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

ЛАБОРАТОРНЫЙ ПРАКТИКУМ «ТЕХНОЛОГИИ УДАЛЕННОГО ДОСТУПА»

Выпускная квалификационная работа бакалавра
по направлению 44.03.04 Профессиональное обучение (по отраслям)
профиля «Информатика и вычислительная техника»
профилизация «Компьютерные технологии»

Идентификационный номер ВКР: 011

Екатеринбург 2016

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

К ЗАЩИТЕ ДОПУСКАЮ
Заведующая кафедрой ИС
_____ Н. С. Толстова
«____» _____ 2016 г.

ЛАБОРАТОРНЫЙ ПРАКТИКУМ «ТЕХНОЛОГИИ УДАЛЕННОГО ДОСТУПА»

Выпускная квалификационная работа бакалавра
по направлению 44.03.04 Профессиональное обучение (по отраслям)
профиля «Информатика и вычислительная техника»
профилизация «Компьютерные технологии»

Идентификационный номер ВКР: 011

Исполнитель:
студент группы КТ-401 Н. В. Городилов
Руководитель:
ст. преподаватель каф. ИС С. С. Венков
Нормоконтролер: Б. А. Редькина

Екатеринбург 2016

РЕФЕРАТ

Пояснительная записка к выпускной квалификационной работе выполнена на 52 страницах, содержит 15 рисунков, 31 источник информации, 3 приложения.

Ключевые слова: CISCO PACKET TRACER, VPN, SSH, TELNET. REMOTE ACCESS VPN, КОММУНИКАЦИИ, ВИРТУАЛЬНЫЕ СЕТИ.

Объект исследования – процесс обучения студентов направления подготовки 44.03.04 «Профессиональное обучение (по отраслям)» профиля «Информатика и вычислительная техника» профилизации «Компьютерные технологии» разделу «Технологии удаленного доступа» в рамках дисциплины «Компьютерные коммуникации и сети».

Предмет исследования — учебные материалы по теме «Технологии удаленного доступа» дисциплины «Компьютерные коммуникации и сети».

Цель работы — разработать лабораторный практикум «Технологии удаленного доступа».

Для достижения поставленной цели были решены следующие задачи:

1. Проанализирована литература и интернет-источники с целью выделения требований, предъявляемых к лабораторным практикумам на современном этапе развития образования.
2. Выполнен анализ инструментов и средств решения задачи выбраны программы создания практикума.
3. Спроектирована структура и реализован интерфейс и функционал лабораторного практикума «Технологии удаленного доступа».

Результаты выпускной квалификационной работы будут использоваться студентами третьего курса направления подготовки «Профессиональное обучение (по отраслям)» профиля «Информатика и вычислительная техника» профилизации «Компьютерные технологии».

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Важной составляющей сети Internet является сеть передачи данных. Это совокупность трёх и более оконечных устройств (терминалов) связи, объединённых каналами передачи данных и коммутирующими устройствами (узлами сети), обеспечивающими обмен сообщениями между всеми оконечными устройствами. Поэтому возникает потребность в специалистах, для обслуживания и работы большим количеством оборудования в сетях передачи данных, что в свою очередь требует знаний и умений для работы с технологиями удаленого доступа к оборудованию. С целью обучения студентов основам технологий удаленного доступа разработано множество практикумов и лабораторных работ, применяемых в рамках дисциплины «Компьютерные коммуникации и сети».

Актуальность выбранной темы состоит в том, что для эффективного изучения обучающимися основ технологий удаленного доступа необходимо наличие комплексного педагогического программного средства (ППС), объединяющего в себе простоту работы с уже имеющимся сетями, так и возможность самостоятельного создания коммуникационной сети со стороны обучающегося.

Объект исследования — процесс обучения студентов направления подготовки 44.03.04 «Профессиональное обучение (по отраслям)» профиля «Информатика и вычислительная техника» профилизации «Компьютерные технологии» разделу «Технологии удаленного доступа» в рамках дисциплины «Компьютерные коммуникации и сети».

Предмет исследования — учебные материалы по теме «Технологии удаленного доступа» дисциплины «Компьютерные коммуникации и сети».

Цель работы — разработать лабораторный практикум «Технологии удаленного доступа».

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать литературу и интернет-источники по теме «Технологии удаленного доступа» с целью формирования набора навыков, являющихся основными и критическими для обучения данному разделу.

2. Проанализировать литературу и интернет-источники с целью выделения требований, предъявляемых к лабораторному практикуму на современном этапе развития образования.

3. Спроектировать структуру и реализовать интерфейс и функционал лабораторного практикума «Технологии удаленного доступа».

1 АНАЛИЗ ИСТОЧНИКОВ ПО ТЕМЕ «ТЕХНОЛОГИИ УДАЛЕННОГО ДОСТУПА»

1.1 Анализ литературы и интернет-источников

1.1.1 Анализ литературы

Для разработки лабораторного практикума, необходимо проанализировать литературу, что позволит понять теоретическую сторону операций и систематизировать материал.

В книге С. Брауна «Виртуальные частные сети VPN» [3] большое внимание уделено вопросам безопасности в VPN. Безопасность является важнейшей частью данной технологии. Технология VPN изменяет правила, когда дело касается безопасности вашей компании. Безопасность становится новой моделью, где не подходит традиционное мышление. Обычно компании стараются защитить свою сеть от взломщиков и воздвигают некоторую разновидность стены, например, брандмауэр, который не позволяет проникнуть в сеть посторонним. При наличии VPN компания может передавать данные в Интернет и надеяться, что никто не сможет их изменить. Открывая вход в свою сеть (например, почтовый трафик), можно предположить, что никто не сможет войти в нее через этот вход без правильной авторизации.

Учебное пособие С. В. Запечникова «Основы построения виртуальных частных сетей» [7] рассматривает основы построения виртуальных частных сетей. Даются основные определения. Описывается технология туннелирования в сетях. Подробно анализируются стандартные протоколы построения VPN и управление криптографическими ключами в VPN. Выделяются особенности различных вариантов и схем создания VPN. В качестве примеров реализации VPN приводятся различные российские продукты. Для студентов высших учебных заведений, обучающихся по специальностям «Компьютерная безопасность» и «Компьютерные технологии»

Книга Н. В. Максимова «Компьютерные сети» [13] посвящается проблематике телекоммуникационных систем, сетей и технологий доступа к распределенным информационным ресурсам. Основная цель пособия - охватить как можно более широкий круг вопросов, связанных с телекоммуникационными и вычислительными системами, включая использование данных средств для доступа к мировым информационным ресурсам.

В книге Одома Уэнделла «Компьютерные сети. Первый шаг» [19] приведены основные о компьютерных сетях, их компонентах и технологиях. Рассмотрены все разновидности локальных и глобальных компьютерных сетей, рассказано об особенностях их структур, компонентов и методах применения. Особое внимание уделено вопросам безопасности компьютерных сетей.

В книгу Д. Л. Шиндлера «Основы компьютерных сетей» [22] включено введение в выполняющиеся на сетевых компьютерах клиентские и серверные операционные системы. В книгу включены история развития вычислительных сетей, принятая терминология, теория сетей, установившиеся стандарты и способы реализации локальных и глобальных вычислительных сетей.

Издание В. Г. Олифера «Компьютерные сети. Принципы, технологии, протоколы» [15] представляет собой учебный курс, в котором последовательно рассматриваются основные аспекты архитектуры и технологии современных компьютерных сетей. В книге освещены вопросы главных концепций, являющихся фундаментом компьютерных сетей, технологии проводных, беспроводных локальных сетей, глобальной сети, популярных сетевых услуг и сервисов.

Книга М. В. Кульгина «Компьютерные сети. Практика построения. Для профессионалов» [12] рассчитана на более продвинутых пользователей. В ней рассматриваются только те устройства и технологии, которые являются базовыми и основополагающими: маршрутизаторы компании Cisco Systems и их настройка, технология организации очередей, трансляции адресов, построения защитного экрана, настройка протоколов маршрутизации, построе-

ние защищенных виртуальных сетей и т. п. Книга состоит из 10 глав, в которых последовательно описываются вопросы настройки маршрутизаторов Cisco, работа протокола ICMP, TCP/IP, описывается технология трансляции адресов (NAT), маршрутизация в IP-сетях, освещаются вопросы обеспечения безопасности при передаче данных, а также вопросы построения защищенных виртуальных сетей (VPN). В дополнение книга включает в себя приложение, в котором приведены номера портов наиболее популярных программ.

В учебном пособии Галкина В.А. «Телекоммуникации и сети» [5] приведены основы построения систем передачи данных и их характеристики, современные методы и технологии телекоммуникационных систем. Большое внимание в книге уделено методам построения локальных вычислительных сетей и сетевой операционной системе NetWare. Рассмотрены современные сетевые технологии (Frame relay, ISDN, ATM), мобильные и спутниковые сети, а также назначение и сценарии работы основных сетевых протоколов, вопросы объединения сетей и построения корпоративной электронной почты.

Книга В. М. Вишневского «Теоретические основы проектирования компьютерных сетей» [4] рассматривает методы анализа и синтеза компьютерных сетей. Приводятся точные и приближенные математические методы исследования систем и сетей очередей, а также эффективные вычислительные алгоритмы расчета таких сетей. С позиций теории сетей очередей описываются различные аспекты проектирования компьютерных сетей. Рассматриваются стохастические сетевые модели анализа задержек, управления потоками и расчета узлов коммутации пакетов. Систематизируются и исследуются алгоритмы выбора оптимальных маршрутов в сетях пакетной коммутации и динамической маршрутизации в АТМ-сетях. Дается описание комбинаторного алгоритма синтеза топологической структуры корпоративных компьютерных сетей. Приводятся результаты в области проектирования и оценки производительности сетей.

В книге К. Пакет «Создание сетей удаленного доступа Cisco» [17] представлена основная техническая информация о различных технологиях,

используемых при организации удаленного доступа к сети предприятия. Книга основана на одноименном специализированном курсе для подготовки и сертификации специалистов и представляет собой учебник, содержащий сведения о том, как разрабатывать, настраивать, управлять и расширять сеть удаленного доступа, которая построена на основе оборудования корпорации Cisco.

Материал, представленный в книге М. Ю. Захватова «Построение виртуальных частных сетей (VPN) на базе технологии MPLS» [8] представляет собой достаточно подробное описание основных аспектов внедрения технологии MPLS в сетях операторов для предоставления услуги Виртуальная частная сеть и производных услуг. В документе подробно рассматриваются вопросы, связанные с обоснованием выбора технологии MPLS-VPN; приведены примеры решения услуг по построению интранет- и экстранет-сетей, рассмотрены вопросы, связанные с предоставлением внешних услуг, Интернет и сетевого управления, аспекты, связанные с обеспечением качества обслуживания и трафик-инжиниринга, приведены различные варианты организации системы доступа и вопросы организации маршрутизации. Документ ориентирован на инженерно-технический персонал, использующий или планирующий применение данной технологии в своей сети, сетевых дизайнеров и консультантов, чья область интересов распространяется на технологию MPLS.

Учебное пособие Андрончик А. Н. «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 CiscoIOS, вопросы администрирования маршрутизаторов и межсетевых экранов, способы обнаружения сетевых компьютерных атак на базе комплексов Cisco IDS Sensor и Cisco MARS. Основной акцент в пособии делается на практическое изучение

материала, что реализуется благодаря применению технологии виртуальных машин и использованию в образовательном процессе программных эмуляторов аппаратуры фирмы Cisco Systems.

В учебном пособии Иванова М. А. «Криптографические методы защиты информации в компьютерных системах и сетях» [9] излагаются основы классической криптографии, рассматриваются современные криптографические методы защиты информации: криптосистемы с открытым ключом, гибридные криптосистемы, системы вероятностного шифрования, протоколы аутентификации и электронной подписи. Рассматриваются современные синхронные и самосинхронизирующиеся поточные шифры, дается описание стандарта AES — криптографической защиты XXI в. для студентов и аспирантов вузов компьютерных специальностей. Может быть полезна разработчикам и пользователям компьютерных систем и сетей.

1.1.2 Анализ интернет-источников

Основная информация по теме «Технологии удаленного доступа» остается неизменной с момента основания, но, с течением времени, нюансы работы сильно меняются и актуальную информацию можно найти только в Интернет-источниках. Интернет-источники предоставляют обширное количество наглядных примеров настройки в открытом доступе, а также научно-популярные статьи на данную тему. С другой стороны, для разработки лабораторного практикума необходимо знание средств разработки и, в данном случае, основ HTML. Для данной цели Интернет-источники подходят намного лучше литературных источников, в силу своей актуальности.

Сайт «Хабрахабр» [21] представляет собой электронный ресурс, посвященный всевозможным областям индустрии информационных технологий, включая создание и настройку веб-серверов. В частности, на данном сайте опубликована подробная статья, посвященная основам администрирования. Данная статья включает в себя вводную информацию о кроссплатформенных

технологиях удаленного доступа, подробное описание всех основных операций над ними, сопровождаемых примерами.

Статья Покровского П. И. «Развертывание сети VPN» [18] рассматривает пример крупной компании, в которой имелась разветвленная сеть удаленных площадок, где потребовалось развернуть виртуальную частную сеть и наладить шифрование информации между центральным и удаленными офисами, чтобы каждый филиал мог связываться с другим через защищенное соединение. Цель статьи была проектирование схемы организации VPN.

