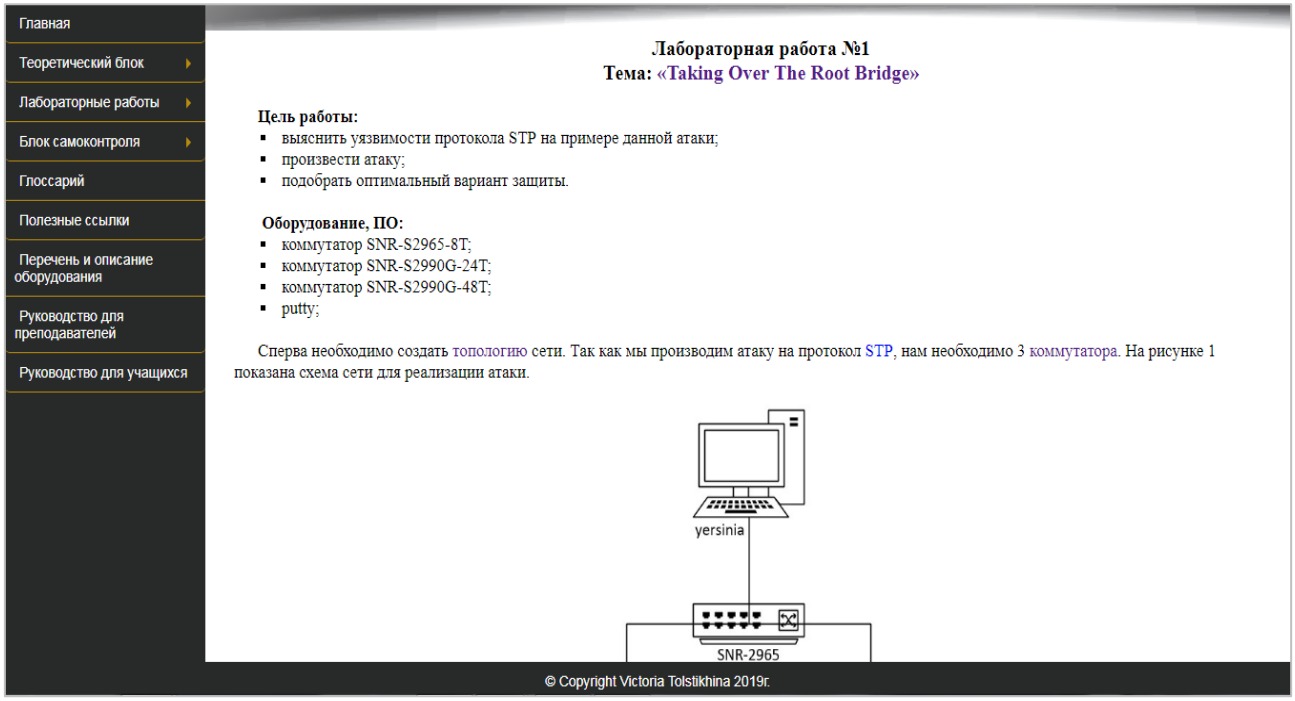

Рисунок 4 — Пример страницы с лабораторной работой

Рисунок 5 — Переходы на лабораторные работы

На рисунке 6 представлен блок самоконтроля. В нем расположены задания для вводного и итогового контроля.

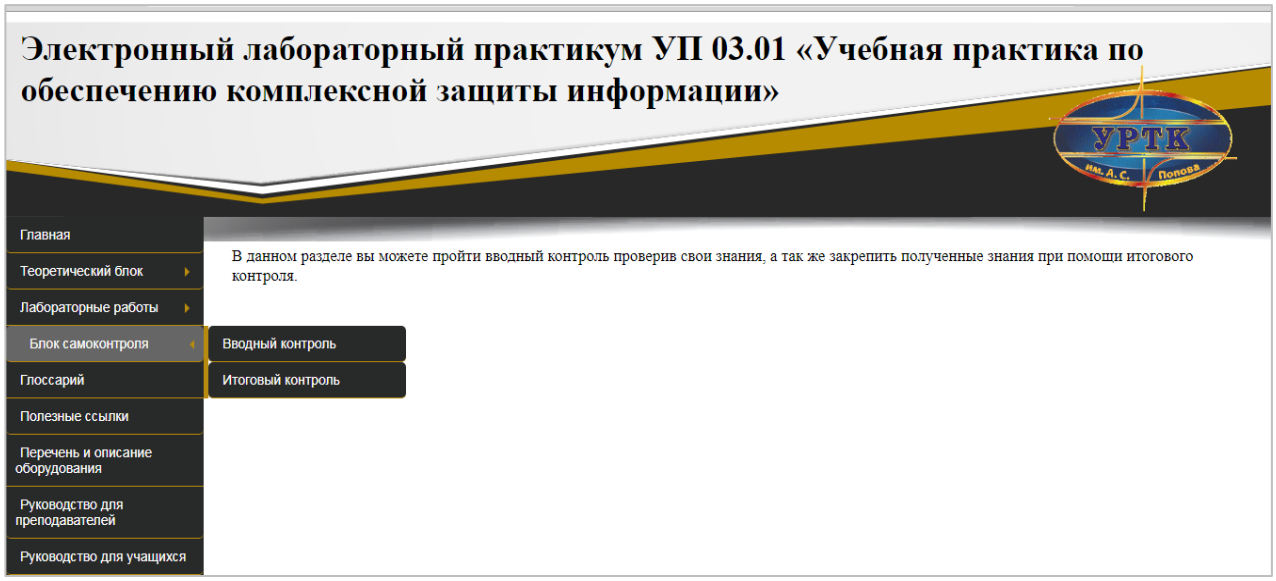

Рисунок 6 — Вид блока самоконтроля

В данном практикуме в текстах лабораторных работ и теоретического материала работают ссылки на глоссарий. При нажатии на выделенное слово, пользователь попадает на описательную часть данного выделения (рисунок 7).

