Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт кибернетики
Направление подготовки 09.04.02 «Информационные системы и технологии»
Кафедра информационных систем и технологий

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Разработка моделей вычислительных сетей на основе платформы UnetLab

УДК 004.7.051:004.946

Студент

Группа	ФИО	Подпись	Дата
8ИМ5А	Окунев Дмитрий Александрович		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. ИСТ	Шерстнев В.С.	к.т.н.		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. менеджмента	Попова С.Н.	к.э.н		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ассистент каф. ЭБЖ	Акулов П.А.	-		

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
ИСТ	Мальчуков А.Н	к.т.н.		

Томск – 2017 г.

Планируемые результаты обучения

Код результатов	Результат обучения (выпускник должен быть готов)
Общепрофессиональные компетенции	
Р1	Воспринимать и самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте.
Р2	Владеть и применять методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях.
Р3	Демонстрировать культуру мышления, способность выстраивать логику рассуждений и высказываний, основанных на интерпретации данных, интегрированных из разных областей науки и техники, выносить суждения на основании неполных данных, анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями.
Р4	Анализировать и оценивать уровни своих компетенций в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и профессиональной мобильности. Владеть, по крайней мере, одним из иностранных языков на уровне социального и профессионального общения, применять специальную лексику и профессиональную терминологию языка.
Профессиональные компетенции	
Р5	Разрабатывать стратегии и цели проектирования, критерии эффективности и ограничения применимости, новые методы, средства и технологии проектирования геоинформационных систем (ГИС) или промышленного программного обеспечения.
Р6	Планировать и проводить теоретические и экспериментальные исследования в области создания интеллектуальных ГИС и ГИС технологии или промышленного программного обеспечения с использованием методов системной инженерии.
Р7	Осуществлять авторское сопровождение процессов проектирования, внедрения и сопровождения ГИС и ГИС технологий или промышленного программного обеспечения с использованием методов и средств системной инженерии, осуществлять подготовку и обучение персонала.
Р8	Формировать новые конкурентоспособные идеи в области теории и практики ГИС и ГИС технологий или системной инженерии программного обеспечения. Разрабатывать методы решения нестандартных задач и новые методы решения традиционных задач. Организовывать взаимодействие коллективов, принимать управленческие решения, находить компромисс между различными требованиями как при долгосрочном, так и при краткосрочным планировании.
Общекультурные компетенции	
Р9	Использовать на практике умения и навыки в организации исследовательских, проектных работ и профессиональной эксплуатации современного оборудования и приборов, в управлении коллективом.
Р10	Свободно пользоваться русским и иностранным языками как средством делового общения.
Р11	Совершенствовать и развивать свой интеллектуальный и общекультурный уровень. Проявлять инициативу, в том числе в ситуациях риска, брать на себя всю полноту ответственности.
Р12	Демонстрировать способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности, способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, способность к педагогической деятельности.

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт кибернетики
Направление подготовки 09.04.02 «Информационные системы и технологии»
Кафедра информационных систем и технологий

УТВЕРЖДАЮ:
Зав. Кафедрой
_____ _____ Мальчуков А.Н.
(Подпись) (Дата)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

магистерской диссертации

(бакалаврской работы, дипломного проекта/работы, магистерской диссертации)

Студенту:

Группа	**ФИО**
8ИМ5А	Окуневу Дмитрию Александровичу

Тема работы:

Разработка моделей вычислительных сетей на основе платформы UnetLab	
Утверждена приказом директора (дата, номер)	№897/с от 20.02.2017 г.

Срок сдачи студентом выполненной работы:	16.06.2017 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе *(наименование объекта исследования или проектирования; производительность или нагрузка; режим работы (непрерывный, периодический, циклический и т. Д.); вид сырья или материал изделия; требования к продукту, изделию или процессу; особые требования к особенностям функционирования (эксплуатации) объекта или изделия в плане безопасности эксплуатации, влияния на окружающую среду, энергозатратам; экономический анализ и т. Д.).*	На основе современной онлайн-платформы виртуализации сетевого оборудования UnetLab, разработать модели сложных вычислительных сетей.

Перечень подлежащих исследованию, проектированию и разработке вопросов *(аналитический обзор по литературным источникам с целью выяснения достижений мировой науки техники в рассматриваемой области; постановка задачи исследования, проектирования, конструирования; содержание процедуры исследования, проектирования, конструирования; обсуждение результатов выполненной работы; наименование дополнительных разделов, подлежащих разработке; заключение по работе).*	Проведение анализа современных платформ виртуализации сетевого оборудования; Разработка концепций вычислительных сетей; Моделирование вычислительных сетей в платформе UnetLab; Проведение исследований эффективности смоделированных вычислительных сетей.
Перечень графического материала *(с точным указанием обязательных чертежей)*	Презентация работы

Консультанты по разделам выпускной квалификационной работы

(с указанием разделов)

Раздел	Консультант
Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	Попова С.Н.
Социальная ответственность	Акулов П.А.
Раздел ВКР, выполняемый на английском языке	Горбатова Т.Н.

Названия разделов, которые должны быть написаны на русском и иностранном языках:

Раздел 1.3 Выбор эмулятора сетевого оборудования

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	15.02.2017 г.

Задание выдал руководитель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. ИСТ	Шерстнев В.С.	к.т.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ИМ5А	Окунев Дмитрий Александрович		

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт кибернетики
Направление подготовки 09.04.02 «Информационные системы и технологии»
Уровень образования магистратура
Кафедра информационных систем и технологий
Период выполнения осенний/весенний семестр 2016/2017 учебного года

Форма представления работы:

магистерская диссертация

(бакалаврская работа, дипломный проект/работа, магистерская диссертация)

КАЛЕНДАРНЫЙ РЕЙТИНГ-ПЛАН
выполнения выпускной квалификационной работы

Срок сдачи студентом выполненной работы:	16.06.2017 г.

Дата контроля	Название раздела (модуля) / вид работы (исследования)	Максимальный балл раздела (модуля)
13.03.17	Обзор наиболее популярных платформ виртуализации сетевого оборудования	*10 баллов*
26.04.17	Разработка концепция вычислительных сетей	*15 баллов*
20.05.17	Моделирование вычислительных сетей на платформе UnetLab	*15 баллов*
25.05.17	Проведение исследования эффективности спроектированных вычислительных сетей	*20 баллов*
9.06.17	Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	*15 баллов*
13.06.17	Социальная ответственность	*15 баллов*
14.06.17	Раздел ВКР, выполняемый на иностранном языке	*10 баллов*

Составил преподаватель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. ИСТ	Шерстнев В.С.	к.т.н.		

СОГЛАСОВАНО:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
ИСТ	Мальчуков А.Н.	к.т.н.		

Реферат

Выпускная квалификационная работа 106 с., 37 рис., 19 табл., 28 источников.

Ключевые слова: эмуляция, сетевой оборудование, сетевой протокол, вычислительная сеть, моделирование.

Объектом исследования работы являются процесс моделирования вычислительных сетей и сетевые протоколы для управления вычислительными сетями.

Цель дипломной работы на основе современной онлайн-платформы виртуализации сетевого оборудования UNetLab, разработать модели сложных вычислительных сетей.

Поставленные задачи: произвести анализ существующих систем виртуализации сетевого оборудования, спроектировать концепции сложных вычислительных сетей и разработать их модели. На основе разработанных моделей провести исследования их эффективности.

В процессе исследования проводились: анализ существующих систем-аналогов виртуализации сетевого оборудования.

Основные конструктивные, технические и технико-эксплуатационные характеристики: модели сложных вычислительных сетей основываются на использовании оборудования компании Cisco Systems.

Область применения: моделирование сложных вычислительных сетей**.**

Экономическая эффективность/значимость работы: результат позволяет повысить эффективности проектирования вычислительных сетей и снизить финансовые потери предприятия при современной стоимости сетевого оборудования

Определения

VLAN (Virtual Local Area Network) – виртуальная локальная сеть.

DHCP (Dynamic Host Configuration Protocol) – протокол динамической настройки узла.

EIGRP (Enhanced Interior Gateway Routing Protocol) – протокол динамической маршрутизации.

NAT (Network Address Translation) — преобразование сетевых.

STP (Spanning Tree Protocol**)** – протокол остовного дерева.

VPN (Virtual Private Network) –виртуальная частная сеть.

IPsec (сокращение от **IP Security**) – набор протоколов для обеспечения защиты данных.

GRE (Generic Routing Encapsulation) – общая инкапсуляция маршрутов.

Оглавление

Введение

Практический интерес к вычислительным сетям в настоящее время вызван потребностями пользователей в информационном обеспечении. Создание вычислительных сетей требует больших затрат. Каждая организация, принимающая решение о построении сети, понимает необходимость расходования довольно значительных финансовых средств и поэтому тем более желает получить определенные гарантии качества приобретаемых информационно - вычислительных средств.

Часто при проектировании вычислительных сетей используют аналоги – известные, хорошо зарекомендовавшие себя в работе проектные решения, накопленный опыт. Однако, своеобразие и уникальность функций, выполняемых каждой организацией, их постоянное развитие, возникновение новых информационных технологий обгоняют накопленный опыт и тогда вычислительная сеть, даже содержащая все современные средства, может работать с точки зрения пользователя недостаточно эффективно. При современной стоимости промышленного сетевого оборудования, ошибки, допущенные при проектировании таких сетей, могу привести к большим финансовым потерям компании. Именно поэтому особый интерес в настоящее время приобретают методы, которые на основе эмулирования сетевого оборудования позволяют смоделировать будущую структуру и организацию вычислительных сетей.

Цель дипломной работы на основе современной онлайн-платформы виртуализации сетевого оборудования UNetLab, разработать модели сложных вычислительных сетей.

Практическая значимость результатов ВКР: результат позволяет повысить эффективности проектирования вычислительных сетей и снизить финансовые потери предприятия при современной стоимости сетевого оборудования.

1 Программные эмуляторы сетевого оборудования

Повсеместное создание компьютерных сетей обуславливает резкое развитие в сфере передачи информации. Компьютерные сети создаются для обеспечения пользователей удалённым доступом к ресурсам сети. Поэтому фактически все компании, имеющие более одного компьютера, объединяют их в локальные сети. Очень принципиально, чтобы сеть компании работала бесперебойно, была надёжной, как можно лучше справлялась с обработкой информации, циркулирующей между сотрудниками компании, и позволяла принимать им значимые и оптимальные решения [1,2].

Сложные составные сети состоят из большого количества элементов - маршрутизаторов, концентраторов, коммутаторов, модемов, мостов и т.п. телекоммуникационного оборудования [9].

При разработке сложных составных сетей нередко встает задача предварительного моделирования такой сети с целью проверки используемых технических решений [1]. Анализ работы созданной модели сети позволяет до ее физической реализации оценить характеристики проектируемой сети, а также разработать необходимую конфигурацию интеллектуальных сетевых устройств.

Данная задача, при всей ее кажущейся простоте, является довольно сложной из-за большого разнообразия применяемого оборудования.

Наиболее простым решением для создания моделей будущих вычислительных сетей являются программные эмуляторы оборудования. Они не требуют больших затрат, так как нет необходимости приобретать сетевое оборудование, все, что необходимо, это персональный компьютер и программный эмулятор [4].

Программные эмуляторы сетевого оборудования – это программные продукты, позволяющие соединить в себе функции и параметры реальной вычислительной сети. Они были разработаны для проектирования, моделирования и тестирования работы сети. [7]

Большинство эмуляторов достаточно удобны в использовании, так как предоставляют графический интерфейс для управления сетевой инфраструктурой, что бывает намного удобнее чем управление подключениями реальных устройств [4].