На ресурсе «Для системных администраторов» в статье «Введение в архитектуру MPLS» [6] изучается технология быстрой коммутации пакетов в многопротокольных сетях, основанная на использовании меток. По мере появления новых мультимедийных приложений типа IP-телефонии, требующих более высоких скоростей передачи и поддержки более широкой полосы пропускания, возникла потребность в создании технологий и устройств, обеспечивающих возможность быстрой коммутации на уровне 2 (уровне звена данных) и уровне 3 (сетевом уровне) аппаратными средствами. Появились устройства коммутации на уровне 2, решающие проблему узких мест коммутации в среде LAN, а также новые маршрутизаторы, улучшающие ситуацию с маршрутизацией на уровне 3 путем перевода в быстродействующую аппаратную реализацию процедур просмотра маршрутных таблиц для пересылки пакетов. Достигли своего апогея наиболее перспективные технологии 90-х годов Frame Relay и ATM. Появились разнообразные средства обеспечения качества обслуживания DiffServ и IntServ, рассматриваемый в этой книге протокол резервирования RSVP и многое другое.

Динамичный рост рынка услуг VPN-сетей обусловлен множеством различных факторов. Это рассматривается в статье ресурса «Коннект» – ««IP VPN: осознанная необходимость». [10] Снижение темпов макроэкономического роста заставляет компании искать пути сокращения затрат и повышения эффективности работы своих сетей связи. Рассмотрены способы ведения бизнеса: от традиционной модели «продажа - заказ - покупка» до таких мето-

дов, как «телепродажи» и «online-закупки», что способствует внедрению виртуальных частных сетей на основе сетей пакетной коммутации (например, Интернет).

Ресурс «CyberForum» [28] — это форум начинающих и профессиональных программистов, системных администраторов, администраторов баз данных, форум по электронике и бытовой технике, компьютерный форум, обсуждение софта. Бесплатная помощь в решении задач по программированию и наукам, решение проблем с компьютером, операционными системами. Он содержит также огромный раздел и по Cisco Packet Tracer. Его преимущество в отличии от других подобных ресурсов в том, что информации здесь представлено больше, чем на других подобных форумах, а количество уже отвеченных вопросов измеряется сотнями.

Ресурс «Stackoverflow» [31] содержит огромное количество публичных решений задач и вопросов, связанных с сетевыми протоколами. Следует отметить, что данный ресурс не является «Решебником для задач», а больше нацелен на обмен опытом среди системных администраторов и детальным разбором работы тех или иных технологий удаленного доступа.

На обучающем портале «Интуит» [14] расположено множество курсов, в том числе бесплатных, направленных на получение знаний в сфере работы с кроссплатформенными технологиями удаленного доступ. В частности, в рамках курса «Сетевые технологии» обсуждаются типы протоколов, допускаемые в Cisco Packet Tracer, средства определения объектов схемы работы протокола, манипулирование данными, управление соединениями, сессиями и транзакциями, обеспечение безопасности Cisco. Отдельный раздел данного курса посвящен кроссплатформенным технологиям удаленного доступа, реализованными на Cisco Packet Tracer. Также за каждой темой следует тест, проверяющий изученный материал. Несмотря на это, следует отметить, что форма тестирования не предполагает решения обучающимся практических задач, а лишь набор вопросов с несколькими заранее определенными вариантами ответов на выбор, что не позволяет закрепить практические навыки.

Сайт «Networkdoc» [30] содержит подробное описание всех основных технологий удаленного доступа, с большим количеством примеров. Отдельно стоит отметить, что в данном ресурсе имеется огромное количество уроков, связанных с компьютерными сетями. Кроме того, принцип работы также показан схематично, что несомненно упрощает восприятие материала.

Ресурс «Открытые системы» [16] создан в 1993 году для комплексной информационной поддержки профессионалов, отвечающих за построение масштабных компьютерных систем, своей основной целью видит предоставление полной и качественной информации для различных категорий своих читателей. С самого момента основания на данном ресурсе информация, которая публикуется на сайте, отвечает высочайшим требованиям. Тесное сотрудничество с такими мировыми издателями технической литературы и профессиональной прессы как IDG, позволяет поддерживать высочайший профессиональный уровень и обеспечить актуальность публикаций.

Таким образом, анализ печатной литературы и Интернет-источников показал, позволил выявить, где находится более актуальная информация, на данный момент.

1.2 Анализ рабочей программы

Учебная дисциплина «Компьютерные коммуникации и сети» включена в учебный план по подготовке бакалавров по направлению 44.03.04 «Профессиональное обучение (по отраслям)». Дисциплина «Компьютерные коммуникации и сети» входит в вариативную часть дисциплин профессионального цикла ФГОС по направлению подготовки 44.03.04 «Профессиональное обучение (по отраслям)».

Целью освоения дисциплины является знакомство с различными сетевыми технологиями, а также спецификой их использования в различных видах профессиональной деятельности.

Предлагаемый курс обучения предназначен для формирования у студентов представления о назначении и возможностях компьютерных коммуникациях и сетях различных типов и умений их эффективного применения в профессиональной деятельности.

В дальнейшем полученные знания позволяют студентам проектировать, разрабатывать и администрировать web-сервера в различных сферах профессиональной деятельности.

На практических занятиях работа студентов предусматривает формирование умения использования основных свойств сетей и серверов, навыков практического использования данных знаний для решения различных прикладных задач.

В учебном плане подготовки бакалавров на изучение дисциплины «Компьютерные коммуникации и сети» отводится 208 часов, из них 126 аудиторных часов. Дисциплина изучается на третьем и четвертом курсе, в шестом и седьмом семестрах. Предусмотрены лекционные и лабораторные занятия в компьютерном классе. По окончании изучения дисциплины предполагается экзамен. План изучения дисциплины приведен в таблице 1.

Таблица 1 – План изучения дисциплины «Компьютерные коммуникации и сети»

Виды учебной работы	Объем учебной работы в часах
1. Общая трудоемкость дисциплины	324
2. Аудиторные занятия	116
2.1. Лекции	34
2.2. Лабораторные занятия	82
3. Самостоятельная работа	208

План изучения раздела «Технологии удаленного доступа» представлен в таблице 2.

Таблица 2 – План изучения раздела «Технологии удаленного доступа»

Виды учебной работы	Объем учебной работы в часах.
Лекции	2
Лабораторные занятия	6
Самостоятельная работа	14

В преподавании дисциплины «Компьютерные коммуникации и сети» используются следующие формы:

- лекции;
- лабораторные работы, в рамках которых решаются задачи, обсуждаются вопросы лекций и домашних заданий;
- проводятся контрольные работы;
- экспресс-диагностика и тестирование по отдельным темам дисциплины;
- самостоятельная работа студентов, включающая усвоение теоретического материала, выполнение домашних заданий, выполнение и подготовка к защите домашних заданий; подготовка к текущему контролю знаний;
- рейтинговая технология контроля учебной деятельности студентов для обеспечения их ритмичной работы в течение семестра;
- консультирование студентов по вопросам учебного материала;
- выполнения лабораторных и контрольных работ.

Задачи изучения дисциплины:

- познакомить студентов с различными видами кроссплатформенных технологий удаленного доступа, их возможностями, структурой и особенностями каждого типа;
- познакомить студентов с основами сетевых протоколов;
- способствовать формированию у студентов умений разрабатывать и администрировать схемы сетевых протоколов.

Дисциплина формирует культуру и ответственное отношение к профессиональной деятельности, поскольку она является базовой для многих форм деятельности и без нее немыслимо современное производство в любой

сфере жизни. Участие в сложных совместных разработках требует выработки внимательного отношения исполнителей друг к другу, умения поступиться собственными удобствами ради успешного функционирования совместно созданного продукта.

По окончании изучения курса студент должен:

1. Знать:
   - историю развития технологий удаленного доступа;
   - характерные особенности сетевых протоколов;
   - особенности настройки каждого протокола;
   - для чего используется та или иная технология удаленного доступа;
   - какие технологии применяются при настройке каждого сетевого протокола;
   - команды для настройки сетевых протоколов;
   - приводить примеры практического применения VPN, SSH, TELNET, RAVPN.
2. Уметь:
   - создавать схемы RAVPN;
   - конфигурирование ISP и VPN-роутеры;
   - настраивать VPN, SSH, TELNET и Remote Access VPN;
   - настраивать статическую маршрутизацию;
   - осуществлять проверку работоспособности удаленного доступа VPN, SSH, TELNET.
3. Владеть:
   - основными навыками работы в программе Cisco Packet Tracer;
   - навыками настройки всех основных кроссплатформенных технологий удаленного доступа;
   - способами работы с настольными и клиент-серверными системами в ранге администратора сервера.

В соответствии с ФГОС ВО, у выпускника, освоившего программу бакалвриата должны обладать следующими **общепрофессиональными компетенциями:**

- способностью проектировать и осуществлять индивидуально-личностные концепции профессионально-педагогической деятельности (ОПК-1);
- способностью выявлять естественнонаучную сущность проблем, возникающих в ходе профессионально-педагогической деятельности (ОПК-2);
- способностью осуществлять письменную и устную коммуникацию на государственном языке и осознавать необходимость знания второго языка (ОПК-3);
- способностью осуществлять подготовку и редактирование текстов, отражающих вопросы профессионально-педагогической деятельности (ОПК-4);
- способностью самостоятельно работать на компьютере (элементарные навыки (ОПК-5);
- способностью к когнитивной деятельности (ОПК-6);
- способностью обосновать профессионально-педагогические действия (ОПК-7);
- готовностью моделировать стратегию и технологию общения для решения конкретных профессионально-педагогических задач (ОПК-8);
- готовностью анализировать информацию для решения проблем, возникающих в профессионально-педагогической деятельности (ОПК-9)
- владением системой эвристических приемов и методов (ОПК-10).

1.3 Описание технологий удаленного доступа

VPN — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой се-

ти (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений) [13].

Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP, UDP).

Пользователи Microsoft Windows обозначают термином VPN одну из реализаций виртуальной сети — PPTP, причём используемую зачастую не для создания частных сетей.

Чаще всего для создания виртуальной сети используется инкапсуляция протокола PPP в какой-нибудь другой протокол — IP (такой способ использует реализация PPTP — Point-to-Point Tunneling Protocol) или Ethernet (PPPoE) (хотя и они имеют различия). Технология VPN в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» на постсоветском пространстве для предоставления выхода в Интернет.

При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации. При правильной настройке всех компонентов технология VPN обеспечивает анонимность в Сети.

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет). Возможно также подключение к виртуальной сети отдельного компьютера. Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети.

При подключении удалённого пользователя (либо при установке соединения с другой защищённой сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов удалённый пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс авторизации.

SSH — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов). Схож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем [21].

SSH позволяет безопасно передавать в незащищённой среде практически любой другой сетевой протокол. Таким образом, можно не только удалённо работать на компьютере через командную оболочку, но и передавать по шифрованному каналу звуковой поток или видео (например, с вебкамеры). Также SSH может использовать сжатие передаваемых данных для последующего их шифрования, что удобно, например, для удалённого запуска клиентов X Window System.

Большинство хостинг-провайдеров за определённую плату предоставляют клиентам доступ к их домашнему каталогу по SSH. Это может быть удобно как для работы в командной строке, так и для удалённого запуска программ (в том числе графических приложений).

Первая версия протокола, SSH-1, была разработана в 1995 году исследователем Тату Улёненом из Технологического университета Хельсинки (Финляндия). SSH-1 был написан для обеспечения большей конфиденциальности, чем протоколы rlogin, telnet и rsh. В 1996 году была разработана более безопасная версия протокола, SSH-2, несовместимая с SSH-1. Протокол приобрел ещё большую популярность, и к 2000 году у него было около двух

миллионов пользователей. В настоящее время под термином «SSH» обычно подразумевается именно SSH-2, т.к. первая версия протокола ввиду существенных недостатков сейчас практически не применяется.

В 2006 году протокол был утвержден рабочей группой IETF в качестве Интернет-стандарта.

Однако в некоторых странах (Франция, Россия, Ирак и Пакистан) требуется специальное разрешение в соответствующих структурах для использования определённых методов шифрования, включая SSH.

Распространены две реализации SSH: частная коммерческая и бесплатная свободная. Свободная реализация называется OpenSSH. К 2006 году 80 % компьютеров сети Интернет использовало именно OpenSSH. Частная реализация разрабатывается организацией SSH Communications Security, которая является стопроцентным подразделением корпорации Tectia, она бесплатна для некоммерческого использования. Эти реализации содержат практически одинаковый набор команд.

Протокол SSH-1, в отличие от протокола telnet, устойчив к атакам прослушивания трафика («снифинг»), но неустойчив к атакам «человек посередине». Протокол SSH-2 также устойчив к атакам путём присоединения посередине (англ. session hijacking), так как невозможно включиться в уже установленную сессию или перехватить её.

Для предотвращения атак «человек посередине» при подключении к хосту, ключ которого ещё не известен клиенту, клиентское ПО показывает пользователю «слепок ключа» (англ. key fingerprint). Рекомендуется тщательно сверять показываемый клиентским ПО «слепок ключа» со слепком ключа сервера, желательно полученным по надёжным каналам связи или лично.