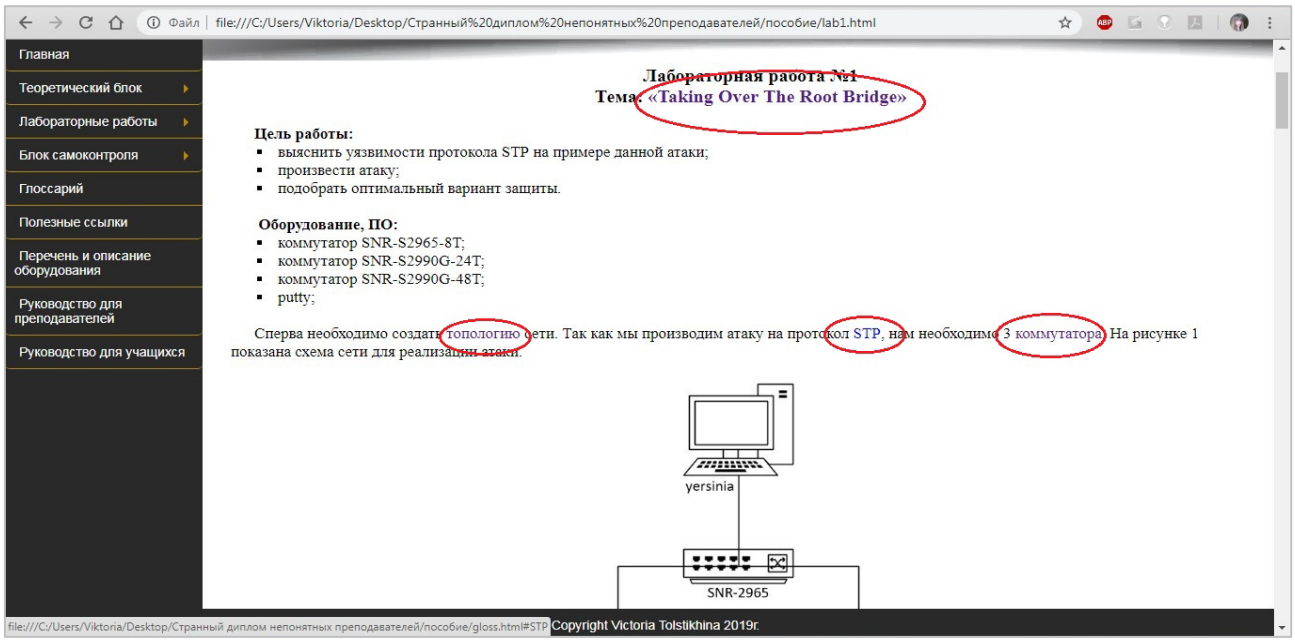

Рисунок 7 — Примеры ссылок в тексте

Структура разработанного лабораторного практикума представлена на рисунке 8.