1.1 Классификация эмуляторов

Все эмуляторы сетевого оборудования можно разделить на две основные группы:

1. Аппаратно-реализованные эмуляторы.

2. Программно-реализованные эмуляторы.

К перовой группе относят, как правило, узко специализированное оборудование, позволяющее при подключении к нему реального телекоммуникационного оборудования имитировать работу реальной телекоммуникационной сети, либо какой-то ее части (как правило - каналов связи). В аппаратных эмуляторах на аппаратном уровне реализованы процессы, протекающие в реальных сетях - возникновение задержек, потерь пакетов, искажения передаваемых данных и т.п. событий. Основная цель разработки и применения аппаратных эмуляторов - исследование работы реального телекоммуникационного оборудования в различных условиях и при различных характеристиках каналов [12].

Ко второй группе эмуляторов относят специально разработанные программы, позволяющие имитировать работу оборудования и каналов связи, а также работу командных интерфейсов активного сетевого оборудования [13]. Основная цель использования программных эмуляторов - применение в качестве научно-исследовательской деятельности, для постановки научных экспериментов. Также, данные программы часто используются в качестве обучающих систем для подготовки персонала в работе с сетевым оборудованием [16].

1.2 Выбор сетевого оборудования

Для решения задач создания вычислительных сетей разрабатывается сетевое оборудование различного назначения: коммутатор – сетевое оборудование для объединения компьютеров в одну или несколько локальных сетей; маршрутизатор – устройство, предназначенное для взаимодействия компьютеров, находящихся в разных локальных сетях и предоставления доступа в сеть Интернет; межсетевой экран – устройство, обеспечивающее безопасность в сети и т.д. На сегодняшний день существует множество компаний, производящих сетевое оборудование, и компания Cisco Systems считается безусловным фаворитом на рынке сетевого оборудования (занимает около 70% рынка) и предлагает устройства для создания вычислительных сетей от небольшого офиса до крупных корпораций [4].

Компания Cisco Systems является производителем сетевого оборудования с 1984 года и по сей день является лидером в этой отрасли. Сетевое оборудование компании заметно выделяется на фоне конкурентов и обладает многими достоинствами:

- Надежность – сетевое оборудование, выпускаемое компанией, функционирует на базе операционной системы Cisco IOS и включает в себя огромный спектр настройки и конфигурирования устройства;
- Гибкость – сетевые устройства под управлением Cisco IOS могу одновременно выполнять совершенно различные функции: маршрутизационные, защитные, отладочные и т.д.;
- Интеллектуальность –устройства компании содержат широкий спектр различных технологий и протоколов, как стандартных, так и разработанных собственно компанией Cisco;
- Централизация – для управление устройствами могут использоваться мощные комплексы управления и отладки оборудования, например, такие, как Cisco Security Manager и д.р.

Из недостатков, можно лишь выделить стоимость оборудования. Однако, стоит отметить то, что высокая стоимость выпускаемого оборудования компанией Cisco окупается за счет надежности и срока службы данного оборудования.

Учитывая широкое распространение сетевого оборудования под управлением Cisco IOS (**I**nternetwork **O**perating **S**ystem — Межсетевая Операционная Система), а также высокую стоимость данного оборудования, еще более ясным становится необходимость в применении программных эмуляторов сетевого оборудования для создания моделей вычислительных сетей [18].

Именно на оборудовании данного производителя будут проектироваться будущие модели вычислительных сетей.

1.3 Выбор эмулятора сетевого оборудования

Рассмотрим подробнее наиболее популярные эмуляторы, позволяющие создать виртуальные копии сетевого оборудования производства компании Cisco Systems.

Cisco Packet Tracer

Самым популярным эмулятором сетевого оборудования является Cisco Packet Tracer, это эмулятор, разработанный самой компанией Cisco Systems для обучения начинающих специалистов. Packet Tracer получил большое распространение за счет необходимости его применения для прохождения обучения в рамках программ Cisco Network Academy, сетевой академии, в которой ежегодно проходят обучение десятки тысяч начинающих специалистов [6].

Создание сетевой инфраструктуры и последующая модификация происходят через графический интерфейс, который является интуитивно понятным и наиболее удобных из графических интерфейсов управления, предоставляемых рассматриваемыми программными средствами эмуляции сетевого оборудования. Интерфейс хорошо адаптирован для начинающих специалистов и очень сильно упрощает процесс создания новых сетевых

инфраструктур или запуск и настройку необходимых для проведения практических занятий сервисов. Пример интерфейса отображен на рисунке 1.

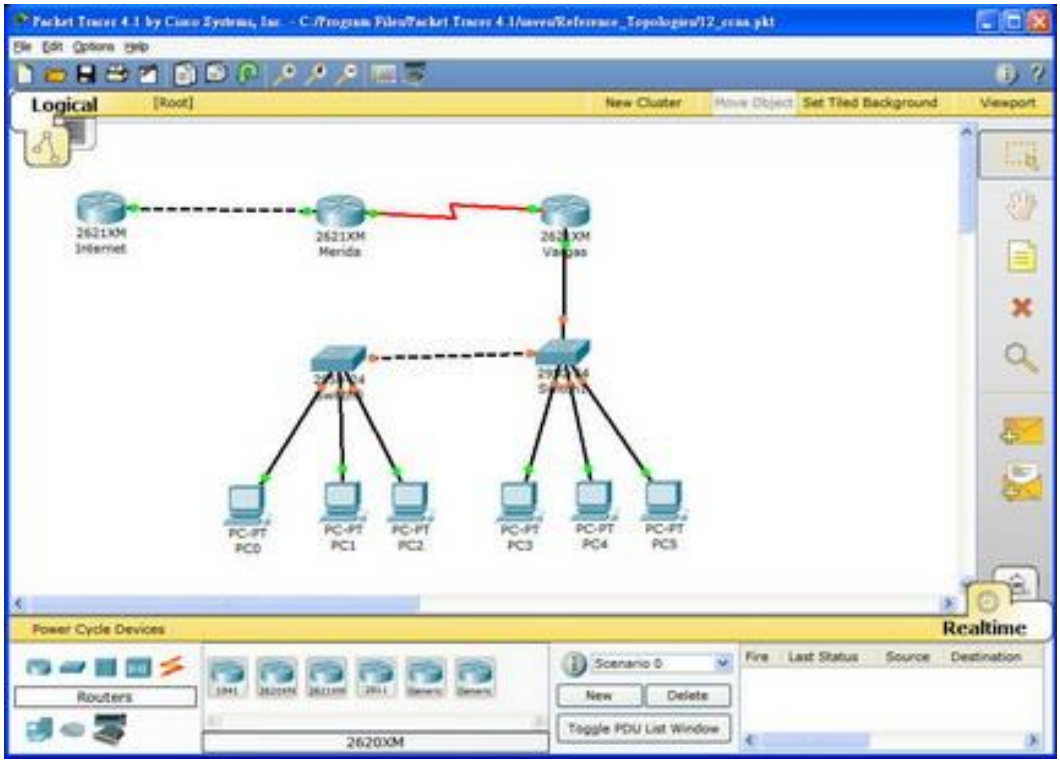

Рисунок 1 - Графический интерфейс эмулятора Cisco Packet Tracer

Основное назначение эмулятора Packet Tracer в создании виртуальных сетей для проведения практических работ для подготовки к сертификационным экзаменам CCNA (Cisco Certified Network Associate) и CCNA Security (Cisco Certified Network Associate Security). Помимо стандартных маршрутизаторов и коммутаторов Packet Tracer поддерживает эмуляцию IP-телефонов, беспроводных точек доступа и серверов с набором стандартных служб [7].

В Packet Tracer встроено множество средств, упрощающих изучение работы сетевой инфраструктуры, таких как снифферы, позволяющие получить подробную информацию о всех блоках данных передаваемых тому или иному устройству, генераторы сетевого трафика, позволяющие искусственно создавать нагрузку, и средства отображения потоков данных, позволяющие проследить маршрут прохождения сети любым пакетом или процесс изменения пакета при прохождении различных устройств.

Packet Tracer является удобным средством эмуляции сетевого оборудования не только для обучающегося, но и для преподавателя. В эмулятор встроены средства автоматической проверки выполнения задания. Преподаватель может разработать лабораторную работу для Packet Tracer, которая будет автоматически проверять степень выполнения задания, и вместо проверки вручную правильности работы всех протоколов и корректности введённых команд, достаточно воспользоваться автоматической проверкой, которая определит процент выполнения задания и работоспособность основных сервисов [9].

Cisco Packet Tracer производит эмуляцию как аппаратной, так и программной части сетевого оборудования. Таким образом, Packet Tracer позволяет создавать копии больших сетевых инфраструктур, вот только эмулируемые устройства не поддерживают очень большое количество технологий, используемых в реальных крупных сетях, многие функции, доступные в реальных устройствах попросту отсутствуют.

Главное преимущество Cisco Packet Tracer – бесплатность данного продукта [6,7].

Таким образом, эмулятор Cisco Packet Tracer является оптимальным инструментом для проведения практических занятий при обучении по базовым курсам компании Cisco и при подготовке к экзаменам уровня специалиста. Но для решения более сложным задач моделирования вычислительных сетей данное ПО не подходит, поскольку является симулятором и не предоставляет всех возможностей реального оборудования, и далее рассматриваться не будет.

GNS3

GNS3 (Graphical Network Simulator 3) – это независимый бесплатный программный эмулятор маршрутизаторов Cisco. GNS3 поддерживается в большинстве операционных систем Linux, Windows и Mac OS X, при этом данный программный эмулятор даёт возможность эмулировать аппаратную часть маршрутизаторов Cisco, для этого он загружает и использует реальный образ операционной системы Cisco IOS [8].

GNS3 – это графическая оболочка, объединяющая в себе ряд различных программных средств эмуляции. Графический интерфейс среды эмуляции, изображенный на рисунке 2, не адаптирован для начинающих специалистов, он скорее рассчитан на тех, кто уже имеет опыт работы со средствами эмуляции, сетевым оборудованием и знаком с основными принципами функционирования сетевых устройств. Но наличие графических средств управления значительно облегчает процесс создания сетевой инфраструктуры и делает работу с ней более удобной.