Поддержка SSH реализована во всех UNIX-подобных системах, и на большинстве из них в числе стандартных утилит присутствуют клиент и сервер ssh. Существует множество реализаций SSH-клиентов и для не-UNIX ОС. Большую популярность протокол получил после широкого развития анализа-

торов трафика и способов нарушения работы локальных сетей, как альтернативное небезопасному протоколу Telnet решение для управления важными узлами.

Для работы по SSH нужен SSH-сервер и SSH-клиент. Сервер прослушивает соединения от клиентских машин и при установлении связи производит аутентификацию, после чего начинает обслуживание клиента. Клиент используется для входа на удалённую машину и выполнения команд.

Для соединения сервер и клиент должны создать пары ключей — открытых и закрытых — и обменяться открытыми ключами. Обычно используется также и пароль.

TELNET — сетевой протокол для реализации текстового интерфейса по сети (в современной форме — при помощи транспорта TCP). Название «telnet» имеют также некоторые утилиты, реализующие клиентскую часть протокола. Современный стандарт протокола описан в RFC 854. Выполняет функции протокола прикладного уровня модели OSI [15].

Хотя в сессии Telnet выделяют клиентскую и серверную стороны, протокол на самом деле полностью симметричен. После установления транспортного соединения (как правило, TCP) оба его конца играют роль «сетевых виртуальных терминалов» (англ. Network Virtual Terminal, NVT), обменивающихся двумя типами данных:

- прикладными данными (то есть данными, которые идут от пользователя к текстовому приложению на стороне сервера и обратно);
- ккомандами протокола Telnet, частным случаем которых являются опции, служащие для уяснения возможностей и предпочтений сторон.

Хотя Telnet-сессии, выполняющейся по TCP, свойственен полный дуплекс, NVT должен рассматриваться как полудуплексное устройство, работающее по умолчанию в буферизированном строковом режиме.

Прикладные данные проходят через протокол без изменений, то есть на выходе второго виртуального терминала мы видим именно то, что было введено на вход первого. С точки зрения протокола данные представляют про-

сто последовательность байтов (октетов), по умолчанию принадлежащих набору ASCII, но при включенной опции Binary — любых. Хотя были предложены расширения для идентификации набора символов, но на практике ими не пользуются.

Все значения октетов прикладных данных кроме \377 (десятичное: 255) передаются по транспорту как есть. Октет \377 передаётся последовательностью \377\377 из двух октетов. Это связано с тем, что октет \377 используется на транспортном уровне для кодирования опций.

1.4 Удаленный доступ в корпоративных сетях

Удаленный доступ — очень широкое понятие, которое включает в себя различные типы и варианты взаимодействия компьютеров, сетей и приложений. Существует огромное количество схем взаимодействия, которые можно назвать удаленным доступом, но их объединяет использование глобальных каналов или глобальных сетей при взаимодействии. Кроме того, для удаленного доступа, как правило, характерна несимметричность взаимодействия, то есть с одной стороны имеется центральная крупная сеть или центральный компьютер, а с другой — отдельный удаленный терминал, компьютер или небольшая сеть, которые должны получить доступ к информационным ресурсам центральной сети. За последние годы количество предприятий, имеющих территориально распределенные корпоративные сети, значительно возросло. Поэтому для современных средств удаленного доступа очень важны хорошая масштабируемость и поддержка большого количества удаленных клиентов [3].

Еще недавно для удаленного управления корпоративными сетями применялись фирменные решения, отличающиеся использованием собственных протоколов передачи данных по телефонным сетям и собственных методов аутентификации удаленных пользователей, а также оригинальными способами предоставления ресурсов центральной сети. Это вызывало определенные

проблемы и при необходимости «сращивания» двух сетей, имевших прежде различную конфигурацию средств управления сетью, и при подготовке специалистов, и в других ситуациях. Сейчас в системах управления работает все больше стандартных компонентов: протокол передачи данных PPP; «джентльменский набор» средств аутентификации — с помощью систем Kerberos, Novell NDS или MicrosoftDirectoryServices; предоставление информационных ресурсов удаленным пользователям с помощью службы WWW или тех же сервисов, которые работают и в локальной сети. Этот процесс облегчает взаимодействие серверов удаленного доступа с клиентами и сетевыми операционными системами, работающими в локальной сети. Хотя до полной стандартизации еще далеко, за последние несколько лет ситуация изменилась коренным образом.

Повышение скорости доступа. Основные усилия операторов телекоммуникационных сервисов сегодня направлены на преодоление для массовых пользователей ограничения в 56,2 Кбит/с, накладываемого аналоговыми модемами. Кроме того, передача информации через сеть Интернет является небезопасной. Поэтому идеальным вариантом было бы создание виртуальной частной сети — VPN.

Подключение корпоративной сети к Internet оправданно в том случае, если вам нужен доступ к соответствующим услугам. Использовать Internet как среду передачи данных стоит только тогда, когда другие способы недоступны и когда финансовые соображения перевешивают требования надежности и безопасности [5].

Одной из наиболее широко обсуждаемых проблем удаленного администрирования является именно безопасность. Если допускается возможность удаленного управления вашей сетью, то какой бы технологией вы ни пользовались, появится ряд проблем, связанных с обеспечением безопасности передающейся по сети информации.

Как показывает практика, случаи взлома сети все еще довольно часто встречаются. Повторим еще раз, какие опасности могут угрожать частной се-

ти при использовании той или иной технологии передачи данных. Прежде всего это перехват информации при передаче. Здесь могут помочь средства шифрования, которые решают проблему лишь частично, поскольку применимы в основном к почте и передаче файлов. Решения же, позволяющие с приемлемой скоростью шифровать информацию в реальном времени (например, при непосредственной работе с удаленной базой данных или файл-сервером), пока малодоступны и дороги. Есть средство защиты от несанкционированного доступа к сети — Firewall (межсетевой экран). Однако, любую защиту можно сломать, особенно если полученная информация окупает стоимость взлома. Таким образом, рекомендовать Internet как основу для систем, в которых требуется надежность и закрытость, можно лишь в крайнем случае и при использовании всех мер защиты, включая межсетевые экраны, шифрование канала и VPN. Кроме того, не стоит забывать и о человеческом факторе — о сотрудниках «внутри» и «снаружи» корпоративной сети [18].

Для организации удаленного доступа можно использовать технологии X.25 и Frame Relay, которые предоставляют ряд весьма интересных возможностей. Проблема несанкционированного доступа также может достаточно эффективно решаться средствами самой сети. Сегодня существуют средства шифрования, которые созданы специально для сетей X.25 и Frame Relay и позволяют работать на достаточно высоких скоростях. Такое оборудование производят компании Racal, Cylink, Siemens. Есть и отечественные разработки, созданные под эгидой ФАПСИ. Существуют разработки и для сетей на основе протокола IP.

Первые три вида удаленного доступа часто объединяют понятием индивидуального доступа, а схемы доступа «сеть-сеть» иногда делят на два класса — ROBO (RegionalOffice/BranchOffice) и SOHO (SmallOffice/ HomeOffice). Класс ROBO соответствует случаю подключения к центральной сети сетей средних размеров — сетей региональных подразделений предпри-

ятия, а классу SOHO — случаю удаленного доступа сетей небольших офисов и домашних сетей.

Особое место среди всех видов удаленного доступа к компьютеру занимает способ, при котором пользователь получает возможность удаленно работать с компьютером так же, как если бы он управлял им с помощью локально подключенного терминала. В этом режиме он может запускать программы на удаленном компьютере и видеть результаты их выполнения. При этом такой способ доступа принято разделять на терминальный доступ и на удаленное управление. Хотя это близкие режимы работы, но в описании продуктов удаленного доступа их не принято объединять в один класс. Обычно под терминальным доступом понимают символьный режим работы пользователя с удаленными многопользовательскими ОС — UNIX, VAXVMS, ОС мэйнфреймов IBM. В класс удаленного управления включают программы эмуляции графического экрана ОС персональных компьютеров — в первую очередь разных версий Windows, а в последнее время к этому классу можно отнести Linux-системы, Solaris и др.

Многие производители операционных систем предусмотрели в своих стеках протоколов средства терминального доступа пользователей к компьютерам по сети. Эти средства позволяют пользователю, работающему за компьютером, подключенным к сети, превратить экран своего монитора в эмулятор терминала другого компьютера, также подключенного к сети. Наиболее популярным средством такого типа является протокол Telnet стека TCP/IP, появившегося в рамках операционной системы UNIX и с тех пор неразрывно с нею связанного.

В отличие от систем терминального доступа, средства поддержки режима удаленного узла (remote node) делают вызывающую машину полноправным звеном локальной сети. Это достигается за счет того, что на удаленном компьютере работает тот же стек протоколов, что и в компьютерах центральной локальной сети, за исключением протоколов канального и физического уровня. На этом уровне вместо традиционных протоколов Ethernet или

Token Ring работают модемные протоколы (физический уровень) и канальные протоколы соединений «точка-точка», такие как SLIP, HDLC и PPP. Эти протоколы используются для передачи по телефонным сетям пакетов сетевого и других протоколов верхних уровней. Таким образом, осуществляется полноценная связь удаленного узла с остальными узлами сети [16].

Сервис удаленного узла обеспечивает ему транспортное соединение с локальной сетью, поэтому на удаленном узле могут использоваться все сервисы, которые доступны локальным клиентам сети, например, файл-сервис NetWare, сервис Telnet или X-Window ОС UNIX, администрирование Windows NT.

Наибольшие сложности вызывает удаленное управление популярными настольными операционными системами семейства Windows, OS/2 и т.п. Это связано с тем, что для данных систем нет стандартного протокола эмуляции терминала, подобного Telnet или X-Window для UNIX или LAT для VAXVMS. Кроме того, эти операционные системы наиболее знакомы конечному пользователю, и ему было бы очень удобно использовать привычный графический интерфейс Windows при управлении удаленным хостом. Поэтому именно средствам удаленного управления, встроенным в ОС семейств UNIX, Windows и NetWare, а также созданным третьими фирмами-разработчиками, будет посвящена оставшаяся часть этой статьи.

UNIX можно назвать операционной системой, хорошо приспособленной для задач системного и сетевого администрирования, но гораздо хуже — для офисных приложений. Поскольку речь идет о системе удаленного администрирования, а не о настольной системе, можно сказать, что благодаря сервисам Telnet любой имеющий на то право пользователь может управлять сетью из любой точки земного шара, запустив на своем компьютере удаленный терминал. Единственный серьезный недостаток такого подхода — высокие требования к квалификации администратора: он должен хорошо владеть утилитами командной строки.

В последнее время эта ситуация меняется в лучшую сторону — появляются клиент-серверные приложения, позволяющие удаленно администрировать UNIX/Linux-системы в графическом режиме. Примером может служить VNC Server для Suse Linux.

Telnet входит в число стандартов, которых насчитывается три десятка на полторы тысячи рекомендуемых официальных материалов сети, называемых RFC (Request For Comments).

Изначально под Telnet подразумевалась триада, состоящая из: Telnet-интерфейса пользователя, Telnet-процесса и Telnet-протокола.

Telnet строится как протокол приложения над транспортным протоколом TCP. При установке telnet-соединения программа, работающая с реальным терминальным устройством, и процесс обслуживания этой программы используют для обмена информацией сетевой виртуальный терминал (Network Virtual Terminal, NVT) — стандартное описание наиболее широко используемых возможностей реальных физических терминальных устройств. NVT позволяет описать и преобразовать в стандартную форму способы ввода и вывода информации. Терминальная программа (user) и процесс (server), работающий с ней, преобразуют характеристики физических устройств в спецификацию NVT, что позволяет обеспечить принцип совместимости устройств с разными возможностями.

Принцип договорных опций или команд позволяет согласовать возможности вывода информации на терминальных устройствах. NVT — это минимально необходимый набор параметров, который позволяет работать по Telnet даже самым допотопным устройствам. Реально используемые современные устройства обладают гораздо большими возможностями вывода информации, и принцип договорных команд позволяет использовать эти возможности.

Взаимодействие по протоколу Telnet симметрично, что позволяет в течение одной сессии программе-user и программе-server меняться местами. Это принципиально отличает взаимодействие в рамках Telnet от традицион-

ной схемы «клиент-сервер». Если же речь идет об обмене информацией между двумя терминальными программами в режиме «терминал-терминал», то каждая из сторон может выступать инициатором изменения принципов представления информации и при этом здесь проявляется еще одна особенность протокола Telnet. Протокол использует не принцип «запрос — подтверждение», а принцип «прямого действия». Это значит, что если терминальная программа хочет расширить возможности представления информации, то она делает это (например, вставляет в информационный поток Esc-последовательности), а если в ответ она получает информацию в новом представлении, то это обозначает удачную попытку, в противном случае происходит возврат к стандарту NVT [16].

Однако у Telnet есть достаточно серьезные минусы — проблемы с безопасностью. Он не имеет никаких прав на чтение/запись информации и не идентифицируется системой UNIX. Сложность удаленного администрирования сервера Windows NT всегда удручала системных администраторов, сталкивавшихся с этой задачей. Этот пробел восполняется рядом продуктов третьих фирм-разработчиков. Но существует также несколько пакетов для управления настольными системами на базе Windows, созданных разработчиками фирмы Microsoft.

Один из них — Systems Management Server (SMS) 2.0, который тесно интегрирован с СУБД Microsoft SQL Server и программой Crystal Reports и имеет широкие возможности в плане управления информацией. Кроме того, в SMS имеется возможность планирования процесса сопровождения базы данных.