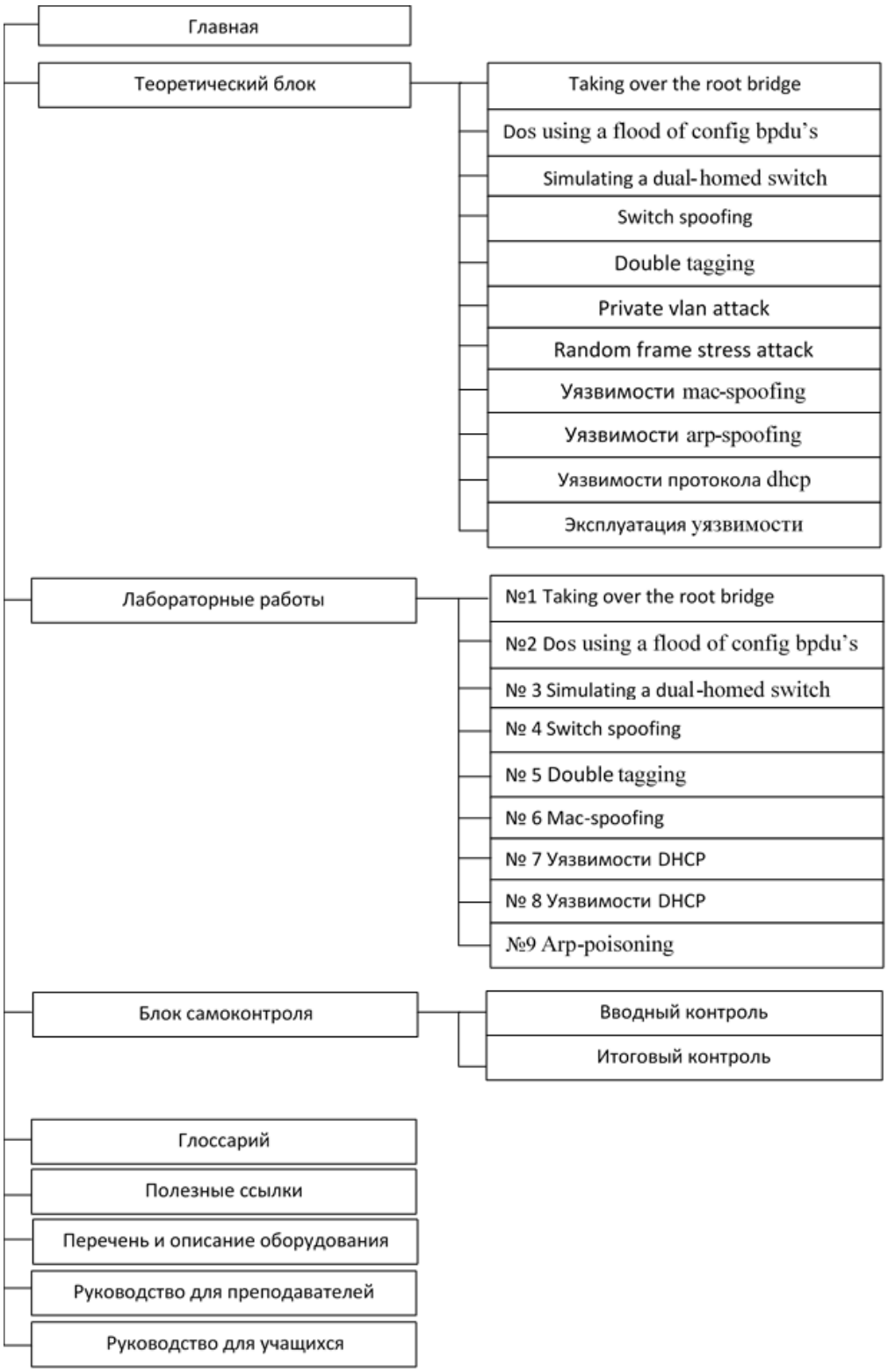

Рисунок 8 — Структура электронного учебного пособия

Данный электронный практикум предназначен для прохождения учебной практики студентами специальности 09.02.02 «Компьютерные сети» строго внутри учебного заведения.

Преподаватель при использовании данного практикума только консультирует студентов по возникшим у них вопросам.

2.4.2 Панель навигации

Навигация и все переходы по электронному практикуму осуществляется с помощью навигационного блока в виде кнопок и выпадающих списков, расположенного в левой части экрана (рисунок 9).

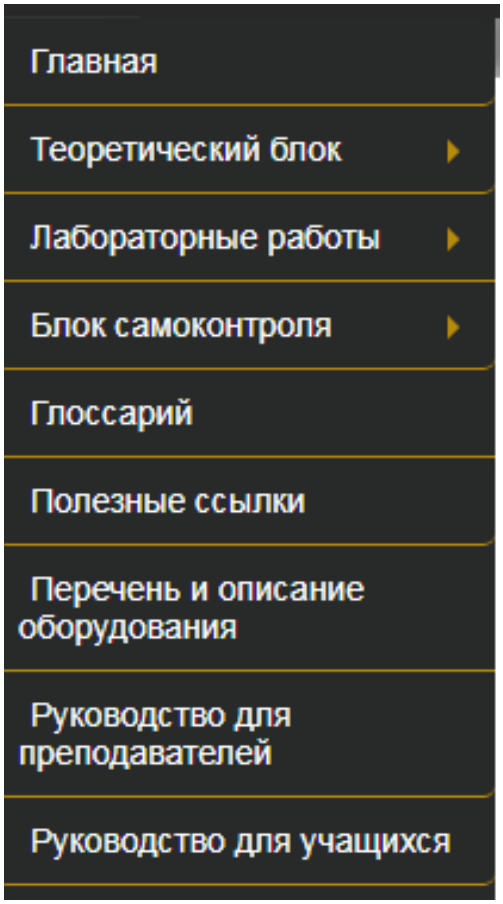

Рисунок 9 — Вид блока навигации

2.4.3 Блоки контента

Практикум представляет собой обработанный, скомпонованный теоретический материал к лабораторным работам и методические указания к лабораторным заданиям, представленный в удобной для обучающегося форме.

Раздел «Теоретический материал»

Данный раздел содержит 11 тем теоретического материала по модулю «Эксплуатация объектов сетевой инфраструктуры» (рисунок 10).

Цель раздела — сформировать у студента знания об различных уязвимостях и атаках на сетевое оборудование, и способах устранения данных проблем.