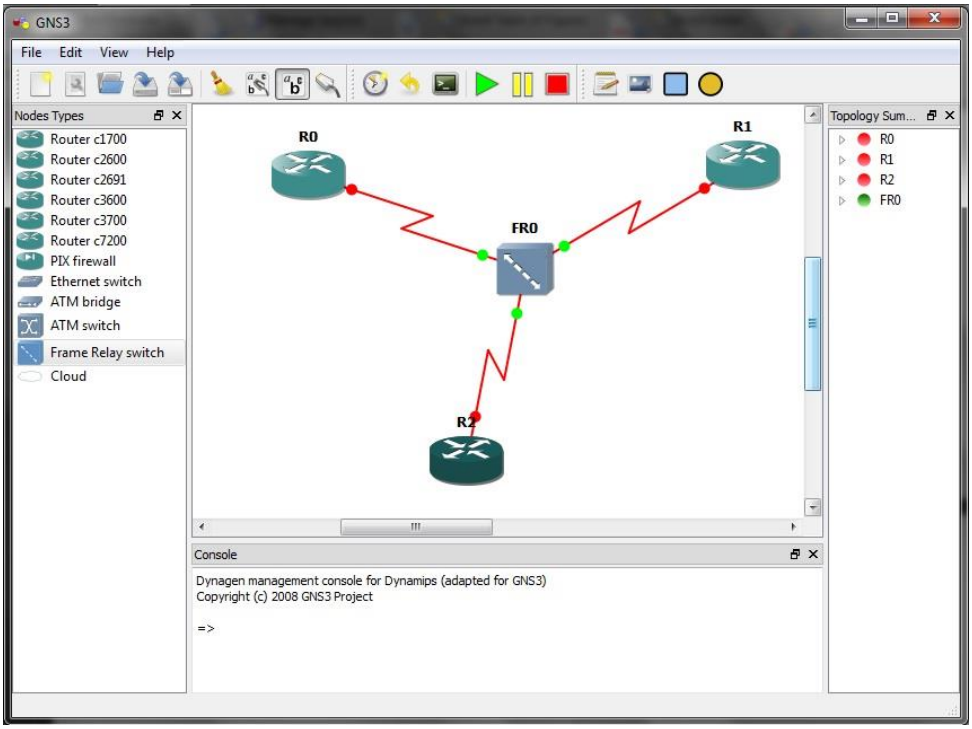

Рисунок 2 - Графический интерфейс эмулятора GNS3

GNS3 включает в себя три отдельных программных эмулятора. Первый из них Dynamips. Многие специалисты, изучающие сетевые технологии, применяют Dynamips исключительно в среде GNS3, так как отпадает необходимость работы с конфигурационными файлами и командной строкой. Вторым является Qemu, который позволяет эмулировать межсетевые экраны Cisco PIX и ASA и системы предотвращения вторжений Cisco IPS, наличие поддержки данных устройств значительно расширяет возможность применения GNS3 в обучении по направлениям, связанным с обеспечением безопасности сетевых инфраструктур [5]. Третьим элементов является система виртуализации

VirtualBox, которая позволяет интегрировать в сетевую инфраструктуру из эмулируемых устройств виртуальные сервера или виртуальные персональные компьютеры, которые позволят более точно воссоздать реальную информационную инфраструктуру, а значить изучить больший ряд технологий.

GNS3 является очень требовательной к ресурсам системой эмуляции. Так как запускаются одновременно несколько независимых систем эмуляции, а поверх них контролирующая среда, обеспечивающая еще и графический интерфейс, постоянно отображающих изменения в состоянии инфраструктуры, требуются серьезные вычислительные мощности. Хоть GNS3 и дает нам функциональные возможности создать достаточно точную копию реальных информационных инфраструктур с их сетевым, серверным оборудованием и компьютерами конечных пользователей, вычислительной мощности персонального компьютера хватит на эмуляции лишь очень маленькой информационной инфраструктуры. В результате, практические занятия на GNS3 могут проводиться на искусственно созданных сегментах сети, но не на копиях реальных инфраструктур [6,8].

UNetLab

Unified Networking Lab (UNetLab, UNL) – сетевой эмулятор, который представляет собой многопользовательскую платформу для моделирования и создания виртуальных сетей, различных лабораторий, поддерживающий внушительный список телекоммуникационного оборудования. Таким образом, концептуальной новизной продукта UNetLab является возможность запуска и использования программы между разными платформами и разными производителями устройств. Пример графического интерфейса отображен на рисунке 3.

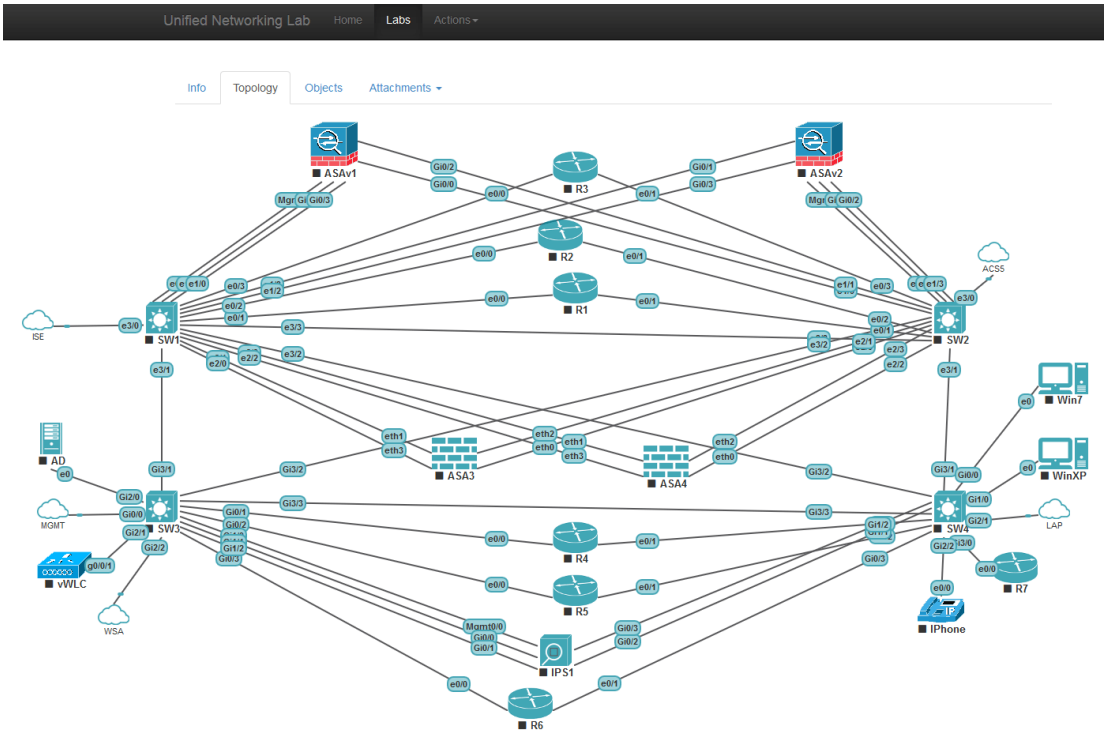

Рисунок 3 - Графический интерфейс эмулятора UNL

В настоящее время эмулятор UNetLab является не только платформой для моделирования виртуальных сетей, но и инструментом для подготовки к различным сертификациям Cisco (для новичков к CCNA/CCNP, так и для профессионалов для подготовки CCIE Routing and Switching, CCIE Security и др.). Кроме того, UNL используется в сетевом инженеринге, в том числе и для системного подхода в выявлении и устранении причин проблемы неполадки сетей (troubleshooting) [8].

Проект UNetLab стартовал в марте 2014 года, но за столь короткий срок стал серьезным конкурентом для таких известных эмуляторов как GNS3 и Cisco Packet Tracer, имея в своем багаже ряд огромных преимуществ. При этом разработка продукта осуществляется и по сей день, выявляются ошибки и выходят различные обновления для расширения функционала программы и списка поддерживаемых устройств [7].

Использование данного подхода позволяет UNL отойти от концепции использования автономных виртуальных машин для эмуляции соответствующих сетевых устройств, и создавать цифровые сетевые лаборатории на основе

программных эмуляторов IOU/IOL, Dynamips и узлов QEMU, объединяя все необходимые программные модули и сценарии в виде одного файла в рамках одной платформы.

Выгодным преимуществом эмулятора UNetLab является то, что он полностью бесплатен, и поэтому может использоваться не только для коммерческих целей, но и для обучения обычными пользователями.

Из достоинств так же следует отметить возможность запуска неограниченного количества экземпляров оборудования (роутеров, коммутаторов, устройств безопасности и т.д.), количество ограничено только аппаратными возможностями рабочего места.

Поддержка оборудования в UNetLab очень широкая. UNL дает возможность запуска образов из VIRL (vIOS-L2 и vIOS-L3), образов ASA, Cisco IOL-образов, образов Cisco IPS, образов XRv и CSR1000v, образов dynamips из эмулятора GNS, образов Cisco vWLC и vWSA. Кроме перечисленных образов поддерживается внушительный список из оборудования других вендоров: Aruba ClearPass, Alcatel 7750 SR, Arista vEOS, Brocade Virtual ADX, Citrix Netscaler VPX virtual, Checkpoint Firewall, HP VSR1000, Juniper Olive (porting), Juniper Networks vMX router, Juniper vSRX, S-Terra Firewall, MS Windows и др [15].

Исходя из общего сравнительного анализа программных платформ эмулятора сетевого оборудования, можно выделить UNetLab и GNS3 как наиболее актуальные и эффективные. Следует отметить, что UNetLab в сравнении с GNS3 имеет ряд технических преимуществ, с помощью которых достигается повышение функционала и, как результат, расширение портфеля предоставления услуг в области сетевого проектирования. Сравнительный анализ функциональных характеристик платформ эмулятора сетевого оборудования UNL и GNS3 приведён в табл. 1 [4,6,7].

Таблица 1 - Сравнительный анализ функциональных характеристик платформ

	UNetLab	GNS3
Графический интерфейс	Удобный единый графический интерфейс пользователя на основе технологии WEB автоматически устанавливается вместе с платформой.	Графический интерфейс пользователя в виде специализированного клиента платформы устанавливается пользователем на ПК и отдельно от платформы.
Специализированное ПО	Нет необходимости в отдельных клиентах для использования платформы.	Требует установки специализированного клиента для последующего использования платформы.
Функциональность	Полноценная поддержка эмуляции канального и сетевого уровней (L2 и L3) без ограничений.	Частичная поддержка эмуляции канального и сетевого уровней (L2 и L3).
Поддержка многопользовательского режима	Многопользовательский функционал, возможность работы нескольких пользователей одновременно.	Строго однопользовательская система.
Ограничения ОЗУ	Нет ограничений ОЗУ под эмуляцию QEMU-устройств.	QEMU поддерживает использование до 2 Гб ОЗУ.
Количество соединений	Отсутствие ограничений по количеству соединений между устройствами в условиях виртуализации QEMU.	Ограничения в 16 соединений между устройствами в рамках виртуализации QEMU.
Масштабируемость	Образы запускаются и работают в рамках одной виртуальной машины или физического сервера.	Необходимость в создании отдельных виртуальных машин для запуска образов в GNS3.
Нативная поддержка графических обозначений	Интерфейс пользователя обеспечивает нативную поддержку пользовательских графических обозначений устройств.	Поддержка организации собственных значений устройств частично присутствует.

Исходя из анализа всех вышеперечисленных программных продуктов, явным фаворитом является UNetLab, в силу своего бесплатного распространения, огромного функционала, большого количества поддерживаемых эмулируемых устройств, а также в удобстве создания тестовых стендов сетевого оборудования в проектирования вычислительных сетей,

именно UNetLab будет выбран в качестве программного эмулятора сетевого оборудования для разработки моделей вычислительных сетей.

1.4 Процесс моделирования вычислительных сетей в UNetLab

Для запуска UNetLab необходимо создать виртуальную машину, на которой и будет развертана наша система. Для создания виртуальной машины использовалось ПО VMware Workstation 12 PRO. Этот программный продукт виртуализации позволяет установить на физический компьютер одну или несколько виртуальных машин. Процесс развертывания UNetLab происходит путем установки исходных файлов на созданной виртуальной машине. По завершению установки, UNetLab готов к работе и становится доступен по IP-адресу, указанному в ходе инсталляции.

Процесс моделирования в UNetLab происходит в графическом интерфейсе программы, который становится доступен через веб-браузер. Пользователю необходимо перейти по веб-адресу в браузере, на котором было развернуто программное обеспечение. После чего, он увидит следующее окно аутентификации пользователя, изображенного на рисунке 4.