Для управления рабочими станциями в состав операционной системы NetWare 5 входит пакет Z.E.N. works (Zero Effort Networking, — работа в сети с нулевыми усилиями. Для облегчения управления рабочими столами Windows пакет Z.E.N. works тесно интегрирован со службой справочника NDS. Этот пакет хорошо подходит также для территориально распределен-

ных сервисных центров, серверы которых могут хранить копии разделов NDS.

Системный администратор может настраивать рабочий стол пользователя, используя две специальные политики Z.E.N. works: системную политику пользователя (в пакете политик пользователя) и системную политику компьютера (в пакете политик рабочей станции). Соответственно системная политика пользователя позволяет настроить функции рабочего стола, которые будут доступны определенному пользователю, а политика компьютера — настроить параметры Windows каждой рабочей станции. Большим плюсом Z.E.N. works является возможность конфигурировать пользовательскую среду печати при помощи NDS. Можно автоматически загружать необходимый драйвер печати для каждого пользователя, когда он регистрируется в сети. Также существует возможность настраивать профили пользователей, то есть такие настройки рабочего стола, как обои, заставка и звуки, могут быть стандартизованы и разосланы всем пользователям предприятия.

Пакет Z.E.N. works содержит специальную версию средства запуска приложений (NAL), позволяющую распространять сетевые приложения по рабочим станциям пользователей и управлять ими как объектами дерева NDS. Реализованы такие решения, как отказоустойчивость и выравнивание нагрузки, гарантирующие доступ пользователя к нужному приложению [3].

UNIX/Linux-системы изначально приспособлены к дистанционному управлению. Сложилось так, что первыми UNIX-машинами были дорогие мини-компьютеры, к которым через последовательные порты подключалось множество терминалов. Даже сегодня, когда UNIX обзавелась графическим интерфейсом, установка сеанса связи остается одинаково простой на удаленной и на локальной машине (при условии, что пользователь имеет право на запуск сеанса с удаленного хоста).

Средств сетевого администрирования, представленных в большинстве Windows-систем достаточно на уровне пользователя и рабочей группы. Однако, они уступают по разнообразию поддерживаемых функций продуктам

независимых разработчиков. Так, например, Windows NT Server хорош для администрирования сервера и пользователей по отношению к разделяемым ресурсам, но игнорирует множество других задач, таких, например, как контроль за лицензиями. В состав Windows NT входит приложение сетевого мониторинга для контроля соответствия количества пользователей или подключений в сети числу приобретенных лицензий, но оно не в состоянии делать то же самое для других приложений, выполняющихся на сервере или рабочих станциях [9].

1.5 Общие требования по созданию лабораторных практикумов

Лабораторный практикум — существенный элемент учебного процесса в вузе, в ходе которого обучающиеся фактически впервые сталкиваются с самостоятельной практической деятельностью в конкретной области. Лабораторные занятия, как и другие виды практических занятий, являются средним звеном между углубленной теоретической работой обучающихся на лекциях, семинарах и применением знаний на практике. Основное назначение лабораторного практикума для обучающихся — систематизация знаний, полученных обучаемыми при изучении дисциплины [2].

Любое учебное пособие в системе непрерывного образования должно содержать в себе стройную систему замечаний методического характера, включать в себя достаточно полную систему упражнений и текстовых заданий по всем основным разделам, а также обширный перечень итоговых тематических контрольных работ и тестов по всем разделам.

Перед разработчиком педагогического программного средства стоят следующие основные задачи:

1. Разработать программный продукт, доступный для непрограммирующего пользователя и необходимый для проведения учебного процесса в условиях использования новых информационных технологий.

2. Подготовить конкретный набор планов занятий с использованием этого продукта.

3. Апробировать разрабатываемое педагогическое программное средство.

Дидактические требования к лабораторным практикумам решают задачу необходимого уровня обучения [11]:

1. Научность содержания — обеспечение возможности построения содержания учебной деятельности с учетом основных принципов педагогики, психологии и т.д.

2. Адаптивности — возможность любого способа управления учебной деятельностью, выбор которого обусловлен, с одной стороны, теоретическими воззрениями разработчиков лабораторного практикума, а с другой – целями обучения.

3. Обеспечение мотивации — стимулирование постоянной и высокой мотивации обучаемых, подкрепляемой целенаправленностью, активными формами работы, наглядностью, своевременной обратной связью.

4. Целенаправленность — обеспечение обучаемого постоянной информацией о ближайших и отдалённых целях обучения, степени достижения целей; стимуляции тех видов познавательной активности обучаемых, которые необходимы для достижения основных учебных целей.

5. Наличие входного контроля — диагностика обучаемого перед началом работы с целью обеспечения индивидуализации обучения, а также оказания требуемой первоначальной помощи.

6. Креативность — программа должна формировать логическое и системное мышление, обеспечивать подготовку специалистов с творческим потенциалом, способных видеть противоречия, а также самостоятельно ставить и решать проблемы.

7. Индивидуализация обучения — содержание учебного предмета и трудность учебных задач должны соответствовать возрастным возможностям

и индивидуальным особенностям обучаемых и строиться с учётом их уже приобретенных знаний и умений.

8. Обеспечение систематической обратной связи — обратная связь должна быть педагогически оправданной, не только сообщать о допущенных ошибках, но и содержать информацию достаточную для их устранения.

9. Педагогическая гибкость — программа должна позволять обучаемому самостоятельно принимать решения о выборе стратегии обучения, характере помощи, последовательности и темпе подачи учебного материала; должна быть обеспечена возможность доступа к ранее пройденному учебному материалу, выхода из программы в любой ее точке.

К лабораторным практикумам предъявляются следующие технологические требования [23]:

1. Открытость — возможность модификации, внесения изменений в способы управления учебной деятельностью.

2. Наличие резервной системной помощи — система помощи должна быть многоуровневой, педагогически обоснованной, достаточной для того, чтобы решить задачу и усвоить способы её решения.

3. Наличие многоуровневой организации учебного материала, базы знаний и банка заданий — соблюдение этого требования позволяет организовать систему повторов по спирали с постоянной опорой на зону ближайшего развития, добавлением на каждом уровне повторения нового.

4. Наличие интеллектуального ядра — программные средства могут обеспечить такое ядро за счет реализации в них методов обработки данных, используемых при построении экспертных систем и средств искусственного интеллекта.

5. Обеспечение двустороннего диалога, управляемого не только компьютером, но и обучаемым — предоставление обучаемым возможности задавать вопросы.

6. Возможность возврата назад — при самостоятельной работе должна быть предусмотрена отмена обучаемым ошибочных действий.

7. Возможность документирования хода процесса обучения и его результатов — лабораторный практикум должен иметь модули, предназначенные для сбора и обработки необходимой информации разработчиком программы, а также руководством учебных заведений и специалистами системы управления образованием.

8. Наличие интуитивного понятного, дружелюбного интерфейса — программа должна адекватно использовать все способы представления информации в виде текста, графики, анимации, гипертекста, мультимедиа; обучаемый должен иметь возможность пролистывать информационный материал в обоих направлениях (вперед-назад).

9. Обеспечение получения твердой копии статических разделов программы.

10. Наличие развитой поисковой системы.

11. Наличие блока контроля утомления обучаемых, блока релаксации.

12. Надёжность работы и системная целостность — техническая корректность; защита от случайного или неправильного ввода данных.

При разработке интерфейса следует принимать во внимание две группы требований:

- определяемые существующими стандартами в области создания интерактивных приложений;
- определяемые психофизиологическими особенностями человека.

Как таковых законодательно утверждённых принципов построения пользовательского интерфейса нет [11].

Принцип пропорции. Данный принцип требует, чтобы различные объекты не были хаотично разбросаны по экрану.

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.

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

Принцип равновесия. Равномерное расположение по экрану оптической тяжести изображения.

Принцип единства. Элементы изображения должны выглядеть взаимосвязано, правильно соотноситься по размеру, форме, цвету. Идентичные данные должны быть представлены однотипно. Для достижения единства в целом используются рамки, оси, поля.

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 [23].

2 ОПИСАНИЕ ЛАБОРАТОРНОГО ПРАКТИКУМА

2.1 Педагогический адрес

Лабораторный практикум «Технологии удаленного доступа» предназначено для студентов третьего курса направления подготовки 44.03.04 «Профессиональное обучение (по отраслям)» профиля «Информатика и вычислительная техника» профилизации «Компьютерные технологии».

2.2 Программно-технические средства

Для создания лабораторного практикума «Технологии удаленного доступа использовались следующие программы:

Cisco Packet Tracer — симулятор сети передачи данных, выпускаемый фирмой Cisco Systems. Позволяет делать работоспособные модели сети, настраивать (командами Cisco IOS) маршрутизаторы и коммутаторы, взаимодействовать между несколькими пользователями [26]. Симулятор Cisco маршрутизатор может быть использован не только в профессиональной подготовке и образовании, но и в научных исследованиях для простой компьютерной сети моделирования.

Cisco Packet Tracer предоставляет возможности моделирования, визуализации, разработки, компьютерных сетей и облегчает изучение сложных технологических сетевых концепций.

Cisco Packet Tracer разработан компанией Cisco и рекомендован использоваться при изучении телекоммуникационных сетей и сетевого оборудования, а также для проведения уроков по лабораторным работам в высших заведениях [16].

Основные возможности Packet Tracer:

- дружественный графический интерфейс (GUI), что способствует к лучшему пониманию организации сети, принципов работы устройства;
- возможность смоделировать логическую топологию: рабочее пространство для того, чтобы создать сети любого размера на CCNA-уровне сложности;
- моделирование в режиме real-time (реального времени);
- режим симуляции;
- многоязычность интерфейса программы: что позволяет изучать программу на своем родном языке.
- усовершенствованное изображение сетевого оборудования со способностью добавлять / удалять различные компоненты;
- наличие Activity Wizard позволяет сетевым инженерам, студентам и преподавателям создавать шаблоны сетей и использовать их в дальнейшем.
- проектирование физической топологии: доступное взаимодействие с физическими устройствами, используя такие понятия как город, здание, стойка и т.д.

Широкий круг возможностей данного продукта позволяет сетевым инженерам: конфигурировать, отлаживать и строить вычислительную сеть. Также данный продукт незаменим в учебном процессе, поскольку дает наглядное отображение работы сети, что повышает освоение материала учащимися.

Эмулятор сети позволяет сетевым инженерам проектировать сети любой сложности, создавая и отправляя различные пакеты данных, сохранять и комментировать свою работу. Специалисты могут изучать и использовать такие сетевые устройства, как коммутаторы второго и третьего уровней, рабочие станции, определять типы связей между ними и соединять их [7].

На заключительном этапе, после того как сеть спроектирована, специалист может приступать к конфигурированию выбранных устройств посредством терминального доступа или командной строки.

Packet Tracer способен моделировать большое количество устройств различного назначения, а также немало различных типов связей, что позволяет проектировать сети любого размера на высоком уровне сложности [1].

Моделируемые устройства:

1. Коммутаторы третьего уровня:
   - Router 2620 XM;
   - Router 2621 XM;
   - Router-PT.
2. Коммутаторы второго уровня:
   - Switch 2950-24;
   - Switch 2950T;
   - Switch-PT;
   - соединение типа «мост» Bridge-PT.
3. Сетевые концентраторы:
   - Hub-PT;
   - повторитель Repeater-PT.
4. Оконечные устройства:
   - рабочая станция PC-PT;
   - сервер Server-PT;
   - принтер Printer-PT.

Так же целесообразно привести те протоколы, которые студент может отслеживать:

- ARP;
- CDP;
- DHCP;
- EIGRP;
- ICMP;
- RIP;
- TCP;

- UDP.

Как известно, локальная вычислительная сеть – это компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий. В нашем случае это всего-навсего 6 рабочих станций, определенным образом связанных между собой. Для этого используются сетевые концентраторы (хабы) и коммутаторы (свичи).

Notepad++ — свободный текстовый редактор с открытым исходным кодом для Windows с подсветкой синтаксиса большого количества языков программирования и разметки. Поддерживает открытие более 100 форматов. Базируется на компоненте Scintilla, написан на C++ с использованием STL, а также Windows API и распространяется под лицензией GNU General Public License [31].

Программа поставляется в двух версиях: UNICODE и ANSI, причём последний вариант доступен только при ручной распаковке архива. Плагины могут быть написаны под определённую версию программы, но чаще плагин работает в обеих версиях, хотя в последнее время акцент делается на UNICODE-версию, как наиболее перспективную.

HTML — стандартизированный язык разметки документов во Всемирной паутине. Большинство веб-страниц содержат описание разметки на языке HTML (или XHTML). Язык HTML интерпретируется браузерами; полученный в результате интерпретации форматированный текст отображается на экране монитора компьютера или мобильного устройства [29].

CSS — формальный язык описания внешнего вида документа, написанного с использованием языка разметки. Пример CSS-кода показан на рисунке 2. Главная особенность Notepad++ - поддержка плагинов, которые способствуют расширению базового функционала редактора. В программу интегрируются дополнительные плагины, позволяющие настроить проверку орфографии, автоматическое сохранение документов, симметричное и асимметричное шифрование текста, HEX-редактор, FTP-менеджер [27].

HTML используется создателями веб-страниц для задания цветов, шрифтов, расположения отдельных блоков и других аспектов представления внешнего вида этих веб-страниц (рисунок 1).