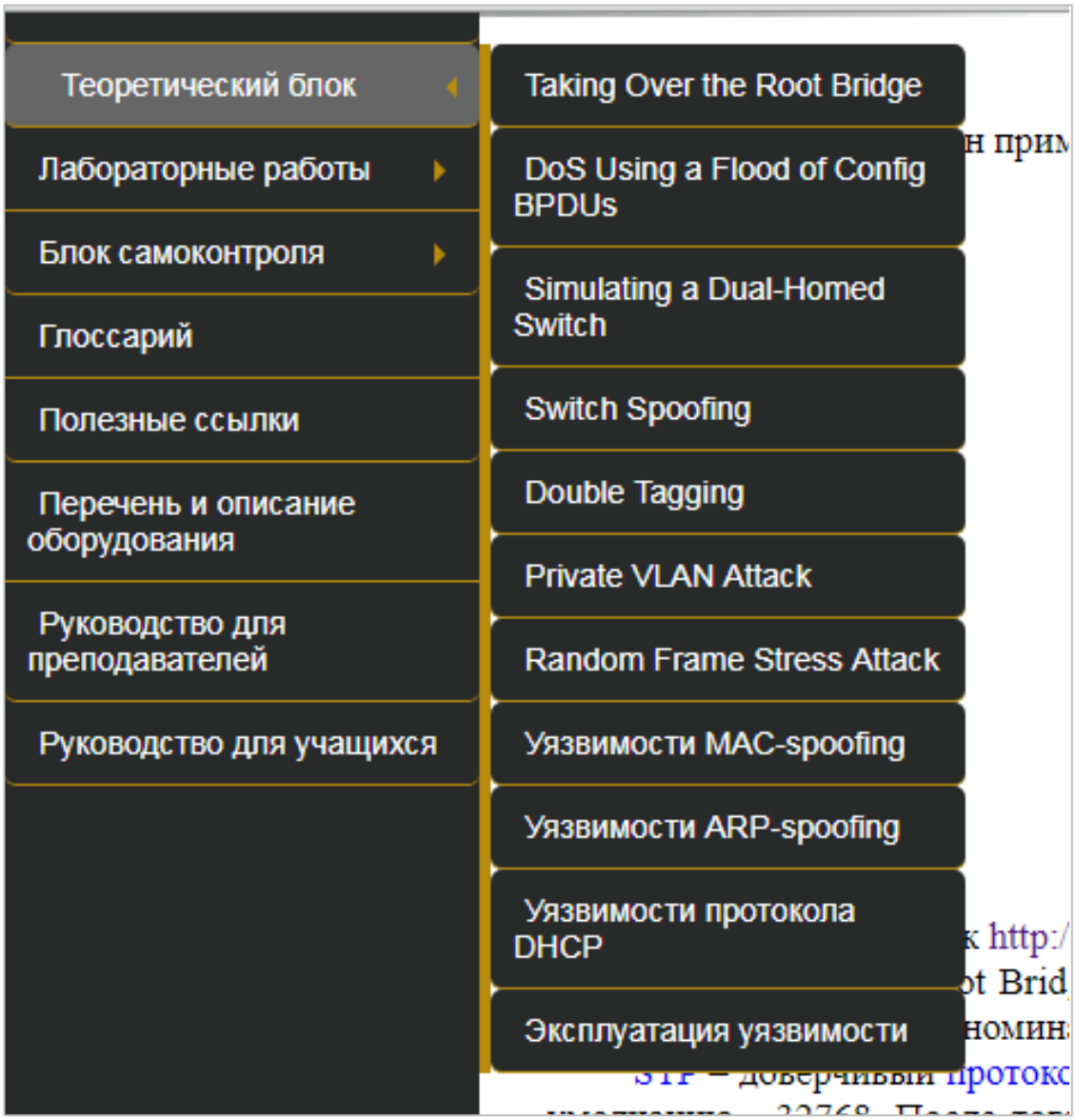

Рисунок 10 — Подразделы блока теории

Раздел «Лабораторные работы»

Раздел содержит методические указания для описания порядка выполнения лабораторных работ, предусмотренных учебной практикой. В разделе содержится 9 лабораторных работ (рисунок 11) и страница краткого описания (рисунок 12).

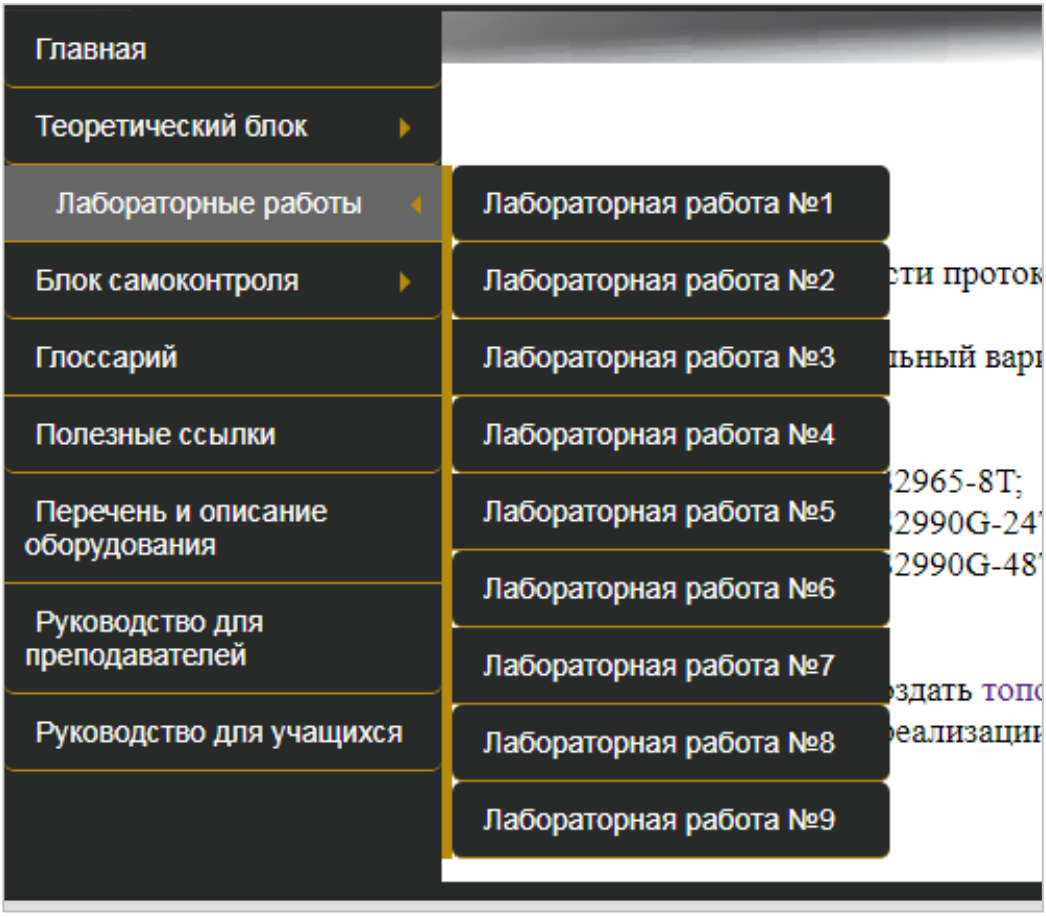

Рисунок 11 — Раздел «Лабораторные работы»

Рисунок 12 — Страница с описанием Лабораторных работ

«Блок самоконтроля». В данном разделе приведены задания для вводного и итогового контроля (рисунки 13, 14).