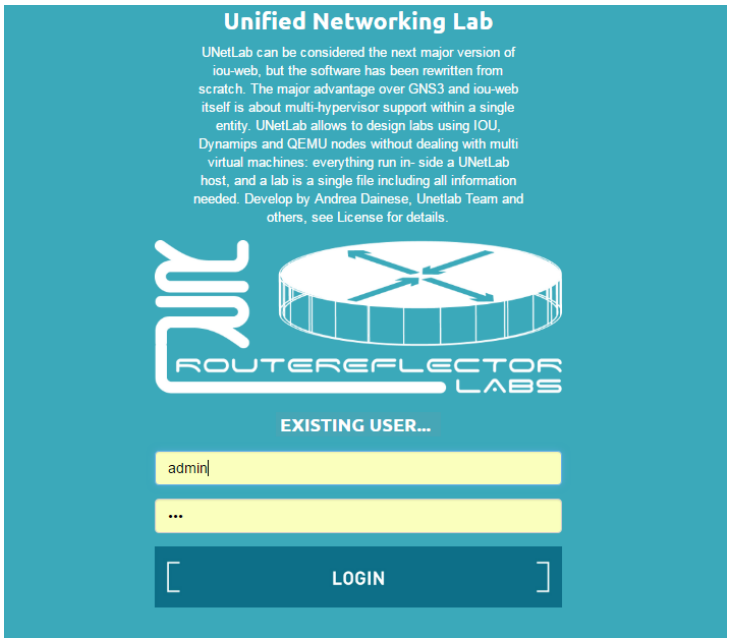

Рисунок 4 - Аутентификация пользователя в системе UNetLab

После успешной аутентификации, пользователь увидит следующее меню, рисунок 5. На котором отображен список всех проектов и панель управления. С помощью панели управления можно управлять уже созданными проектами (удалять, переименовывать, перемещать, импортировать), так и создавать новые. Так же, в меню “Users” можно создать нового пользователя системы и назначить ему права.

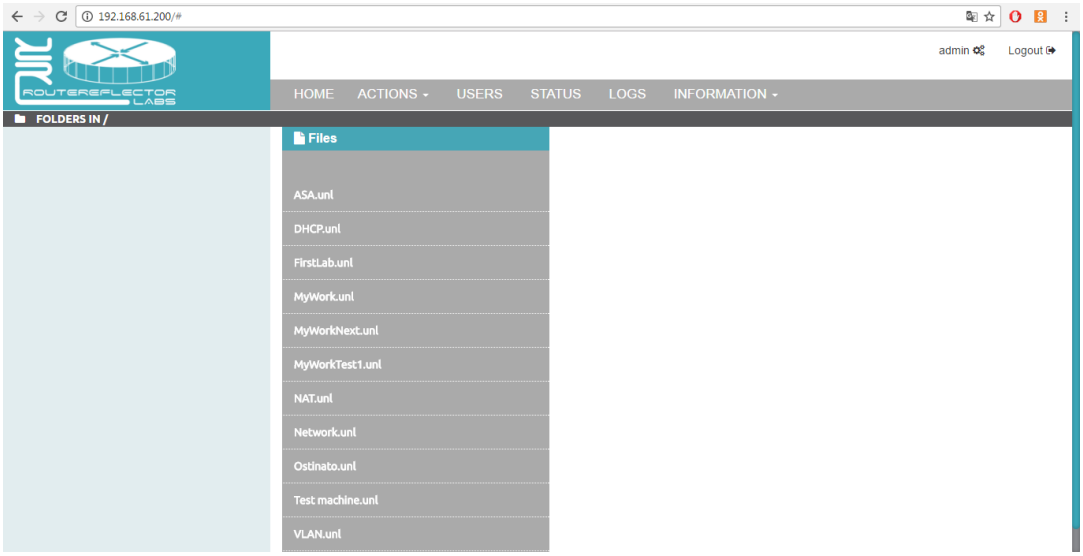

Рисунок 5 - Главное меню системы UNetLab

В меню “Status”, рисунок 6, можно просмотреть текущую статистику используемых ресурсов системой (загрузку ЦП и ОЗУ, количество используемой памяти и т.д.) и количество запущенных образов.

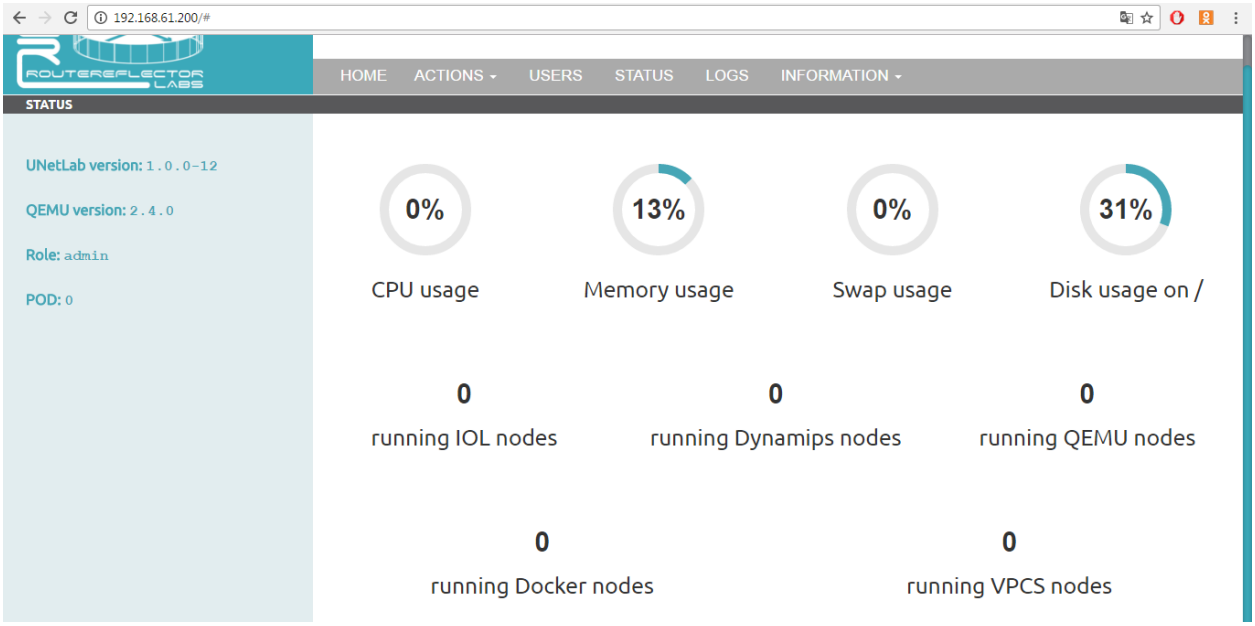

Рисунок 6 - Информация об используемых ресурсах системой UNetLab

Создав новый проект, пользователь попадет на окно рабочего места, рисунок 7. Проектирование будущих вычислительных сетей происходит путем добавления сетевых устройств на рабочую область.

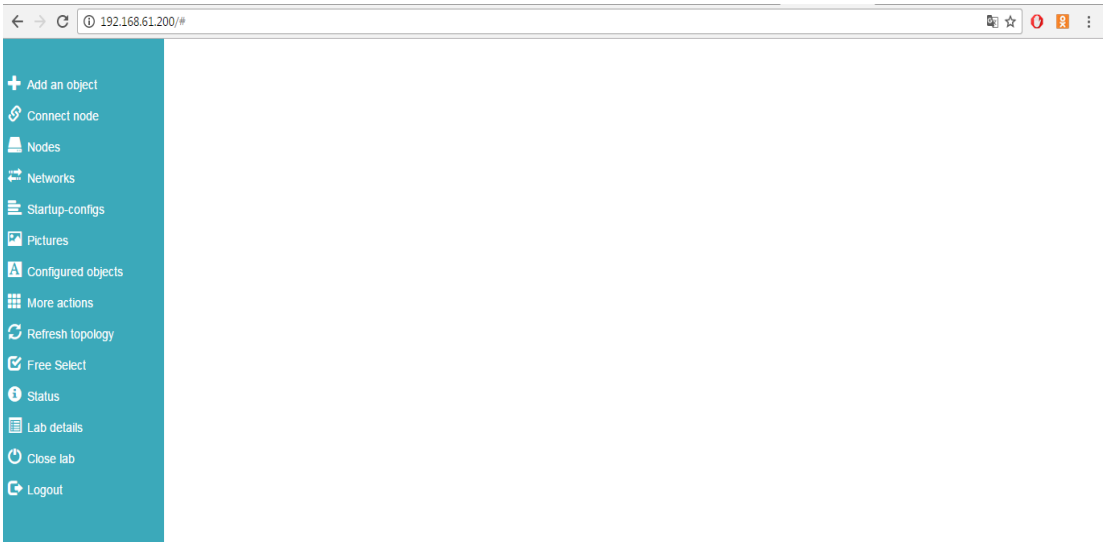

Рисунок 7 - Рабочее место в UNetLab

Во вкладке “Add an object” пользователю доступен список сетевых устройств различных производителей. Выбрав конкретное устройство, появляется возможность задания характеристик устройства: задание имени,

выбор эмулируемого образа устройства, объем оперативной и флэш памяти, количество групп Ethernet портов (в каждой группе по 4 Ethernet порта) и т.д., рисунок 8. Система предоставляет возможность пользователю самому настроить выбранное сетевое устройство. На примере устройств компании Cisco, пользователь выбирает эмулируемый образ сетевого устройства, который эмулирует программную оболочку устройства (Cisco IOS) и путем задания параметров, сам конфигурирует будущее физическое устройство. Таким образом, варьируя параметрами, пользователь может имитировать работу различных, реальных устройств.

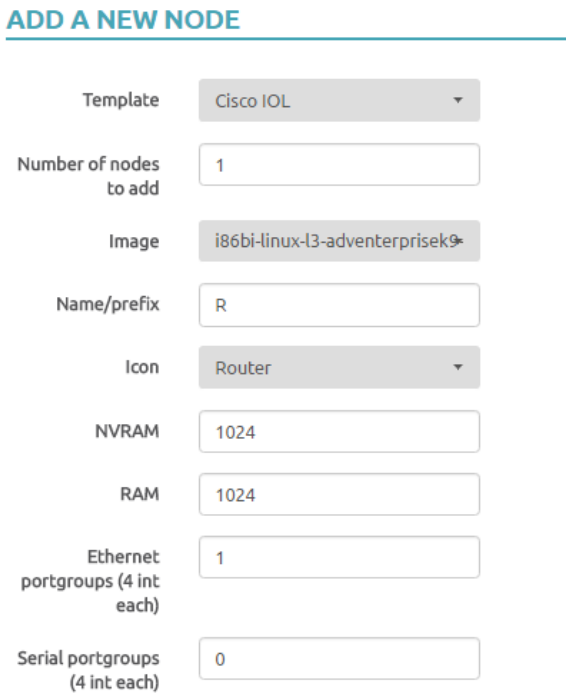

Рисунок 8 - Конфигурирование добавляемого устройства

После того как устройство задано, оно отображается на рабочем поле. Таким образом, пользователь, добавляя на рабочее поле сетевые устройства, конфигурирует будущую архитектуру вычислительной сети.

Для связи устройств между собой необходимо выбрать пункт в меню “Connect node” и соединить необходимые устройства между собой, таким образом сымитировать физическое подключение между ними, рисунок 9.