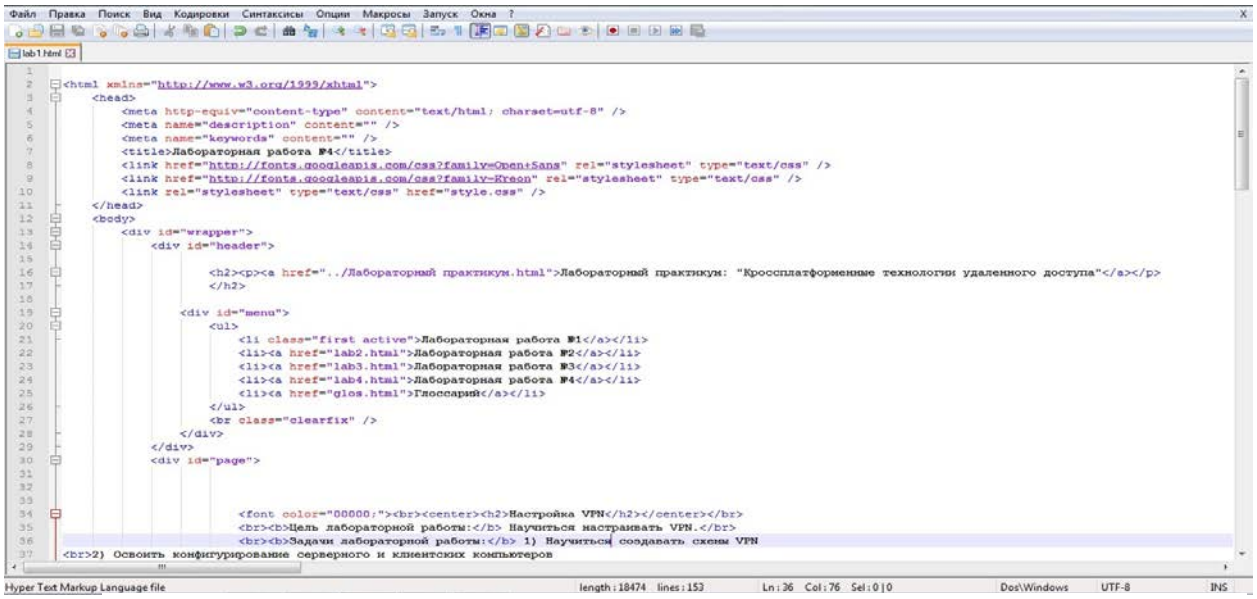


Рисунок 1 – Пример использования кодировки посредством программы Notepad ++

Основной целью разработки CSS являлось разделение описания логической структуры веб-страницы (которое производится с помощью HTML или других языков разметки) от описания внешнего вида веб-страницы которое теперь производится с помощью формального языка CSS (рисунок 2).

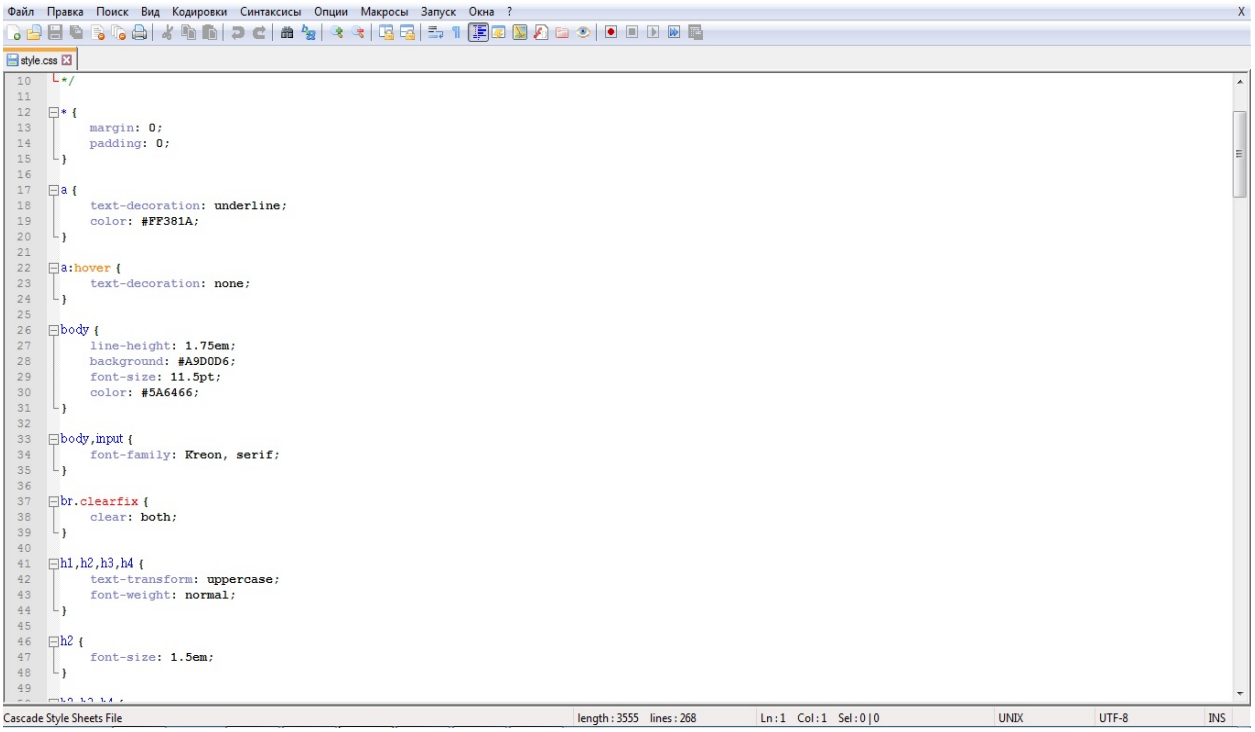


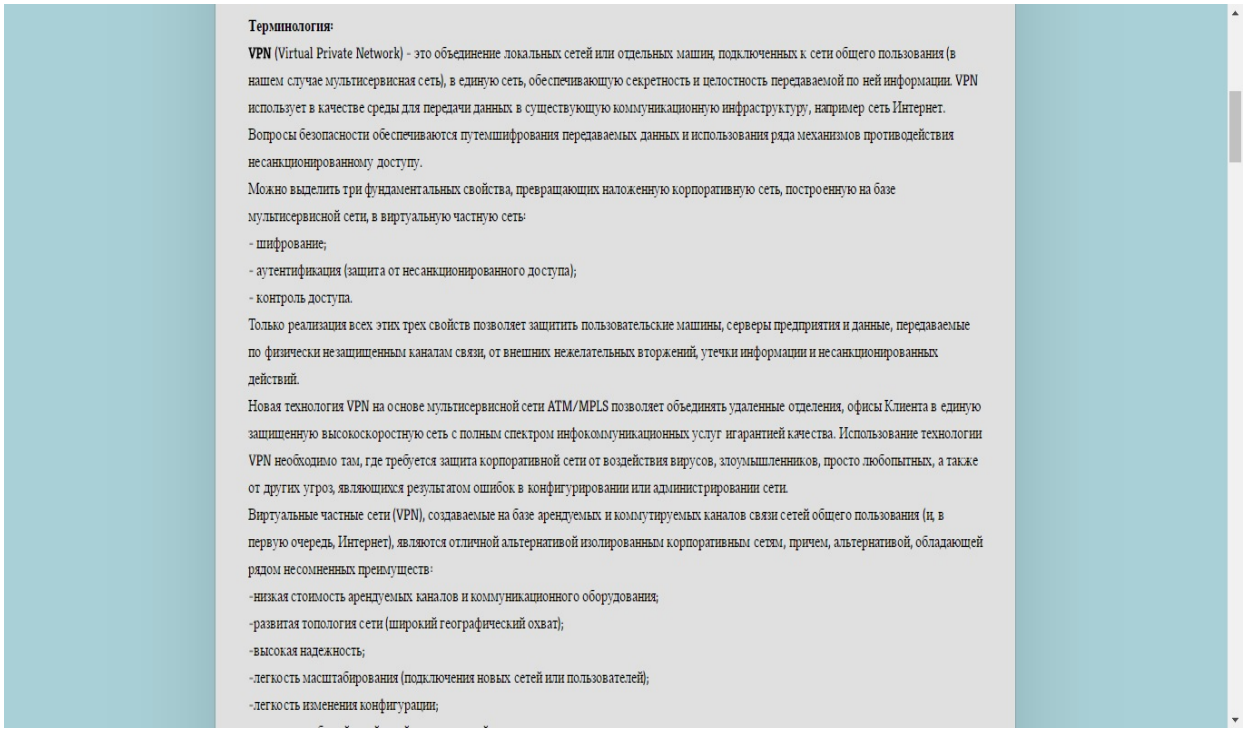
Рисунок 2 – Пример использования кода посредством программы Notepad++

2.3 Интерфейс и навигация

Данный лабораторный практикум был разработан средствами web-программирования и может работать в любом современном браузере. В ходе создания пособия были использованы технологии HTML и CSS. Вводная страница разработана в графическом редакторе Adobe Photoshop CS7 (рисунок 3).

Рисунок 3 – Вводная страница лабораторного практикума

Практикум содержит в себе пять пунктов: «Лабораторная работа №1», «Лабораторная работа №2», «Лабораторная работа №3», «Глоссарий» и «Справочные материалы» Пункты «Лабораторная работа №1-3» являются основным и включает в себя все шаги создания и настройки кроссплатформенных технологий удаленного доступа. Они направлены на проверку действующих знаний студента, т. к. в лабораторной работе студенту предлагается выполнить задания высокого уровня. Также, там предоставлен соответствующий материал, для выполнения работы, позволяющий студентам ознакомиться с новой темой. Материалы лабораторных работ не связаны между собой и можно приступать к выполнению любой из них (рисунок 4).



Терминология:

VPN (Virtual Private Network) - это объединение локальных сетей или отдельных машин, подключенных к сети общего пользования (в нашем случае мультисервисная сеть), в единую сеть, обеспечивающую секретность и целостность передаваемой по ней информации. VPN использует в качестве среды для передачи данных в существующую коммуникационную инфраструктуру, например сеть Интернет. Вопросы безопасности обеспечиваются путемшифрования передаваемых данных и использования ряда механизмов противодействия несанкционированному доступу.

Можно выделить три фундаментальных свойства, превращающих наложенную корпоративную сеть, построенную на базе мультисервисной сети, в виртуальную частную сеть:

- шифрование;
- аутентификация (защита от несанкционированного доступа);
- контроль доступа.

Только реализация всех этих трех свойств позволяет защитить пользовательские машины, серверы предприятия и данные, передаваемые по физически незащищенным каналам связи, от внешних нежелательных вторжений, утечки информации и несанкционированных действий.

Новая технология VPN на основе мультисервисной сети ATM/MPLS позволяет объединять удаленные отделения, офисы Клиента в единую защищенную высокоскоростную сеть с полным спектром инфокоммуникационных услуг игарантией качества. Использование технологии VPN необходимо там, где требуется защита корпоративной сети от воздействия вирусов, злоумышленников, просто любопытных, а также от других угроз, являющихся результатом ошибок в конфигурировании или администрировании сети.

Виртуальные частные сети (VPN), создаваемые на базе арендуемых и коммутируемых каналов связи сетей общего пользования (и, в первую очередь, Интернет), являются отличной альтернативой изолированным корпоративным сетям, причем, альтернативой, обладающей рядом несомненных преимуществ:

-низкая стоимость арендуемых каналов и коммуникационного оборудования;
-развитая топология сети (широкий географический охват);
-высокая надежность;
-легкость масштабирования (подключения новых сетей или пользователей);
-легкость изменения конфигурации;

Рисунок 4 – Пример материала для работы в Лабораторной работе №4

Пункт «Глоссарий» содержит общую теоретическую информацию, которая не относится к конкретной теме выполняемой лабораторной работы (рисунок 5).