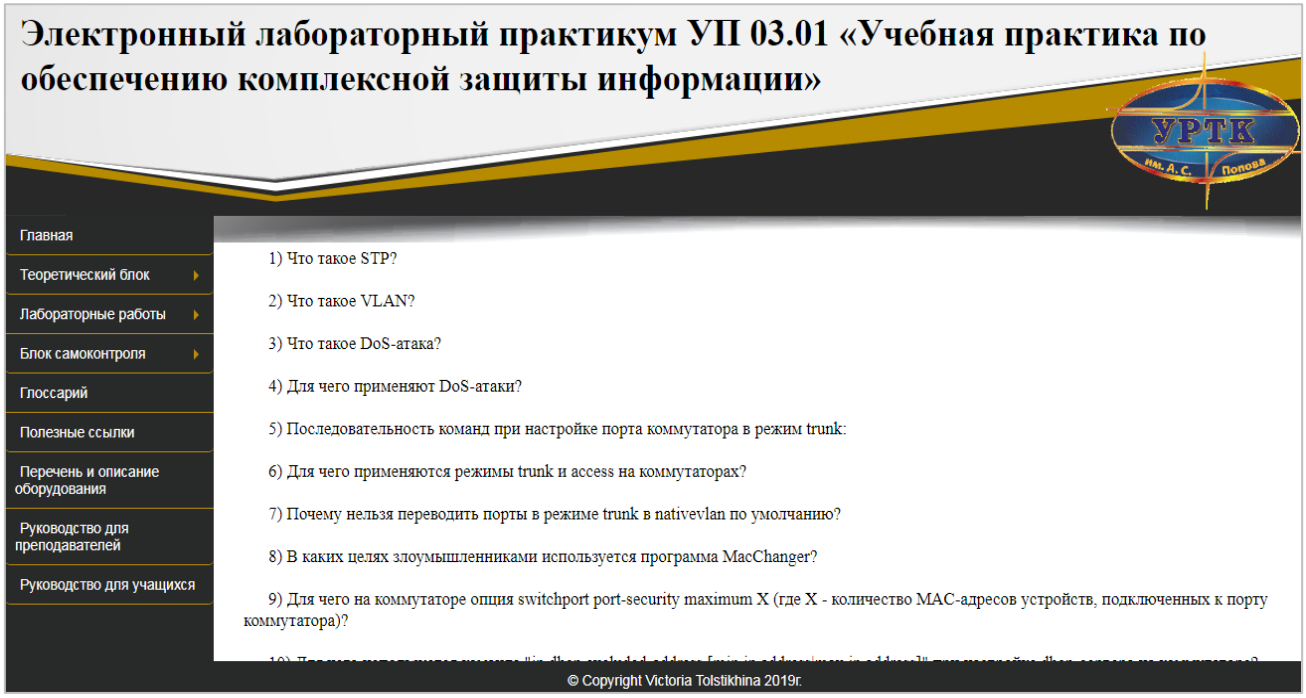

Рисунок 13 — Задания для вводного контроля

Рисунок 14 — Задания для итогового контроля

В разделе «Глоссарий» содержаться термины и определения, используемые в лабораторном практикуме. В данный раздел можно войти как из блока навигации, так и ссылок внутри текста. Пример страницы глоссария приведен на рисунке 15.[H11]

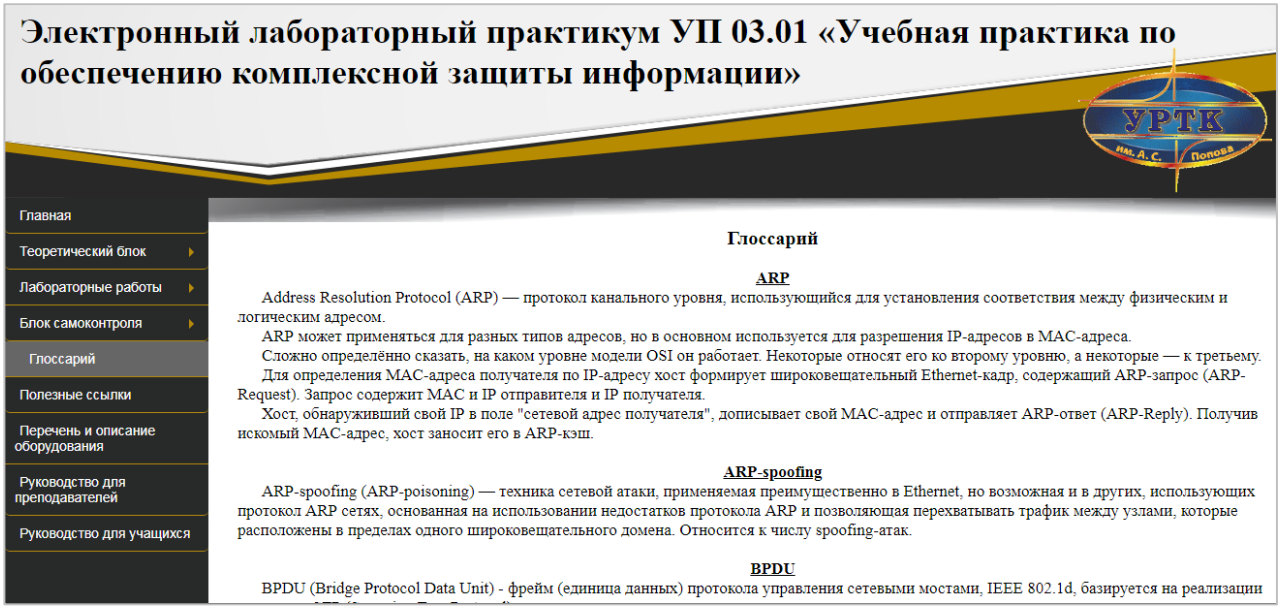

Рисунок 15 — Раздел «Глоссарий»

В разделе «Полезные ссылки» расположены ссылки на разнообразные сайты (рисунок 16), связанные с сетевым оборудованием, их настройкой. Так же имеются ссылки на источники, посвящённые информационной безопасности и различного рода угрозам на активное сетевое оборудование.