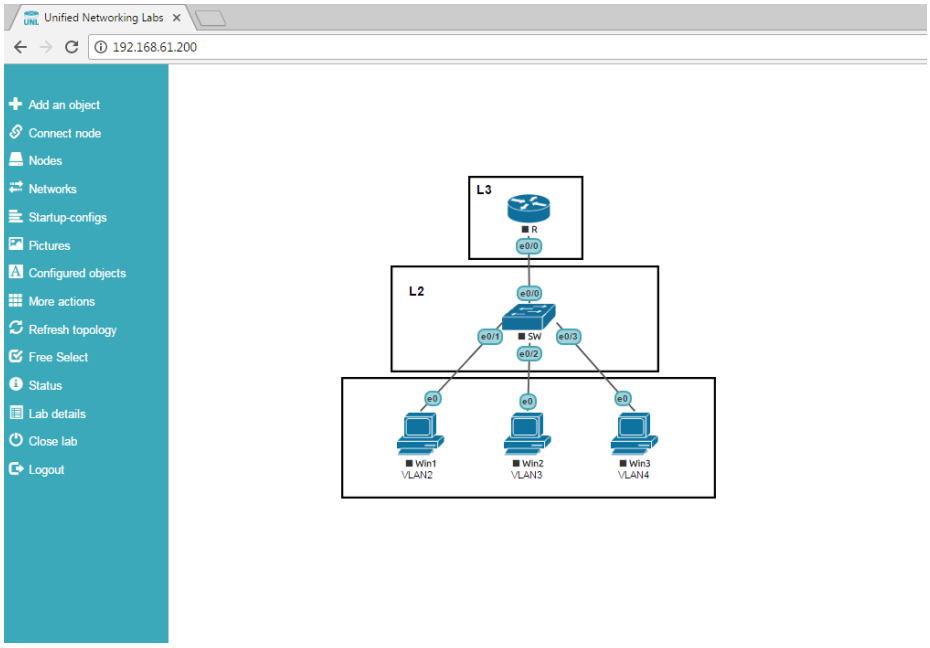

Рисунок 9 - Создание модели вычислительной сети

Так же пользователю доступно добавление различных объектов на рабочее поле, таких как: геометрические объекты, изображения, надписи и их настойка, для организации моделей вычислительных сетей.

Для настройки и конфигурирования добавленных на рабочее поле устройств, в UNetLab встроено ПО PuTTY. PuTTY – это клиент для удаленного доступа к устройствам. После запуска устройства, если нажать на него левой кнопкой мыши, то происходит автоматическое подключение к консоли устройства через PuTTY, в котором пользователь производит настройку устройства.

Также, в UNetLab встроено дополнительно ПО WireShark, являющееся программой-анализатором трафика, с помощью которой можно перехватывать и анализировать сетевой трафик (просматривать содержимое сетевых пакетов) протекающего между устройствами при их взаимодействии.

2 Проектирование вычислительных сетей

2.1 Анализ архитектуры вычислительных сетей

Одним из главных принципов в архитектуре вычислительных сетей является принцип модульности. Принцип модульности подразумевает то, что всю архитектуру вычислительной сети можно разбить на отдельные модули, что, в свою очередь, позволяет сосредоточиться на функционале каждого модуля по отдельности, при этом, такой подход упрощает ее внедрение и управление. Разбиение большой сети на маленькие модули способствует, в первую очередь, устойчивости сети, так как при возникновении неполадок или сбоев в сети можно локализировать имеющуюся проблему. При этом другие модули сети, которые работают стабильно, не затрагиваются. Еще одним преимуществом модульности сети является возможность упрощенной и безболезненной масштабируемости, которая достигается за счет введения дополнительных модулей при возникающей необходимости расширения вычислительно сети [1].

В архитектуре вычислительных сетей используется иерархическая модель сети, изображенная на рисунке 10, которая впервые была предложена инженерами компании Cisco Systems. Согласно данной модели вычислительная сеть подразделяется на три уровня иерархии, каждый из которых выполняет свою определенную функцию [3]. К уровням иерархической модели относятся: уровень доступа (Access Layer), уровень распределения (Distribution Layer) и уровень ядра или ядро сети (Core Layer).

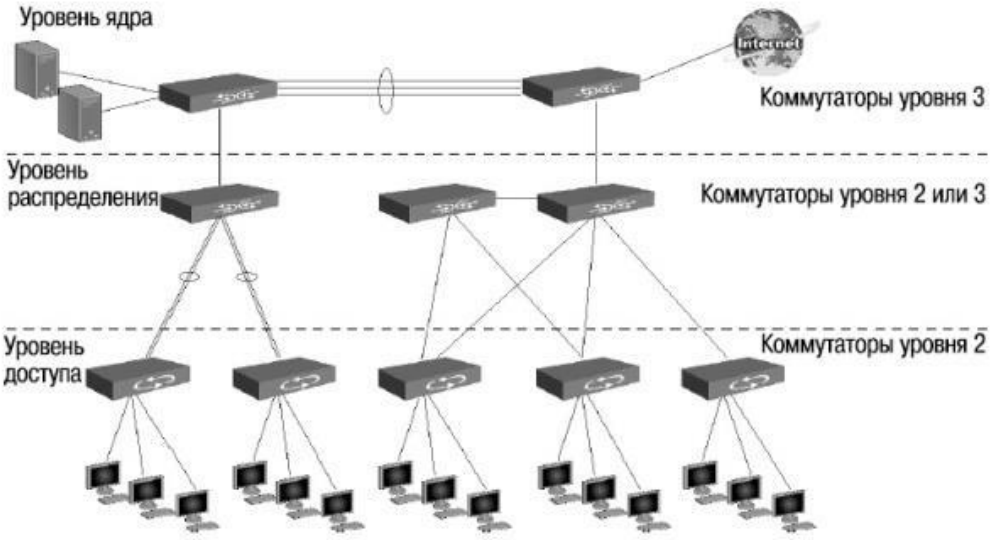

Рисунок 10 - Трехуровневая иерархия вычислительной сети

На уровне доступа (Access Layer) предоставляется доступ к ресурсам сети пользователям или устройствам, таким как сканер, принтер, IP-телефоны и др. Таким образом основная задача этого уровня – это создание точек входа пользователей в объединенную сеть. Уровень доступа зачастую представлен в сети коммутаторами второго уровня (L2) сетевой модели OSI (Open System Interconnection), в редких случаях используются L3-коммутаторы [3,12,13].

Следующим уровнем является уровень распределения (Distribution Layer), основной функцией которого является агрегирование уровней доступа и решение задач маршрутизации. На этом уровне используются устройства третьего уровня L3-коммутаторы (маршрутизаторы), осуществляющие маршрутизацию различного трафика между разными сегментами сети. Также на уровне распределения выполняются функции фильтрации и доступа к глобальным сетям. Объединение коммутаторов в одну сеть позволяет уменьшить количество соединений [2,7,8].

Уровень ядра (Core Layer) используется, как правило, в больших сетях, объединяющих несколько офисов или зданий. Этот уровень отвечает за быструю и своевременную передачу больших объемов трафика. Кроме того, следует отметить, что уровень ядра объединяет уровни распределения, поэтому отказоустойчивость этого уровня имеет важное значение. Ошибка на

уровне ядра будет влиять на всех пользователей сети. Ядро сети представляет собой совокупность мощных коммутаторов и маршрутизаторов.

При построении вычислительной сети помимо иерархической структуры сети нужно руководствоваться следующими основными принципами:

- вычислительная сеть должна быть мультисервисной, что предполагает передачу всех типов трафика, используя единые каналы;
- вычислительная сеть должна строиться на базе открытых стандартов и интерфейсов с целью обеспечения возможности наращивания сети и объединения ее с другими сетями;
- принцип минимизации всех расходов, связанных с созданием и эксплуатацией вычислительной сети. Этот принцип подразумевает, что наиболее эффективной с экономической точки зрения будет сеть, использующая коммутацию пакетов, которая позволит эффективно использовать каналы связи.

Модульность вычислительной сети, о которой упоминалось выше, предполагает под собой создание отдельных модулей под различные функции. К основным модулям вычислительной сети можно отнести модуль сети Интернет, модуль территориальных сетей и серверный модуль [9].

2.2 Описание проектируемых вычислительных сетей

На основе выбранной онлайн-платформы виртуализации UNetLab, будут разработаны несколько моделей сложных вычислительных сетей. Разрабатываемые модели вычислительных сетей буду основываться на использовании сетевого оборудования компании Cisco Systems, являющейся безусловным фаворитом на рыке сетевого оборудования и предлагающей устройства для создания вычислительных сетей от небольшого офиса до крупных корпораций.

Именно путь становления компании от небольшого офиса до крупной компании, имеющей территориально отдаленные филиалы, нуждающейся в

высоких вычислительных ресурсах и их защите, будет отражен в проектируемых моделях вычислительных сетей.

Вся работа будет разделена на несколько этапов, на каждом из которых будет спроектирована вычислительная сеть, отображая развитие компании и решая новые задачи.

На первом этапе будут спроектированы модели вычислительных сетей начального уровня, для предприятия малого уровня. Офисы такого предприятия могут располагаться в одном или нескольких соседних зданиях. Данная модель вычислительной сети будет отображать схему объединения рабочих станций предприятия к сети, для предоставления возможности сетевого взаимодействия между собой, а также продемонстрирует различные варианты этих подключений. Буду рассмотрены как варианты объединения рабочих станций предприятия в единую сеть, находящихся в одном здании (на разных этажах), так и возможность объединения в сеть рабочих станций, расположенных в разных зданиях, находящихся вблизи друг от друга.

На следующем этапе будет спроектирована модель вычислительных сетей, отображающая развитие предприятия. На примере развития будет отображено увеличение подключаемых рабочих станций к сети, а также будет произведена их градация на различные подразделения, включая различные методы подключения рабочих станций к сети продемонстрированных в предыдущей модели. Кроме того, для всех рабочих станций предприятия будет предоставлен доступ в сеть Интернет. Будет смоделирована ситуация, при которой, предприятие, для доступа в сеть Интернет, будет арендовать у провайдера “белый” IP-адрес и только один. Т.е. доступ в глобальную сеть для всех рабочих станций предприятия будет осуществляться только через один, выделенный провайдером, IP-адрес, что значительно сокращает финансовые затраты предприятия. Такой способ доступа в глобальную сеть хорош еще и тем, что скрывает внутреннюю структуру организации вычислительной сети от посторонних.

На заключительном этапе будут спроектированы модели вычислительных сетей, на которых будет отражен рост предприятия и деление на территориально отдаленные филиалы. Будут рассмотрены разные варианты построения сообщающего туннеля для объединения филиалов. При возникновении необходимости сетевого взаимодействия филиалов, весь информационный трафик будет протекать через этот туннель. Поскольку передача информации между филиалами будет происходить за рамками внутренней структуры вычислительной сети, то эту информацию необходимо будет защитить от несанкционированного доступа. Поэтому необходимо будет настроить шифрование всего протекающего трафика “заворачиваемого” в этот сообщающий тоннель.

При росте предприятия его логическим развитием является появление у своего серверного оборудования. Будь то файловый, почтовый или же веб-сервер. В проектируемой модели будет рассмотрен случай, при котором сервер организации, находящийся во внутренней структуре вычислительной сети, скрытой от посторонних пользователей, будет иметь открытый доступ. Т.е. любой пользователь, даже находящийся за пределами сети предприятия, мог иметь доступ к серверу предприятия.