ЛАБОРАТОРНАЯ РАБОТА №1 ЛАБОРАТОРНАЯ РАБОТА №2 ЛАБОРАТОРНАЯ РАБОТА №3

Глоссарий СПРАВОЧНЫЕ МАТЕРИАЛЫ

ТЕРМИНОЛОГИЯ К ЛАБОРАТОРНОЙ РАБОТЕ №1

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет). Возможно также подключение к виртуальной сети отдельного компьютера. Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети. При подключении удалённого пользователя (либо при установке соединения с другой защищённой сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов удалённый пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс авторизации. Site to Site VPN устанавливается в соответствии со следующими протоколами:

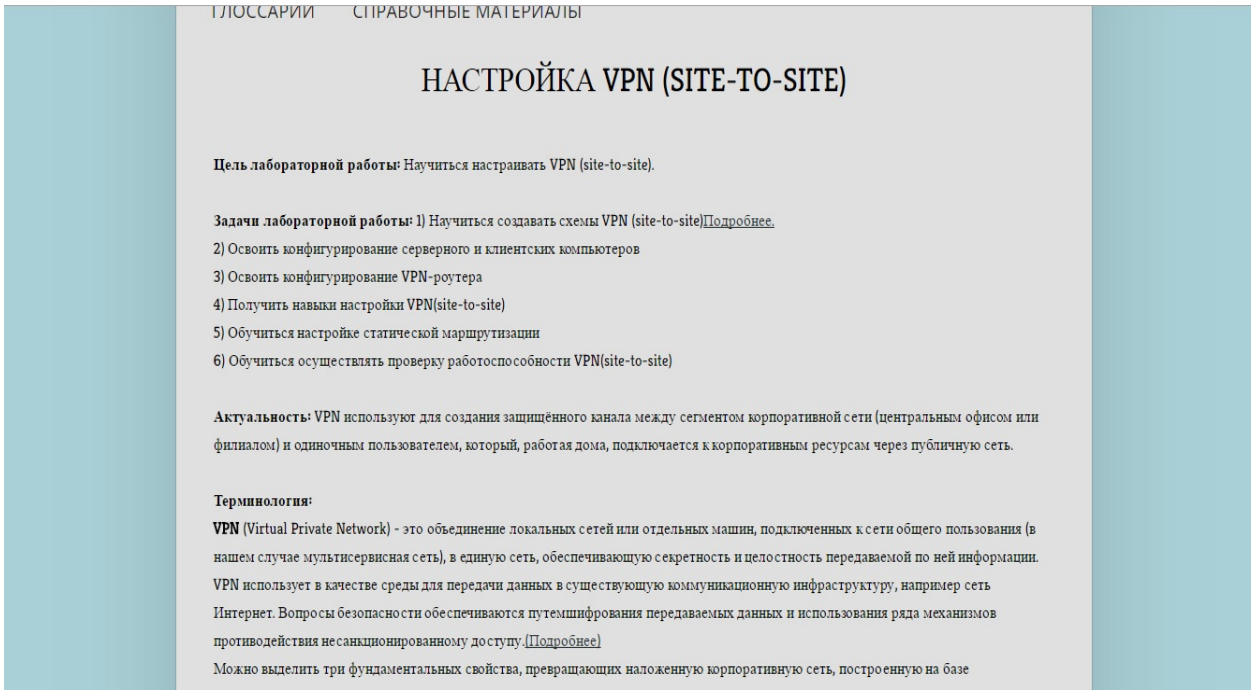
- IPSEC
- L2TP через IPSEC
- PPTP

Можно выделить три фундаментальных свойства, превращающих наложенную корпоративную сеть, построенную на базе мультисервисной сети, в виртуальную частную сеть:

- шифрование;

Рисунок 5 – Пример терминологии в пункте «Глоссарий»

В пункте «Лабораторная работа №1» студенту предлагается выполнить лабораторную работу, связанную с настройкой VPN (site-to-site) (рисунок 6).


ГЛОССАРИЙ СПРАВОЧНЫЕ МАТЕРИАЛЫ

НАСТРОЙКА VPN (SITE-TO-SITE)

Цель лабораторной работы: Научиться настраивать VPN (site-to-site).

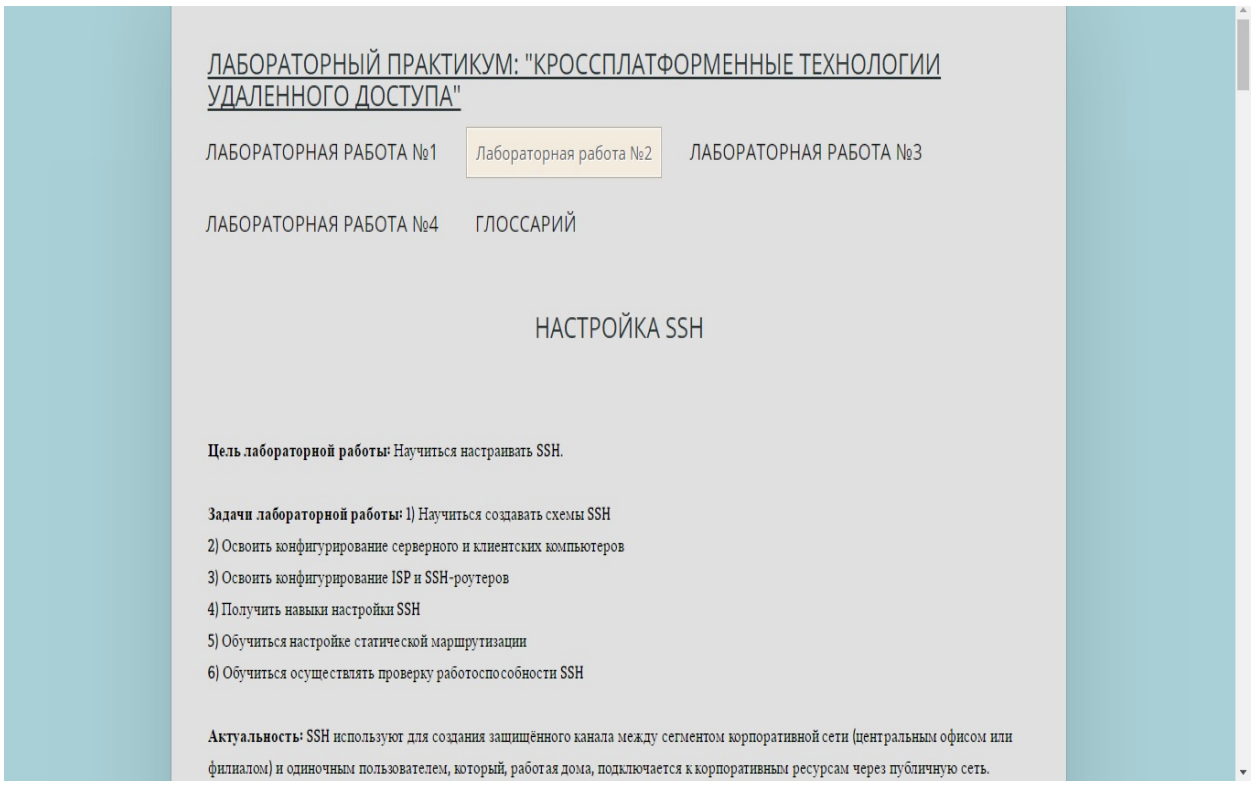
Задачи лабораторной работы: 1) Научиться создавать схемы VPN (site-to-site)Подробнее.
2) Освоить конфигурирование серверного и клиентских компьютеров
3) Освоить конфигурирование VPN-роутера
4) Получить навыки настройки VPN(site-to-site)
5) Обучиться настройке статической маршрутизации
6) Обучиться осуществлять проверку работоспособности VPN(site-to-site)

Актуальность: VPN используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам через публичную сеть.

Терминология:
VPN (Virtual Private Network) - это объединение локальных сетей или отдельных машин, подключенных к сети общего пользования (в нашем случае мультисервисная сеть), в единую сеть, обеспечивающую секретность и целостность передаваемой по ней информации. VPN использует в качестве среды для передачи данных в существующую коммуникационную инфраструктуру, например сеть Интернет. Вопросы безопасности обеспечиваются путемшифрования передаваемых данных и использования ряда механизмов противодействия несанкционированному доступу.(Подробнее)
Можно выделить три фундаментальных свойства, превращающих наложенную корпоративную сеть, построенную на базе

Рисунок 6 – Отрывок из лабораторной работы №1

Пункт «Лабораторная работа №2» представлен двумя частями. В первой части необходимо произвести настройку протокола SSH (рисунок 7).


ЛАБОРАТОРНЫЙ ПРАКТИКУМ: "КРОССПЛАТФОРМЕННЫЕ ТЕХНОЛОГИИ УДАЛЕННОГО ДОСТУПА"

ЛАБОРАТОРНАЯ РАБОТА №1 Лабораторная работа №2 ЛАБОРАТОРНАЯ РАБОТА №3

ЛАБОРАТОРНАЯ РАБОТА №4 ГЛОССАРИЙ

НАСТРОЙКА SSH

Цель лабораторной работы: Научиться настраивать SSH.

Задачи лабораторной работы: 1) Научиться создавать схемы SSH
2) Освоить конфигурирование серверного и клиентских компьютеров
3) Освоить конфигурирование ISP и SSH-роутеров
4) Получить навыки настройки SSH
5) Обучиться настройке статической маршрутизации
6) Обучиться осуществлять проверку работоспособности SSH

Актуальность: SSH используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам через публичную сеть.

Рисунок 7 – Отрывок из первой части лабораторной работы №2

Во второй части лабораторной работы №2 студенту предлагается выполнить лабораторную работу, связанную с настройкой TELNET (рисунок 8).

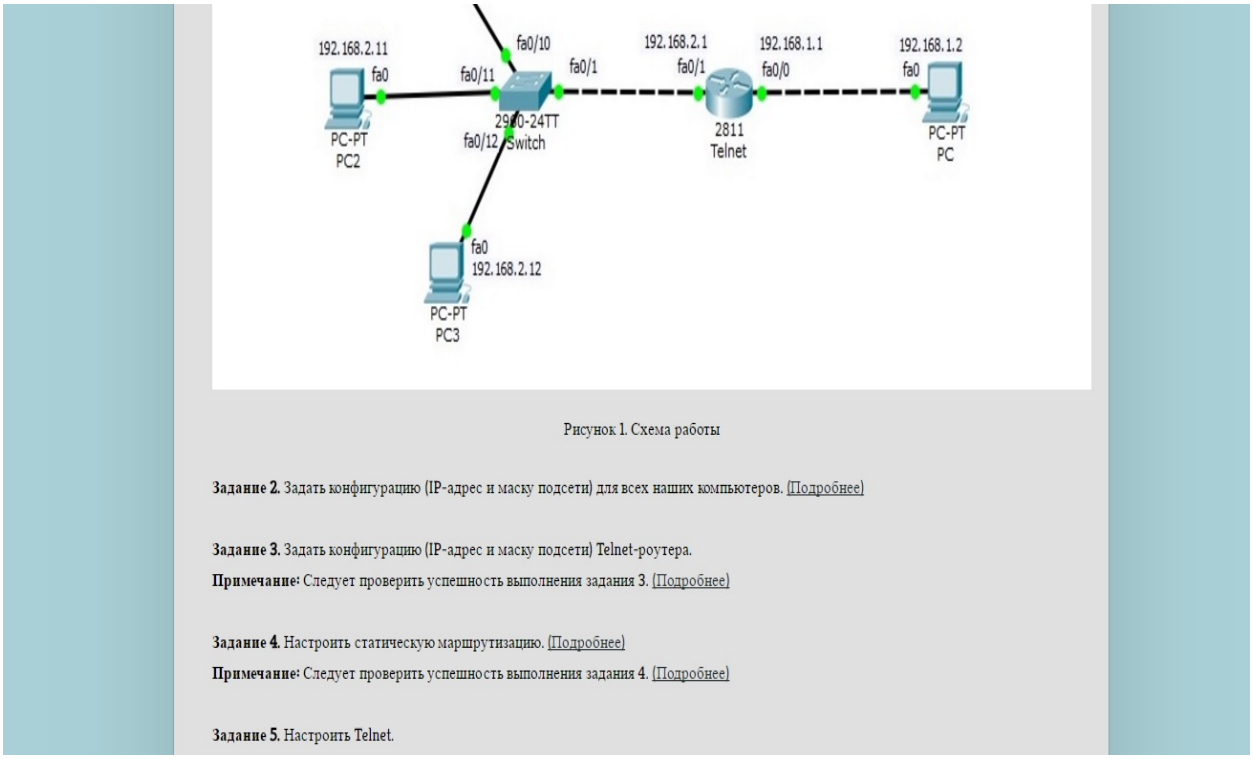


Рисунок 8 – Отрывок из второй части лабораторной работы №2

В пункте «Лабораторная работа №3» студенту предлагается выполнить лабораторную работу, связанную с настройкой Remote Access VPN (рисунок 9).

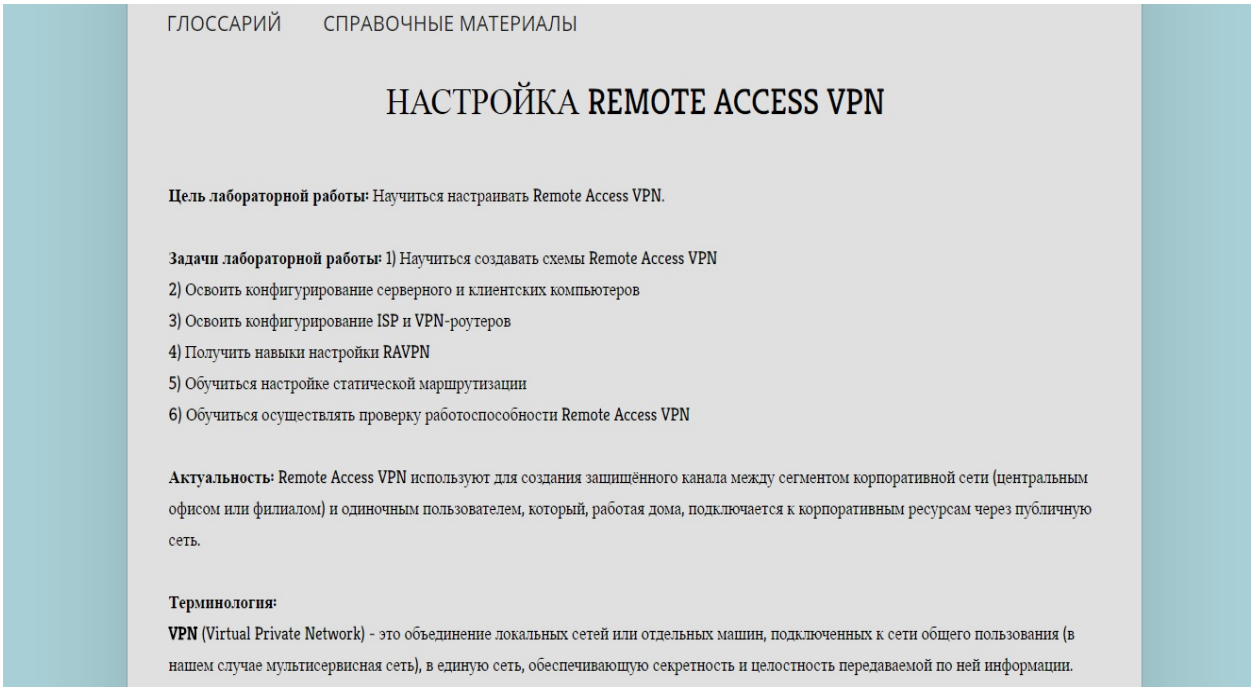


Рисунок 9 – Отрывок из лабораторной работы №3

Для студентов, которые тяжело усваивают материал в пункте «Справочные материалы» есть пояснения для каждого пункта заданий (рисунок 10).