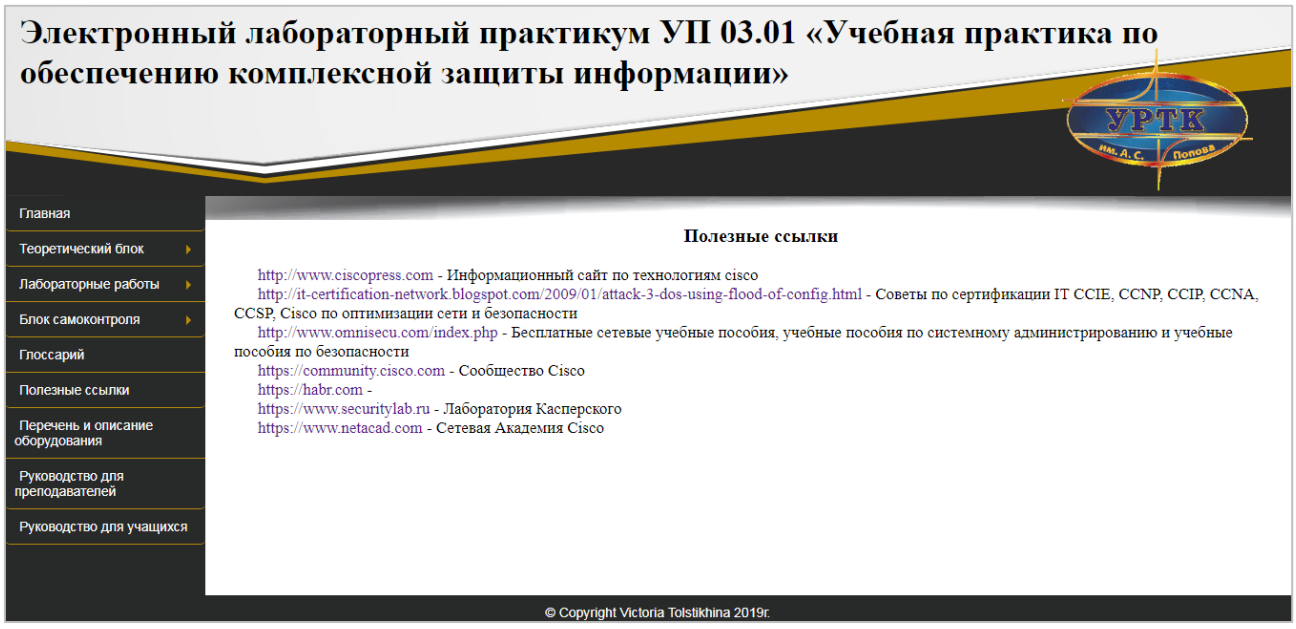

Рисунок 16 — Раздел «Полезные ссылки»

В разделе «Перечень и описание оборудования» расположена информация о используемом оборудовании в ходе выполнения лабораторных работ. Так же в данном разделе описаны полные характеристики каждой используемой единице техники. Внешний вид страницы представлен на рисунке 17.

Рисунок 17 — Раздел «Полезные ссылки»

В разделах «Руководство для преподавателей» и «Руководство для учащихся» (рисунки 18, 19) расположены инструкции к прохождению практики, требования к знаниям и умениям студентов, а также инструкции по использованию данного продукта.

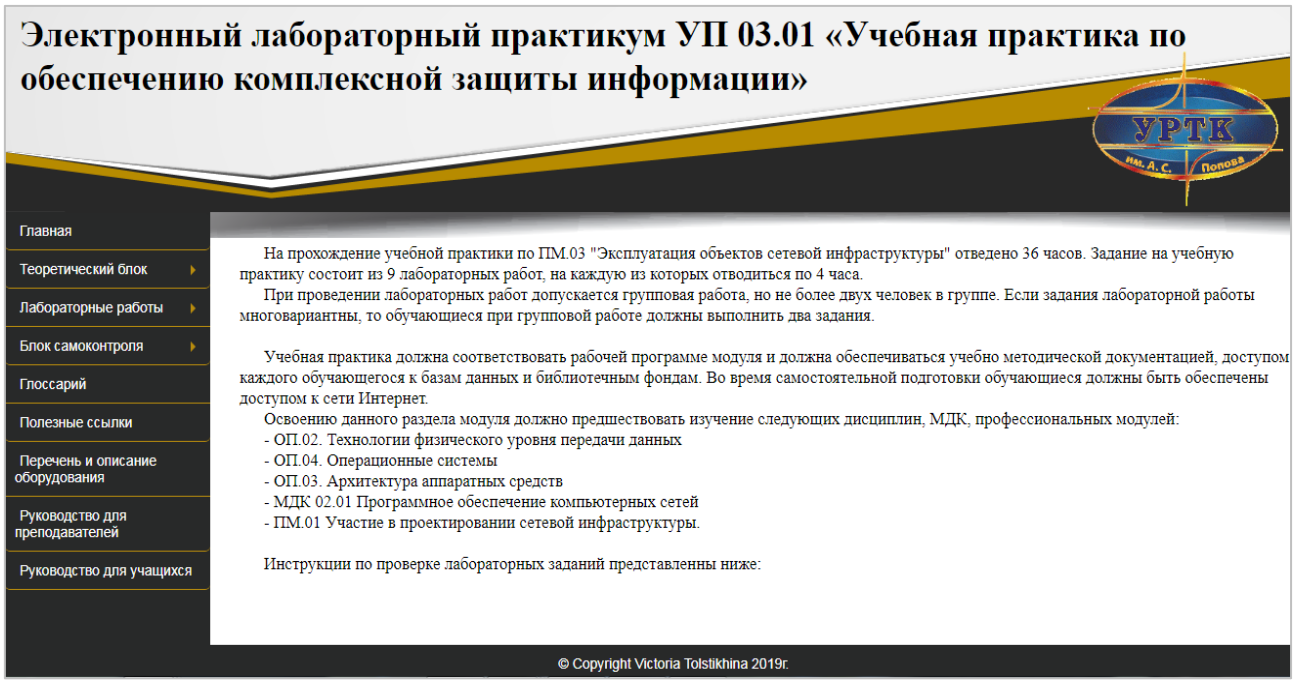

Рисунок 18 — Раздел «Руководство для преподавателей»