В модели также будет рассмотрен вопрос об отказоустойчивости сети филиала компании. Топология вычислительной сети, в которой расположено серверное оборудование, будет спроектирована таким образом, что при возникновении нарушения физической целостности соединения (разрыв передающей среды, кабеля) работа всей сети не прекратится. Модель вычислительной сети, при выявлении неисправности, автоматически перестроится таким образом, чтобы ее функциональность не была нарушена, тем самым не прерывая работу предприятия.

2.3 Разработка концепций вычислительных сетей

Перед тем, как приступить к разработке моделей вычислительных сетей в UNetLab, необходимо сначала спроектировать концепцию будущих моделей.

Спроектированная концепция будет отображать будущую топологию вычислительных сетей. Таким образом будут спроектированы все узлы будущей вычислительно сети. Будет произведено разбиение сегментов на подсети и распределение адресов для них, а также буду спроектированы все соединения между устройствами.

Разработка такой концепции позволяет учитывать все нюансы будущих сетей, а также избежать ошибок на этапе моделирования сетей в эмуляторе.

Первая концепция, изображенная на рисунке 11, будет отображать простейшую вычислительную сеть, главной целью которой является объединение в единую сеть вычислительные машины предприятия и создание возможности сетевого взаимодействия между ними. Данная сеть будет состоять из нескольких коммутаторов для разбиения группы компьютеров на различные локальные сети, разбиение может происходить по любому принципу (например, по отношению компьютеров к определенному подразделению компании), и маршрутизатора, для обеспечения возможности сетевого взаимодействия между рабочими станциями компаниями, находящихся в разных локальных сетях. Построенная вычислительная сеть данным способом может предполагать различное удаление компьютеров, находящихся в одной локальной сети. Например, на разных этажах одного здания. Таким образом, появляется возможность логического объединения компьютеров на подсети, что значительно упрощает в будущем управление такой сетью и логически структурирует ее.

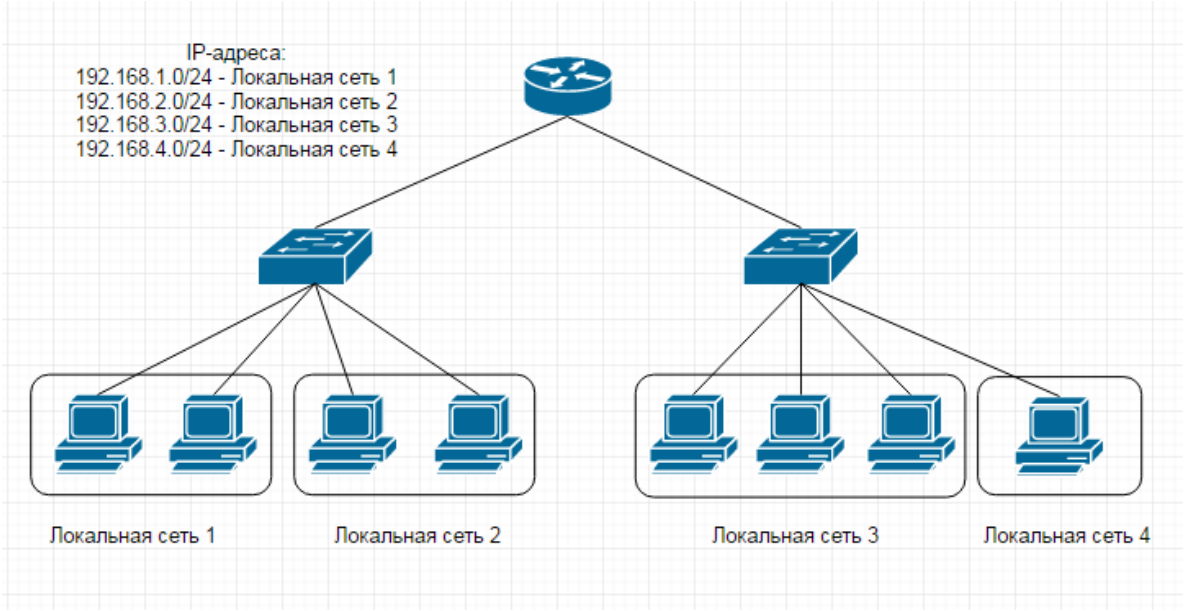

Рисунок 11 - Концепция, отображающая простейшую вычислительную сеть

Следующая концепция, изображенная на рисунке 12, является логическим продолжение предыдущей концепции. На ней продемонстрирован случай, при котором возникает задача логического объединения вычислительных машин в единую локальную сеть, но физически подключенных к разным коммутаторам. В данном случае, компьютеры, логически находящиеся в четвертой локальной сети, но физически подключенные к разным коммутаторам будут иметь возможность сетевого взаимодействия даже без учета маршрутизатора. Однако ситуация с компьютерами логически находящихся в первой локальной сети противоположна, взаимодействие возможно только при наличии маршрутизатора.

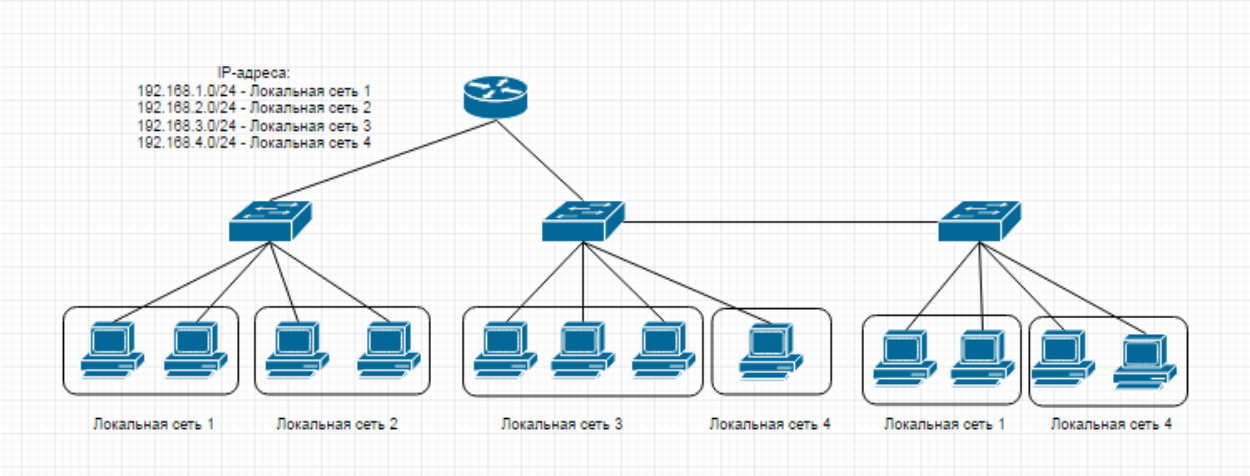

Рисунок 12 - Логическое продолжение предыдущей концепции

Далее, спроектируем концепцию вычислительной сети, изображенную на рисунке 13, отображающую рост предприятия. Увеличивается как количество рабочих станций, так количество сетевых устройств для создания вычислительной сети. Данная концепция включает в себя оба метода подключения рабочих станций из предыдущих концепций. Также в концепции отражено логическое деление компьютеров на локальные сети по отношению к подразделениям на предприятии. Так, например, локальная сеть “Офис2” состоит из компьютеров, физически подключенных к разным коммутаторам.

В концепции также начал фигурировать провайдер – поставщик “белого” IP-адреса. Т.е. доступ в глобальную сеть для всех рабочих станций предприятия будет осуществляется только через один, выделенный провайдером, IP-адрес. Что в свою очередь приведет к экономии финансовых средств компании при аренде только одного IP-адреса.

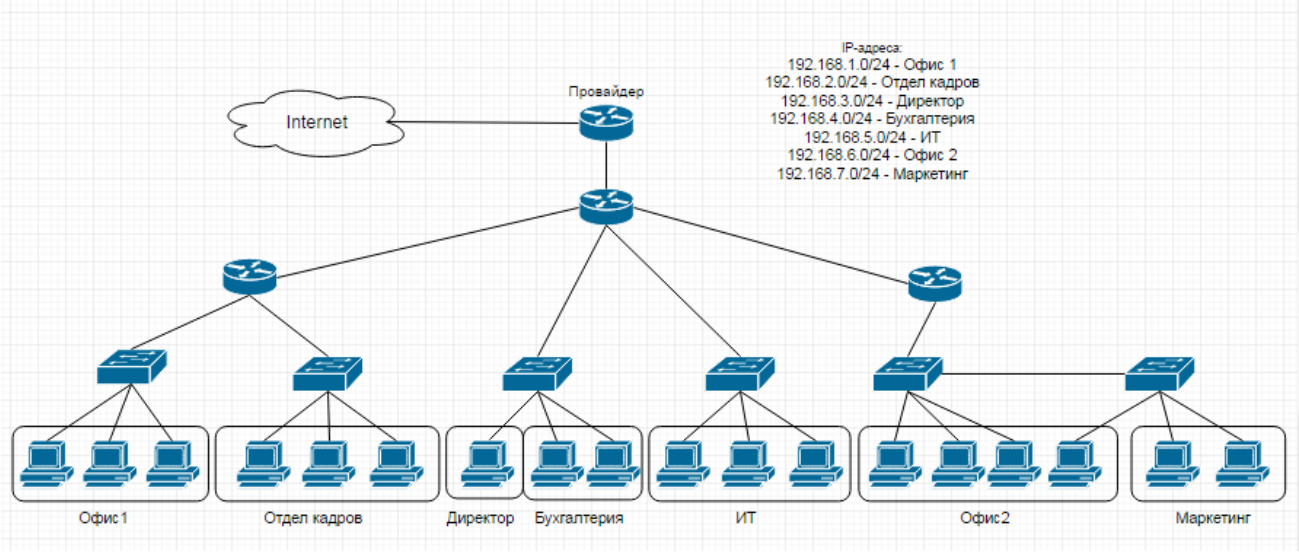

Рисунок 13 - Концепция вычислительной сети развивающегося предприятия

В следующей концепции, изображенной на рисунке 14, отражено деление на территориальные филиалы. Рассмотрен случай, когда у компании появляется территориально отдаленный филиал и появляется необходимость в создании общей вычислительной сети для возможности сетевого взаимодействия между объектами разных филиалов. Поскольку, каждый филиал имеет доступ в интернет через выделенный IP-адрес своим провайдером, то между этими IP-

адресами будет создан специальный тоннель, через который и будет протекать вся информация между филиалами.

Еще в концепции появился новый объект – сервер предприятия. Для любого предприятия серверное оборудование является важнейшим объектом в его инфраструктуре. Это достигается не только стоимостью данного оборудования, но и объемом и значимости хранящейся на нем информации. Выход из строя такого оборудования может привести к полной остановке функционирования всего предприятия, поэтому очень важной целью является обеспечить отказоустойчивый доступ к нему. Для этого топология сети филиала была сформирована таким образом, что при возникновении физического обрыва одного из соединения между коммутационными устройствами, связь с сервером не нарушалась, тем самым не прерывая работу предприятия.