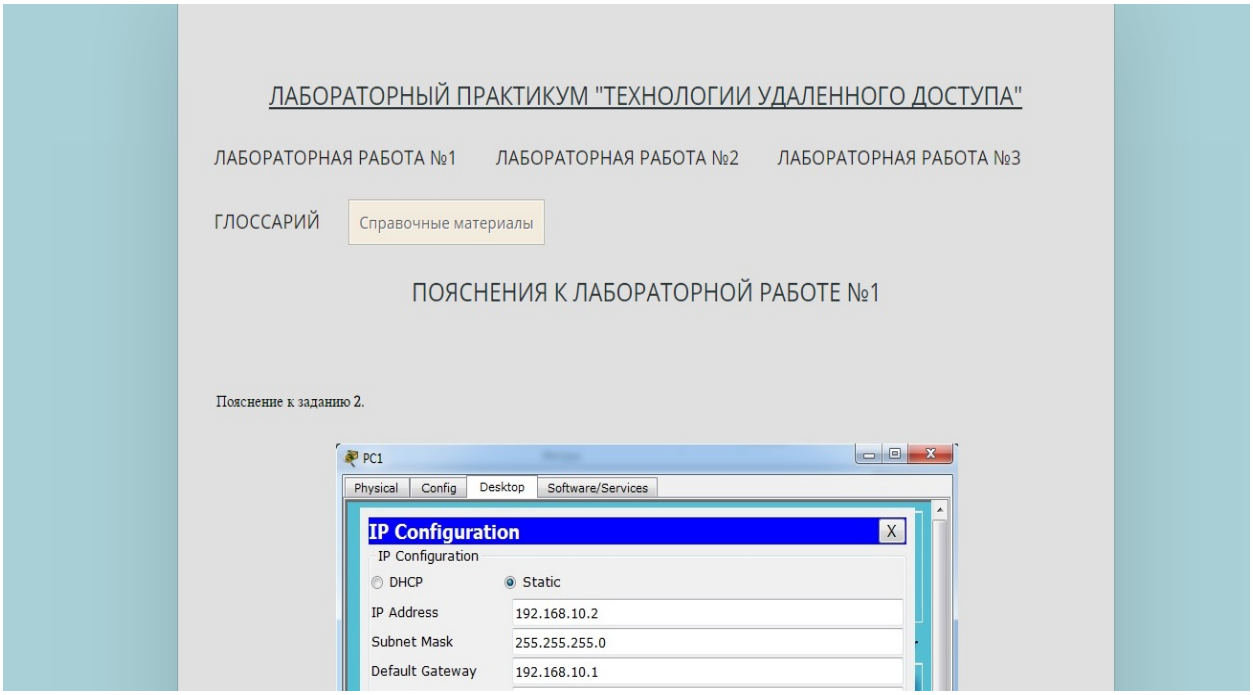


Рисунок 9 – Раздел «Справочные материалы»

В каждой лабораторной работе имеется ссылка на справочный материал в раздел «Справочные материалы» для более детального описания построения схем в лабораторных работах (рисунок 11).

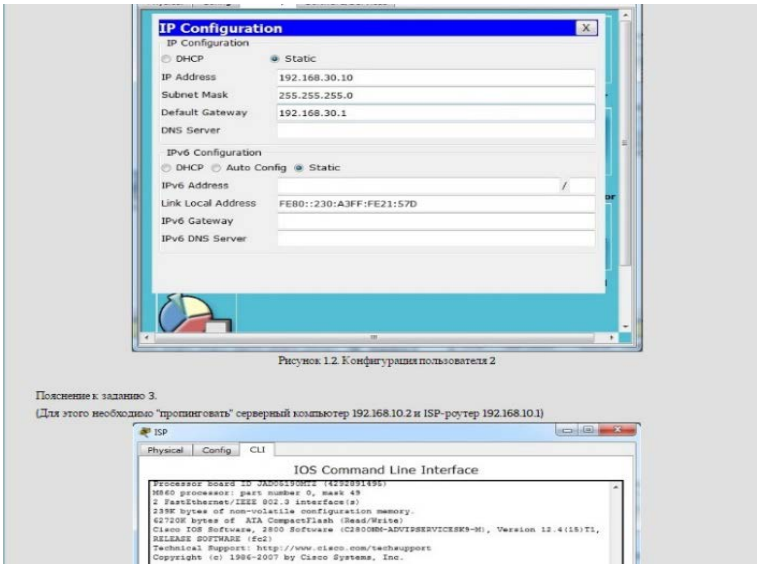


Рисунок 11 – Пример подробного объяснения в разделе «Справочные материалы»

Также, в каждой лабораторной работе представлен видеофайл с подробной настройкой каждого протокола (рисунок 12).

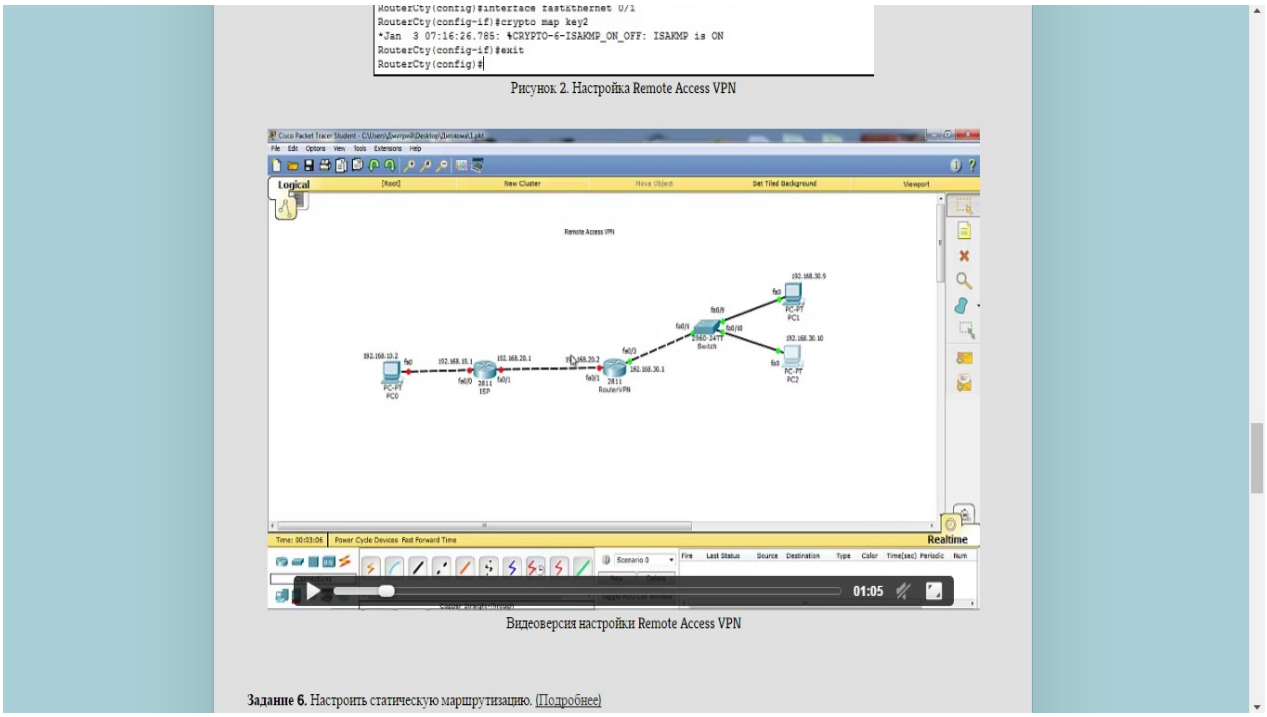


Рисунок 12 – Видеофайл настройки RAVPN в лабораторном практикуме

2.4 Структура лабораторного практикума на примере одной из лабораторных работ

Основная цель лабораторной работы №3 является обучение навыкам настройки Remote Access VPN.

В ходе лабораторной работы студенту предстоит выполнить ряд задач, посвященных настройке схем. Которые в дальнейшем будут использоваться на практике различных предприятий.

Актуальность лабораторной работы определяется следующим примером применения. Remote Access VPN используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам через публичную сеть.

Конфигурирование роутеров также является основополагающей задачей. Поэтому настройке посвящен раздел конфигурирования.

Начальным этапом выполнения лабораторных работ является проектирование схемы коммуникаций для настройки протокола (рисунок 13).

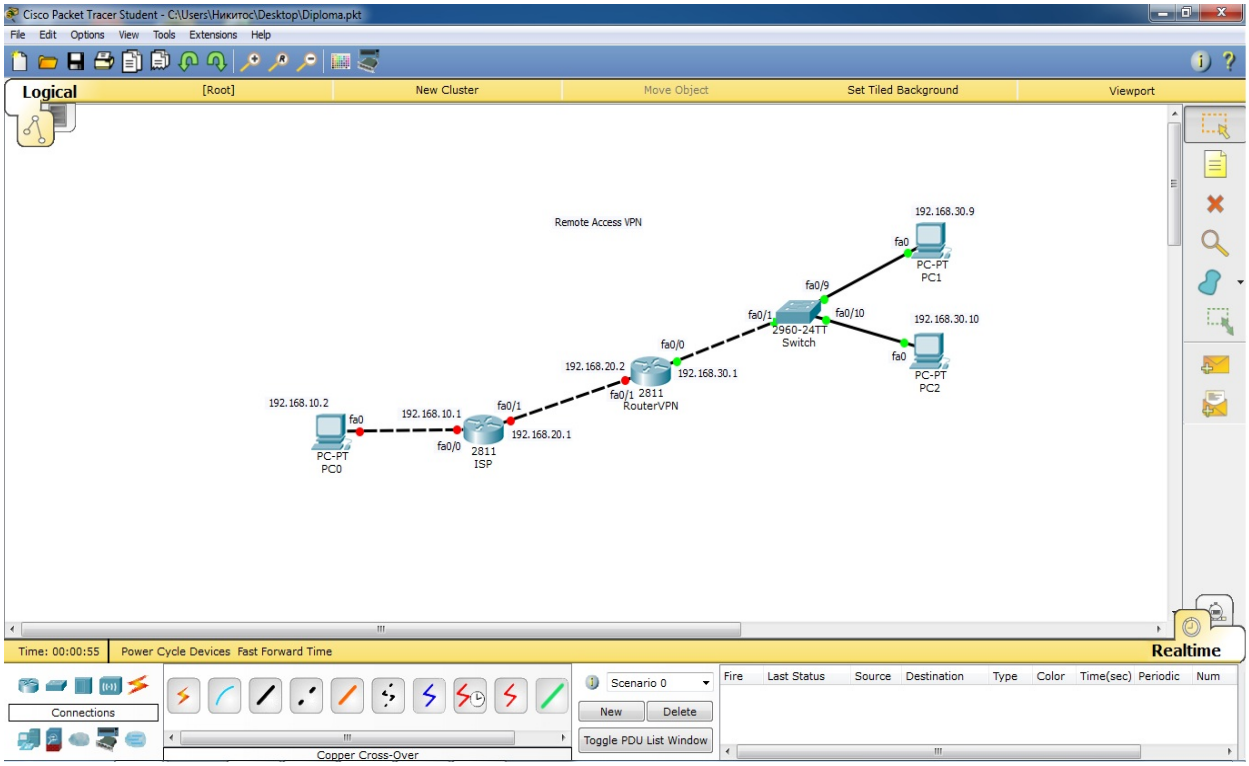


Рисунок 13 – Схема работы

В лабораторных работах студенту необходимо освоить конфигурирование компьютеров. Отдельно стоит уделить внимание конфигурации серверного компьютера, т.к. она отличается от клиентской. (рисунок 14).