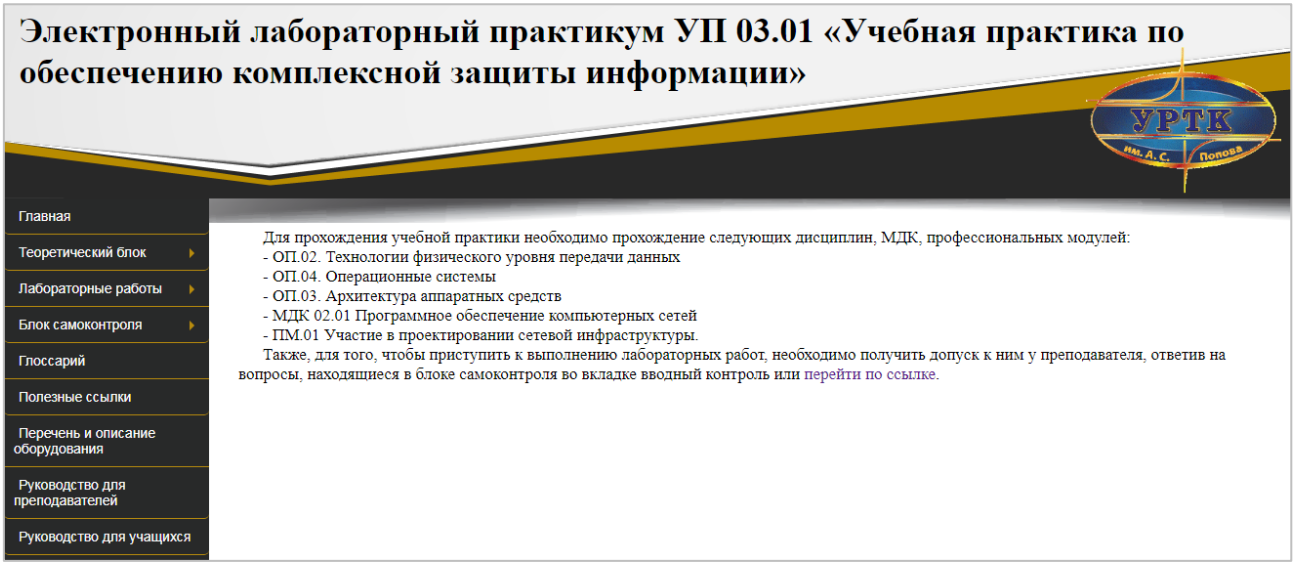

Рисунок 19 — Раздел «Руководство для учащихся»[H12]

Так же в разделах руководств расположены инструкции по пользованию данным приложением.

2.5 Инструкция по использованию электронного практикума

2.5.1 Инструкция для обучающегося

Для работы с электронным лабораторным практикумом рекомендуется использовать следующие инструкции:

- откройте файл «glav.html», размещенный в папке продукт;
- перемещение по разделам практикума осуществляется нажатием на кнопки-ссылки, расположенные с левой стороны практикума;
- для того чтобы вернуться на предыдущую страницу практикума, можно воспользоваться кнопками «Назад» браузера или перейти при помощи меню на необходимый раздел.

Данный электронный практикум предназначен для студентов специальности 09.02.02 «Компьютерные сети» проходящих учебную практику, включенную в ПМ.03 «Эксплуатация объектов сетевой инфраструктуры».

2.5.2 Инструкции по запуску электронного практикума

Аппаратно-программные требования

Практикум предполагает наличие персонального компьютера:

- процессор — IntelPentium 1 700 МГц или выше;
- объем оперативной памяти — 256 Мб;
- место на жестком диске — 100 Мб;
- видеоадаптер — 32 Мб с разрешением 1024x768;
- монитор — 15.6" с возможностью настройки разрешения экрана не менее 800x600;
- мышь.

Требования к программному обеспечению: операционная системы семейства Windows, Linux/Unix.

Данный практикум был разработан с использованием языка разметки гипертекста HTML и стиля CSS.

Для подготовки практикума к работе, необходимо проделать следующее:

1) скопировать папку «УП.03.01» на любой каталог жесткого диска;

2) щелкнуть по файлу «glav.html» правой кнопкой мыши и выбрать команду «Отправить — на рабочий стол (создать ярлык)»;

3) запустить с рабочего стола отправленный ранее файл;

4) при необходимости студент может обратиться к преподавателю, за помощью в запуске данного практикума.

ЗАКЛЮЧЕНИЕ

Во время выполнения выпускной квалификационной работы был разработан электронный практикум для учебной практики «Обеспечение комплексной защиты информации», включающий в себя блок лабораторных работ, теоретический блок для их выполнения и блок самоконтроля включающий в себя вводный и итоговый контроль. Данный электронный практикум апробирован и внедрен в учебный процесс образовательного учреждения Уральский радиотехнический колледж [H13]им. А. С. Попова для специальности «Компьютерные сети», что подвергается актом внедрения.

В результате выполнения выпускной квалификационной работы были решены следующие задачи:

1. Изучить особенности электронных учебных пособий и практикумов, ознакомиться с требованиями, которые к ним предъявляют.
2. Проанализировать литературу и электронные источники по эксплуатации объектов сетевой инфраструктуры.
3. Создать электронный практикум, для учебной практики «Обеспечение комплексной защиты информации»: подобрать материал, разработать задания для входного и итогового контроля обучающихся.

Таким образом, все поставленные задачи решены. Цель достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Атака на протокол Spanning Tree [Электронный ресурс]. — Режим доступа:[H14] https://www.securitylab.ru/analytics/451090.php (дата обращения: 07.05.2018).
2. Балыкина Е. Н.[H15] Сущностные характеристики электронных учебных изданий [Электронный ресурс]. — Режим доступа: http:// www.history.krsu.edu.kg (дата обращения: 21.12.2018).
3. Безопасность в сетях, построенных на Layer2-коммутаторах [Электронный ресурс]. — Режим доступа: http://samag.ru/archive/article/1901 [H16](дата обращения: 10.05.2018).
4. Бирюков А. А. Информационная безопасность: защита и нападение. [Текст] / А. А. Бирюков. — Москва: «Пресс», 2017. — 536 с.
5. Глоссарий [Электронный ресурс]. — Режим доступа: http://www.glossaru.ru (дата обращения: 07.01.2019).
6. Елистратова Н. Н. Электронный учебник как дидактическое средство в педагогике высшей школы [Электронный ресурс]. — Режим доступа: http://web.snauka.ru/issues/2012/01/6523 (дата обращения: 22.12.2018).
7. Защищаем сеть L2 коммутаторами [Электронный ресурс]. — Режим доступа: https://habr.com/post/231491/ (дата обращения: 29.05.2018).
8. Зимина О. В. Печатные и электронные учебные издания в современном высшем образовании: Теория, методика, практика [Текст] / О. В. Зимина[H17]. — Москва: «МЭИ», 2003. — 335 с.
9. Касперский К. Техника сетевых атак. [Электронный ресурс]. — Режим доступа: https://www.e-reading.club/chapter.php/99829/0/Kasperski_ _Tehnika_setevyh_atak.html (дата обращения: 02.01.2019).
10. Кругликов Г. И. Методика профессионального обучения с практикумом. [Текст] / Г. И. Кругликова. — Москва: «Академия», 2012. — 375 с.