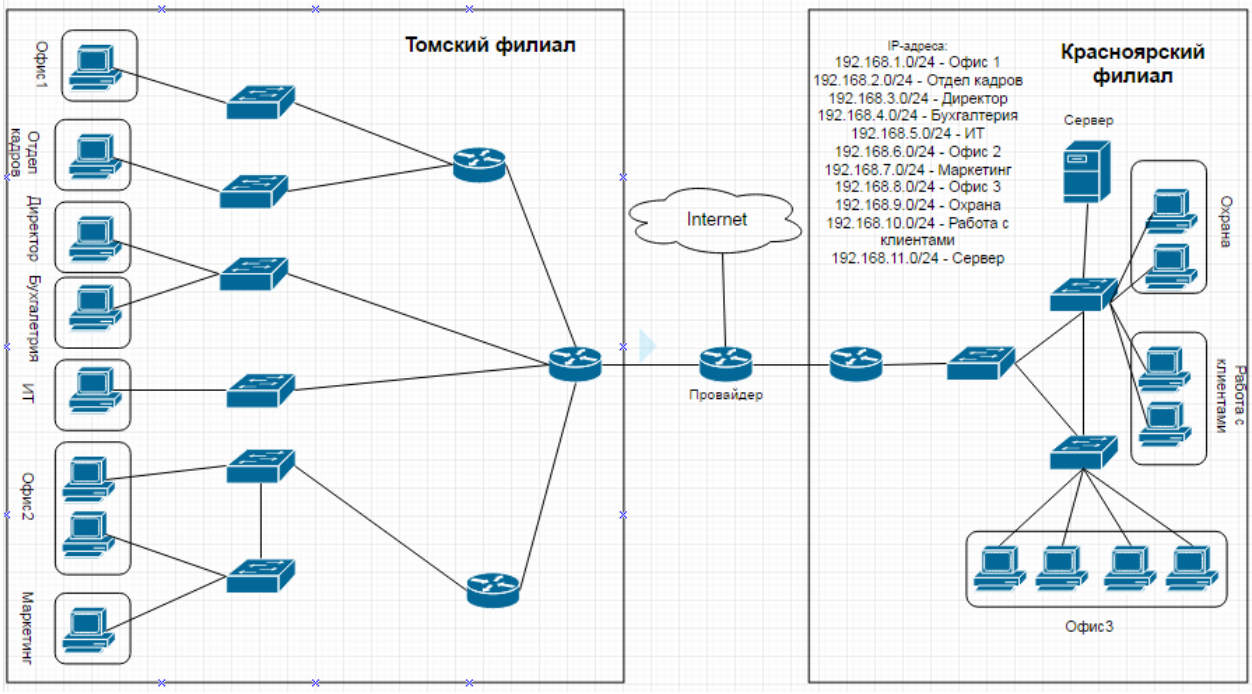

Рисунок 14 - Концепция вычислительной сети с делением на территориально отдаленные филиалы

В заключительной концепции, изображенной на рисунке 15, будет рассмотрен другой вариант построения сообщающего тоннеля между филиалами компании. Данный вариант подразумевать, что каждый филиал арендует как минимум два “белых” IP-адреса у провайдеров. Через каждую пару IP-адресов

будет проведен сообщающий тоннель, один основной и один резервный. В случае обрыва соединения с любой стороны между основным провайдером (на рисунке 15 “Провайдер 1”) топология сети будет в автоматическом режиме перестроена и активизируется второй сообщающийся тоннель через резервного провайдера (на рисунке 15 “Провайдер 2”). Таким образом достигается отказоустойчивость связи между филиалами, что в свою очередь, ведет к надежности функционирования всего предприятия.

Также в концепции отражена возможность доступа к серверу предприятия пользователям из сети Интернет, находящихся за пределами внутренней структуры вычислительной сети предприятия. Т.е. доступ к серверу становится публичным и доступен любым пользователям, вне зависимости от принадлежности к предприятию.

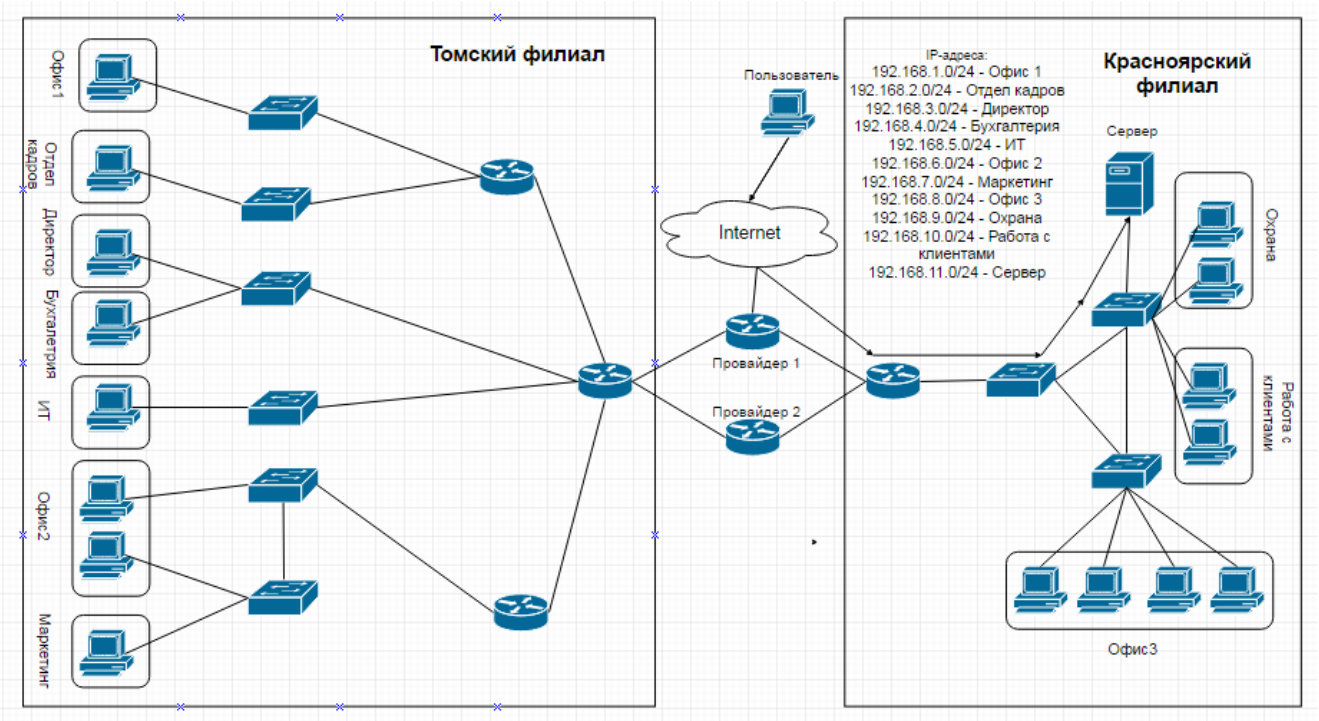

Рисунок 15 - Концепция вычислительной сети с делением на территориально отдаленные филиалы и отказоустойчивостью

Таким образом были сформированы концепции будущих моделей вычислительных сетей. Далее, на основе выбранной онлайн-платформы

виртуализации UNetLab, будут разработаны моделей сложных вычислительных сетей на основе этих концепций и проведены исследования их эффективности.

2.4 Описание используемых технологий

В разработанных ранее концепциях было сформулировано множество различных задач, от логического разбиения на подсети, формирование IP-адресов, для возможности работы в сети, создание сообщающих тоннелей до возможности выхода в сеть Интернет рабочих станций предприятия. Кроме того, для корректного функционирования вычислительной сети, необходимо маршрутизировать весь протекающий трафик внутри сети для возможности сетевого взаимодействия между компьютерами компании. Для достижения всех этих задач, а также задач по повышению отказоустойчивости и защите информации, протекающей по сообщающим тоннелям, необходимо использовать различные сетевые протоколы, с помощью которых и будет организована вся работа внутри вычислительной сети.

Рассмотрим данные технологии поподробнее.

2.4.1 VLAN

Для решения задачи логического структурирования сети будет использоваться технология **VLAN** (Virtual Local Area Network, виртуальная локальная сеть) — это технология, позволяющая на одном физическом сетевом интерфейсе создавать несколько виртуальных локальных сетей, таким образом, разбивай сеть на логические подсети [13]. Технология позволяет устройствам взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях, т.е. с использованием маршрутизаторов.

Отметим основные достоинства данной технологии:

- **Гибкое разделение устройств на группы** как правило, одному VLAN соответствует одна подсеть. Компьютеры, находящиеся в разных VLAN, будут изолированы друг от друга;
- **Уменьшение широковещательного трафика в сети** Каждый VLAN представляет собой отдельный широковещательный домен. Широковещательный трафик не будет транслироваться между разными VLAN;
- **Увеличение безопасности и управляемости сети** в сети, разбитой на виртуальные подсети, удобно применять политики и правила безопасности для каждого VLAN. Политика будет применена к целой подсети, а не к отдельному устройству;
- **Уменьшение количества оборудования и сетевого кабеля** для создания новой виртуальной локальной сети не требуется покупка коммутатора и прокладка сетевого кабеля [12].

2.4.2 DHCP

Для работы компьютера в сети ему необходим IP-адрес. Присваивание IP-адреса компьютеру может быть произведено как статическим методом (ручное задание IP-адреса пользователем), так и динамически (автоматическое присваивание IP-адреса). Поскольку в нашей сети количество рабочих станций может исчисляется десятками, то определенно необходимо использовать именно второй способ.

DHCP (Dynamic Host Configuration Protocol — протокол динамической настройки узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети. Данный протокол работает по модели «клиент-сервер», где в качестве клиента выступает компьютер, запрашивая у DHCP-сервера конфигурации для работы в сети [5]. Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Сетевой администратор может

задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок.

2.4.3 EIGRP

Для корректного функционирования вычислительной сети, необходимо маршрутизировать весь протекающий трафик внутри сети для возможности сетевого взаимодействия между компьютерами. Маршрутизация – это процесс определения маршрута в сети [4].

Маршрутизация бывает 2 видов:

– статическая маршрутизация;

– динамическая маршрутизация.

При статической маршрутизации маршруты будут задаваться администратором сети. Данный вид маршрутизации очень удобен для реализации маленькой сети, но непрактичен в большой сети, так как все маршруты задаются при конфигурации маршрутизатора. Сеть, построенная на статической маршрутизации, является неустойчивой, а также плохо масштабируемой. Данный вид маршрутизации очень неэффективен для реализации вычислительной сети для развивающегося предприятия [12].

В сети, настроенной с помощью динамической маршрутизации, таблица маршрутизации редактируется программно, то есть осуществление динамической маршрутизации происходит за счет протоколов маршрутизации.

EIGRP (Enhanced Interior Gateway Routing Protocol) — это протокол динамической маршрутизации, разработанный фирмой Cisco Systems в 1994 году. Принцип работа протокола заключается в трех основных шагах. Сначала маршрутизаторами происходит обнаружение соседних устройств, затем происходит обмен топологической информацией между соседями и в конце маршрутизаторы анализируют полученную информацию и выбирает из нее маршруты с наименьшей метрикой к каждой сети [6,8].

После того как эти три этапа будут выполнены, в маршрутизаторе будет храниться 3 таблицы: таблица соседних устройств; таблица топологии, полученная от соседних устройств; таблица маршрутизации, с оптимальными маршрутами до всех известных подсетей.

2.4.4 NAT

Для решения задачи доступа в сеть Интернет устройствам компании, через выделенный IP-адрес провайдером, будет использоваться технология NAT.

NAT (Network Address Translation — «преобразование сетевых адресов») — это технология в TCP/IP сетях, с помощью которого несколько компьютеров или устройств частной сети (с частными адресами из таких диапазонов, как 192.168.x.x, 172.x.x.x) могут совместно пользоваться одним адресом IPv4, обеспечивающим выход в глобальную сеть [7]. Основная причина растущей популярности NAT связана со все более обостряющимся дефицитом адресов протокола IPv4 — текущего протокола интернета.