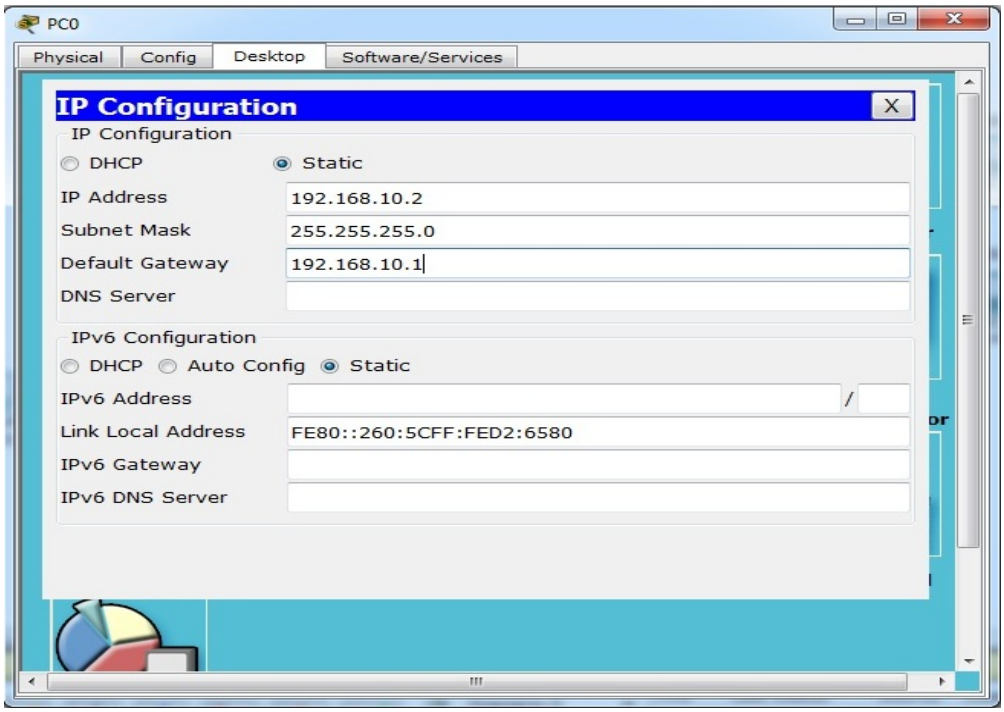


Рисунок 14 – Конфигурация серверного компьютера

Одним из заданий является настройка протокола. Настройка происходит на роутерах и является основным заданием в каждой лабораторной работе (рисунок 15).

Рисунок 15 – Настройка Remote Access VPN

Требуется научиться создавать, редактировать и запускать RAVPN-схему. Для этого следует выполнить самостоятельную работу, состоящую из двух заданий. После всех выполненных этапов, необходимо отчитаться перед преподавателем за проделанную работу. Формат отчета представляет собой ответ на контрольные вопросы.

ЗАКЛЮЧЕНИЕ

В рамках выпускной квалификационной работы был разработан лабораторный практикум «Технологии удаленного доступа».

Реализованы следующие задачи:

- Проанализировать литературу и интернет-источники по теме «Технологии удаленного доступа» с целью формирования набора навыков, являющихся основными и критическими для обучения данному разделу.
- Проанализировать литературу и интернет-источники с целью выделения требований, предъявляемых к лабораторному практикуму на современном этапе развития образования.
- Спроектировать структуру и реализовать интерфейс и функционал лабораторного практикума «Технологии удаленного доступа».

Задачи находятся прямо в лабораторном практикуме, что позволяет проверять знания студентов без отрыва от изучения темы. Если студент не смог решить задачу, то он легко может вернуться к повторению материала.

Программа обеспечивает полностью устойчивое функционирование и не нарушает целостность системы, системного реестра или системного программного обеспечения.

Интерфейс программы представлен в виде окна, написанного на HTML - коде.

Созданный лабораторный практикум не является постоянным, потому что информация по данной теме обновляется и его придется дополнять новой, обновленной информацией.

Главная страница пособия состоит из пяти фреймов – фрейма лабораторных работ, фрейма справки и фрейма глоссария. После открытия главного файла пособия index.htm двойным щелчком во фрейме учебного материала открывается информация о пособии. Также на этой странице представлена структура учебного пособия, содержащая все лабораторные работы, справку

и глоссарий. Для быстрого перехода выберите интересующую вас тему или подтему из списка и щелкните по ней левой кнопкой мыши.

В фрейме лабораторные работы необходимо воспользоваться скроллингом мыши или щелкнуть по стрелкам полосы прокрутки, чтобы просмотреть всю лабораторную работу. В каждой лабораторной работе работает скрипт, который подсвечивает номер лабораторной работы, в которой находится студент. После нажатия на кнопку «Лабораторная работа №1» открывается первая лабораторная работа. Она довольно большой и в полностью раскрытом виде занимает несколько страниц. Это не очень удобно, так как не позволяет пользователю хорошо ориентироваться в содержании учебного пособия.

Текст учебного материала всех четырех лабораторных работ и глоссария пособия читабелен. Все ключевые слова выделены жирным шрифтом. Это позволяет сделать акцент на терминах, которые нужно запомнить. Разработанное пособие включает в себя лабораторные работы по выполнению настройки сетевых протоколов, а также глоссарий для студентов, которым трудно дается усвоение материала, в котором рассмотрены полная терминология и подробное руководство по выполнению лабораторных работ с комментариями. Пособие будет использоваться в Российском государственном профессионально-педагогическом университете студентами третьего курса профилизации «Компьютерные технологии».

Цель выпускной квалификационной работы достигнута, поставленные задачи выполнены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Андрончик А.Н. Сетевая защита на базе технологий фирмы Cisco Systems [Текст]: учебное пособие для вузов / А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков под общ. ред. Н.И. Синадского. — Екатеринбург: Издательство Уральского Федерального Университета, 2014. — 180 с.

2. Балыкина Е.Н. Сущностные характеристики электронных учебных изданий [Электронный ресурс]. — Режим доступа: http://www.history.krsu.edu.kg/index.php?option=com_content&task=view&id=351 (дата обращения: 21.05.2016).

3. Браун С. Виртуальные частные сети VPN [Текст]: учебник для вузов / С. Браун, О.А. Труфанов. — Москва: Лори, 2011. — 502 с.

4. Введение в архитектуру MPLS [Электронный ресурс]. — Режим доступа: http://system-administrators.info/?p=1179 (дата обращения: 10.05.2016).

5. Вишневский В.М. Теоретические основы проектирования компьютерных сетей [Текст]: учебник для вузов В.М. Вишневский. — Москва: Техносфера, 2013. — 512 с.

6. Галкин В.А. Телекоммуникации и сети [Текст]: учебное пособие для вузов / В.А. Галкин, Ю.А. Григорьев — под общ. ред. В.А. Галкина. — Москва: Изд-во МГТУ им. Н.Э. Баумана, 2013. — 608 с.

7. Дрегон М. 9 шагов по настройке маршрутизатора Cisco [Электронный ресурс]. — Режим доступа: http://www.osp.ru/win2000/2009/04/9051071/ (дата обращения: 11.05.2016).

8. Запечников С.В. Основы построения виртуальных частных сетей [Текст]: учебник для вузов / С.В. Запечников, Н.Г. Милославская, Л.И. Толстой — под общ. ред. С.В. Запечникова. — 2-е изд. — Москва: Горячая линия-Телеком, 2011. — 248 с.

9. Захватов М.Ю. Построение виртуальных частных сетей (VPN) на базе технологии MPLS [Текст]: учебник для вузов. / М.Ю. Захватов. — Москва: Циско Системс, 2011. — 52 с.

10. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях [Текст]: учебник для вузов / М.А. Иванов. — Москва: КУДИЦ-ОБРАЗ, 2011. — 368 с.

11. Красильников И.В. Информационные аспекты разработки и применения в ВУЗе электронных учебных пособий [Текст]: монография / И.В. Красильников. — Москва: «РХТУ», 2011. — 114 с.

12. Кульгин М.В. Компьютерные сети. Практика построения. Для профессионалов. [Текст]: учебник для вузов/ М.В. Кульгин. — 2-е изд. — Санкт-Петербург: Питер, 2013. — 462 с.

13. Максимов Н.В. Компьютерные сети [Текст]: учебник для вузов / Н.В. Максимов, И.И. Попов — под общ. ред. Н.В. Максимова. — 3-е изд. — Москва: Форум, 2013. — 448 с.

14. НОУ Интуит [Электронный ресурс]. — Режим доступа: http://www.intuit.ru (дата обращения: 21.05.2016).

15. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В.Г. Олифер, Н.А. Олифер — под общ. ред. В.Г. Олифера. — 4-е изд. — Санкт-Петербург: Питер, 2012. – 943 с.

16. Пакет К. Создание сетей удаленного доступа Cisco [Текст]: учебник для вузов / К. Пакет, А.Н. Крикун. — Москва: Вильямс, 2013. — 672 с.

17. Первичная настройка Cisco коммутатора и маршрутизатора [Электронный ресурс]. — Режим доступа: http://networkdoc.ru/entry/network/pervichnaya-nastrojka-cisco-kommutatora-i-marshrutizatora (дата обращения: 12.05.2016).

18. Покровский П.И Развертывание сети VPN [Электронный ресурс]. — Режим доступа: http://www.osp.ru/lan/2003/01/137054/ (дата обращения: 18.04.2016).

19. Удаленный доступ для мобильных устройств: управляемые и облачные VPN-сервисы [Электронный ресурс]. — Режим доступа: https://habrahabr.ru/company/celecom/blog/230085/ — (дата обращения: 21.05.2016)

20. Уэнделл О. Компьютерные сети. Первый шаг. [Текст]: учебник для вузов / В.С. Гусев. — Москва: Вильямс, 2013. — 432 с.

21. Фримен Э. Изучаем HTML, XHTML и CSS [Текст]: учебник для вузов / Э. Фримен, И. П. Дубенок. — Санкт-Петербург: Питер, 2012. — 656 с.

22. Шиндлер Д.Л. Основы компьютерных сетей [Текст]: учебник для вузов/ Д.Л. Шиндлер. — Москва: Вильямс, 2012. — 615 с.

23. Эрганова Н.Е. Методика профессионального обучения [Текст]: учебное пособие / Н.Е. Эрганова. — Москва: «Академия», 2008. — 160 с.

24. Эрганова Н.Е. Практикум по методике профессионального обучения [Текст]: учебное пособие / Н. Е. Эрганова. — Екатеринбург: Изд-во Рос. гос. проф.-пед.ун-та, 2011. — 89 с.

25. Эрганова Н.Е. Практикум по педагогическим технологиям [Текст]: учеб. пособие / Н.Е. Эрганова. — Екатеринбург: Изд-во Рос. гос. проф.-пед. ун-та, 2011. — 50 с.

26. Cisco Packet Tracer [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/ Cisco Packet Tracer (дата обращения: 25.05.2016).

27. CSS [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org//wiki/Css (дата обращения: 25.05.2016).

28. Cyber Forum [Электронный ресурс]. — Режим доступа: www.cyberforum.ru/cisco (дата обращения: 29.04.2016)

29. HTML [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/HTML (дата обращения: 25.05.2016).

30. IP VPN: осознанная необходимость [Электронный ресурс]. — Режим доступа: http://www.connect.ru/article.asp?id=5343 (дата обращения: 30.04.2016).

31. Notepad++ [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Notepad%2B%2B (19.04.2016).

32. Stackoverflow [Электронный ресурс]. — Режим доступа: http://ru.stackoverflow.com/ (дата обращения: 18.04.2016).

ПРИЛОЖЕНИЕ

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

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

УТВЕРЖДАЮ
Заведующий кафедрой
_____Н. С. Толстова
«_____»_____2016 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра

студентки 4 курса, группы КТ-401 Городилов Никита Вадимович

1. Тема Виртуальный тур по Новоуральскому историко-краеведческому музею утверждена распоряжением по институту от 28.03.2016 г. № 57

2. Руководитель Венков Сергей Сергеевич, ст. преподаватель каф. ИС РГППУ

3. Место преддипломной практики Государственное казенное образовательное учреждение Свердловской области для детей-сирот и детей, оставшихся без попечения родителей, "Серовский детский дом-школа"

4. Исходные данные к ВКР

Браун С. «Виртуальные частные сети»
Пакет К. «Создание сетей удаленного доступа Cisco»
Максимов Н.В. «Компьютерные сети»
Олифер В.Г., Олифер Н.А., Компьютерные сети: принципы, технологии, протоколы

5. Содерание текстовой части ВКР (перечень подлежащих разработке вопросов)
Анализ источнико
Описание технологий удаленного доступа
Общие требования по созданию лабораторных практикумов
Описание лабораторного практикума
6. Перечень демонстрационных материалов
Презентация выполненная в Microsoft PowerPoint

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа дипломной работы	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной работе и сдача зачета по преддипломной практике	23.04.2016	15 %	
2	Выполнение работ по разрабатываемым вопросам их изложение в выпускной работе:		65 %	
	Анализ литературы, интернет-источников	28.04.2016	10 %	
	Обзор и выбор необходимых средств разработки лабораторного практикума	04.05.2016	10 %	
	Подготовка материалов, необходимых для разработки виртуального тура	19.05.2016	20 %	
	Создание лабораторного практикума	02.06.2016	15 %	
3	Оформление текстовой части ВКР		5 %	
4	Выполнение демонстрационных материалов к ВКР		5 %	
5	Нормоконтроль	13.06.2016	5 %	
6	Подготовка доклада к защите в ГЭК	15.06.2016	5 %	

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

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

9. Выпускная квалификационная работа и все материалы проанализированы.
Считаю возможным допустить Городилова Н.В. к защите выпускной квалификационной работы в государственной экзаменационной комиссии.

Руководитель _____ _____
подпись дата

10. Допустить Городилова Н.В. к защите выпускной квалификационной работы в государственной экзаменационной комиссии (протокол заседания кафедры от «__» июня 2016 г., № __)

Заведующий кафедрой _____ _____
подпись дата