11. Лучшие хакерские программы [Электронный ресурс]. — Режим доступа: https://codeby.net/luchshie-hakerskie-programmy/ (дата обращения: 13.05.2018).

12. Мэйволд Э. Безопасность сетей. Самоучитель. [Текст] / Э. Мэйволд. — Москва: «Пресс», 2013. — 528 с.

13. Олифер В. Г. Безопасность компьютерных сетей. [Текст] / В. Г. Олифер, Н. А. Олифер. — Санкт-Петербург: Питер, 2017. — 500 с.

14. Олифер В. Г. Компьютерные сети принципы, технологии, протоколы.[H18] [Текст] / В. Г. Олифер, Н. А. Олифер. — Санкт-Петербург: Питер, 2017. — 996 с.

15. О создании Федерального экспертного совета по учебным электронным изданиям [Электронный ресурс]: Приказ Минобразования РФ от 19 июня 1996 года №1646. — Режим доступа: http://www.lawmix.ru/pprf/125614 (дата обращения 22.01.2019).[H19]

16. Проблемы DHCP [Электронный ресурс]. — Режим доступа: https://xakep.ru/2003/01/04/17284/. (дата обращения: 12.05.2018).

17. Сетевая академия Cisco [Электронный ресурс]. — Режим доступа: http://www.netacad.com (дата обращения 24.12.18).

18. Уймин А. Г. Рабочая программа профессионального модуля «Эксплуатация объектов сетевой инфраструктуры» для студентов специальности 09.02.02 «Компьютерные сети» [Текст] / А. Г. Уймин, УРТК им А.С. Попова, 2016.

19. Управляемый коммутатор уровня 2 SNR-S2965-8T-RPS [Электронный ресурс]. — Режим доступа: http://ipboom.ru/catalog/kommutatory-dostupa-fastethernet/upravlyaemyy-kommutator-urovnya-2-snr-s2965-8t-rps (дата обращения: 03.05.2018).

20. Управляемый коммутатор уровня 2+ SNR-S2990G-24T [Электронный ресурс]. — Режим доступа: https://www.snrshop.kz/catalog/snr1/1907/. (дата обращения: 04.05.2018).

21. Электронные учебники: за и против [Электронный ресурс]. — Режим доступа: http://image.websib.ru/ (дата обращения: 21.12.2018).

22. Attacking the Spanning Tree Protocol [Электронный ресурс]. — Режим доступа: http://www.ciscopress.com/articles/article.asp?p=1016582&seqNum=2. (дата обращения: 08.05.2018).

23. Bpdu guard [Электронный ресурс]. — Режим доступа: http://telecombook.ru/archive/network/cisco/directory/46-bpdu-guard. (дата обращения: 23.05.2018).

24. CentOS [Электронный ресурс]. — Режим доступа: https://distrowatch.com/ (дата обращения: 17.05.2018).

25. Dos атака на dhcp сервер. Dhcp starvation [Электронный ресурс]. — Режим доступа: https://blackdiver.net/it/linux/4031. (дата обращения: 27.05.2018)

26. LAN Switch Security [Электронный ресурс]. — Режим доступа: http://www.tnu.edu.vn/sites/phuongpn/Bi%20ging%20chia%20s/Tailieu%20Network/LAN%20Switch%20Security.pdf. (дата обращения: 26.05.2018).

27. STP (Spanning Tree Protocol) [Электронный ресурс]. — Режим доступа: https://russiancisco.blogspot.com/2012/03/stp-spanning-tree-protoco.html. (дата обращения: 06.05.2018).

28. Understanding, Preventing, and Defending against Layer 2 Attacks [Электронный ресурс]. — Режим доступа: https://www.cisco.com/c/dam/ global/en_ae/assets/exposaudi2009/assets/docs/layer2-attacks-and-mitigation-t.pdf (дата обращения: 05.05.2018).

29. Welcome to Scapy’s documentation! [Электронный ресурс]. — Режим доступа: http://scapy.readthedocs.io/en/latest/#. (дата обращения: 14.05.2018).

30. What is Switch spoofing attack and how to prevent Switch spoofing attack [Электронный ресурс]. — Режим доступа: http://www.omnisecu.com/ccna-security/what-is-switch-spoofing-attack-how-to-prevent-switch-spoofing-attack.php (дата обращения: 25.05.2018).

31. Yersinia [Электронный ресурс]. — Режим доступа: https://tools.kali.org /vulnerability-analysis/yersinia. (дата обращения: 20.05.2018)

ПРИЛОЖЕНИЕ А

3.1 Тематический план профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля*	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6	**Раздел 1 Эксплуатация объектов сетевой инфраструктуры**	**218**	**144**	44	-	**74**	-	-	-
ПК 3.4	**Раздел 2 Обеспечение безопасности функционирования информационных систем**	**180**	**96**	24	-	**48**	-	**36**	-
	Производственная практика (по профилю специальности), часов	-							-
	Всего:	**398**	**240**	68	-	**122**	-	**36**	-

ПРИЛОЖЕНИЕ Б