Отметим основные достоинства данной технологии:

- **Экономия публичных IP-адресов**
  через один адрес, можно выпустить больше 65000 серых адресов;
- **Препятствует внешним соединениям доходить до конечных компьютеров**
  если извне на устройство с включенной технологией NAT приходит пакет, который не разрешён, он просто отбрасывается;
- **Скрывает от посторонних глаз внутреннюю структуру сети**
  при трассировке маршрута извне, ничего далее устройства с включенным NAT доступно не будет;
- **Уменьшение количества оборудования и сетевого кабеля**
  для создания новой виртуальной локальной сети не требуется покупка коммутатора и прокладка сетевого кабеля [5,6].

2.4.5 STP

Для решения задачи отказоустойчивого доступа к серверу, отображённого в последней концепции, будет использоваться сетевой протокол STP, а именно его улучшенная версия RSTP, версия протокола STP с ускоренной реконфигурацией топологии.

STP (Spanning Tree Protocol, протокол остовного дерева) — основная задача STP — предотвратить появление петель на канальном уровне. Работа протокола заключается в блокировки дублирующего маршрута, тем самым предотвращая появление петель [8]. В нашей концепции работа протокола будет заключаться в “резервировании” одного маршрута до сервера. При возникновении неисправности в одном из действующих маршрутов ведущего до сервера, он будет продублирован зарезервированным маршрутом, в другое время, “зарезервированный” маршрут будет заблокирован, во избежание петель в топологии [4,7].

2.4.6 VPN/GRE/IPsec

Задача создания сообщающего тоннеля между территориально отдаленными филиалами, для возможности сетевого взаимодействия, не тривиальна и имеет различные варианты решения. В предложенных, в главе 2.3, концепциях было предложено различное решение данной задачи. Первое, это создать сообщающий тоннель между маршрутизаторами филиалов, второе – это создания двух сообщающих тоннелей, один из которых будет находиться в резервном состоянии и будет использоваться только при возникновении неисправности основного. Кроме того, поскольку данные сообщающие тоннели будут выходить за рамки внутренней сети и проходить через сеть Интернет, возникает необходимость защиты протекающей информации, от посторонних пользователей, по таким тоннелям.

Для решения первой задачи будет использоваться технология VPN.

VPN (Virtual Private Network — виртуальная частная сеть) — технология, которая используется для организации постоянного двустороннего канала между

двумя офисами, при этом не требуется установка какого-то дополнительного программного обеспечения. Использование интернета в качестве канала связи между основными филиалами является экономически эффективной альтернативой дорогостоящих арендуемых частных линий [1,13]. Технология VPN подразумевает использование сложного шифрования передаваемых по тоннелю данных для обеспечения безопасности и предотвращения их перехвата.

Шифрование протекающих по VPN тоннелю будет происходить по сетевому протоколу защищенного доступа IPSec.

IPsec (сокращение от **IP Security**) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.

Он предназначен для аутентификации, туннелирования и шифрования IP–пакетов. IPSec прозрачен и очень удобен тем, что может работать практически во всех сетях. Протокол IPSec предусматривает стандартные методы идентификации пользователей или компьютеров при инициации туннеля, стандартные способы использования шифрования конечными точками туннеля, а также стандартные методы обмена и управления ключами шифрования между конечными точками [6][9].

Таким образом, для решения первой задачи по созданию защищенного сообщающего тоннеля будет создан VPN тоннель с шифрованием данных протоколом IPSec.

Поскольку вторая задача подразумевает наличие двух сообщающих тоннелей и автоматической их конфигурации в случае отказа одного из них, то для решения задачи отказоустойчивого тоннеля будет использоваться уже ранее описанный протокол EIGRP. Однако, поскольку работа протокола EIGRP основывается на широковещательной рассылке пакетов на этапе обнаружения ближайших соседей, то уже ранее описанный протокол построения сообщающего тоннеля VPN не подходит для решения этой задачи, одной из особенности работы протокола VPN заключается в непропускании широковещательного трафика. Поэтому, для построения сообщающего тоннеля для решения второй задачи будет использоваться протокол GRE.

GRE (Generic Routing Encapsulation — общая инкапсуляция маршрутов) — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Данный протокол используется для передачи пакетов одной сети, через другую. GRE туннель представляет собой соединение точка – точка и его можно считать одной и разновидностей VPN туннеля, без шифрования данных. Основное достоинство GRE – это возможность передачи широковещательного трафика, что позволяет пропускать через созданный тоннель протоколы маршрутизации, использующие его [1,7]. Таким образом, для решения второй задачи, по построению отказоустойчивых сообщающих тоннелей, будет использоваться протокол GRE с протоколом динамической маршрутизации EIGRP. Поскольку протокол GRE, в отличие от VPN, по умолчанию не требует шифрование данных, протекающих по тоннелю, то необходимо дополнительно настроить его. Для этого будет использоваться уже раннее упомянутый набор протоколов для обеспечения защиты данных IPSec. В итоге, будут созданы 2 сообщающих GRE тоннеля с динамической маршрутизацией EIGRP и защищенных с помощью IPSec.

3 Моделирование вычислительных сетей в UNetLab

На основе выбранной современной онлайн-платформы виртуализации сетевого оборудования UNetLab, были разработаны несколько моделей сложных вычислительных сетей. В спроектированных моделях отображен путь становления компании от небольшого офиса до крупной компании, имеющей территориально отдаленные филиалы, нуждающейся в высоких вычислительных ресурсах и их защите.

Процесс моделирования вычислительных сетей с использованием оборудования компании Cisco Systems происходил путем эмулирования операционной системы Cisco IOS коммутирующего и маршрутизирующего оборудования. Параметры эмулируемых устройств были заданы: для коммутаторов – 128 MByte для оперативной памяти (RAM) и флэш памяти (NVRAM) соответственно; для маршрутизаторов - 128 Mbyte для флэш памяти (NVRAM) и 256 Mbyte для оперативной памяти (RAM). При создании моделей вычислительных сетей с использованием технологии преобразования сетевых адресов – NAT и технологий построения сообщающих тоннелей VPN/GRE, настроенных на маршрутизируемом устройстве, количество оперативной памяти (RAM) было увеличено до 512 Mbyte. Данное увеличение количества оперативной памяти обусловлено работой вышеперечисленных протоколов.

Для моделирования работы серверного оборудования, на платформе UNetLab был развернут веб-сервер.

Таким образом, при физическом воссоздании спроектированных моделей в UNetLab, выбор типа и серии оборудования, может быть обусловлено указанными характеристиками и необходимым количеством портов для подключения оборудования.

В результате, в платформе UNetLab на основе разработанных концепциях вычислительных сетей и использованием выбранный сетевых технологий, были спроектированы модели вычислительных сетей.

3.1 Описание смоделированных вычислительных сетей

Модель №1, изображенная на рисунке 15, представляет собой модель, состоящую из двух коммутаторов SW1 и SW2 и маршрутизатора R, и отображает простейшую вычислительную сеть, главной целью которой является объединение в единую сеть вычислительные машины предприятия и создание возможности сетевого взаимодействия между ними.

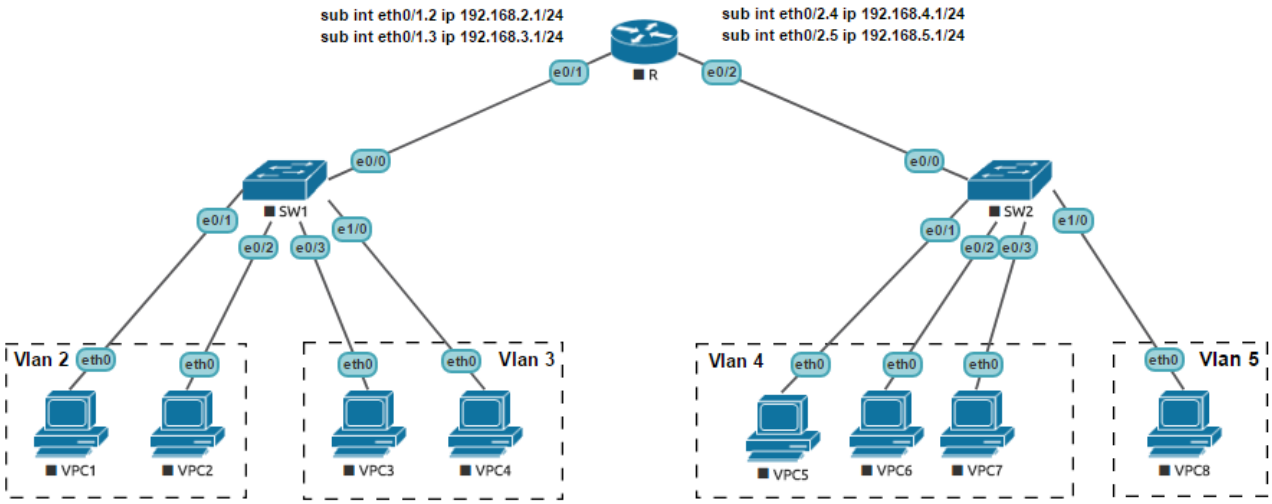

Рисунок 15 - Спроектированная модель вычислительной сети №1

На каждом коммутаторе настроены виртуальные локальные сети (VLAN). На коммутаторе SW1 настроены локальные сети VLAN2 и VLAN3, а на коммутаторе SW2 – VLAN4 и VLAN5. Определение отношения рабочих станций к локальным сетям происходит путем распределения на коммутаторе интерфейсов подключения. Данное распределение интерфейсов по локальным сетям на коммутаторе SW1 продемонстрировано на рисунке 16.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et1/1, Et1/2, Et1/3
2    VLAN0002                          active    Et0/1, Et0/2
3    VLAN0003                          active    Et0/3, Et1/0
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Рисунок 16 - Распределение интерфейсов подключения по локальным сетям на коммутаторе SW1

Таким образом, рабочие станции, находящиеся в распоряжении предприятия, были логически распределены в различные локальные сети. Такое деление рабочих станция на локальные сети позволяет упростить в будущем управление такой сетью и логически структурирует ее.

В модели присутствует маршрутизатор R, задача которого организовывать возможность сетевого взаимодействия между рабочими станциями, находящихся в разных локальных сетях. Так же на маршрутизаторе настроен DHCP-сервер, задача которого заключается в автоматическом присваивании IP-адресов компьютерам-агентам, необходимых для работы рабочих станций в сети. Для этого, на маршрутизаторе были созданы DHCP-пулы с параметрами, передаваемых для каждой локальной сети, необходимые компьютерам для работы в сети. Пример таких DHCP-пулов, настроенных на маршрутизаторе R приведены на рисунке 17.

```
ip dhcp pool DHCP-VLAN2
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 8.8.8.8
!
ip dhcp pool DHCP-VLAN3
 network 192.168.3.0 255.255.255.0
 default-router 192.168.3.1
 dns-server 8.8.8.8
!
ip dhcp pool DHCP-VLAN4
 network 192.168.4.0 255.255.255.0
 default-router 192.168.4.1
 dns-server 8.8.8.8
!
ip dhcp pool DHCP-VLAN5
 network 192.168.5.0 255.255.255.0
 default-router 192.168.5.1
 dns-server 8.8.8.8
```

Рисунок 17 - Настроенные DHCP-пулы на маршрутизаторе R

Модель №2, изображенная на рисунке 18, имеет схожую архитектуру вычислительной сети, что и модель №1, поскольку является логическим продолжение предыдущей.

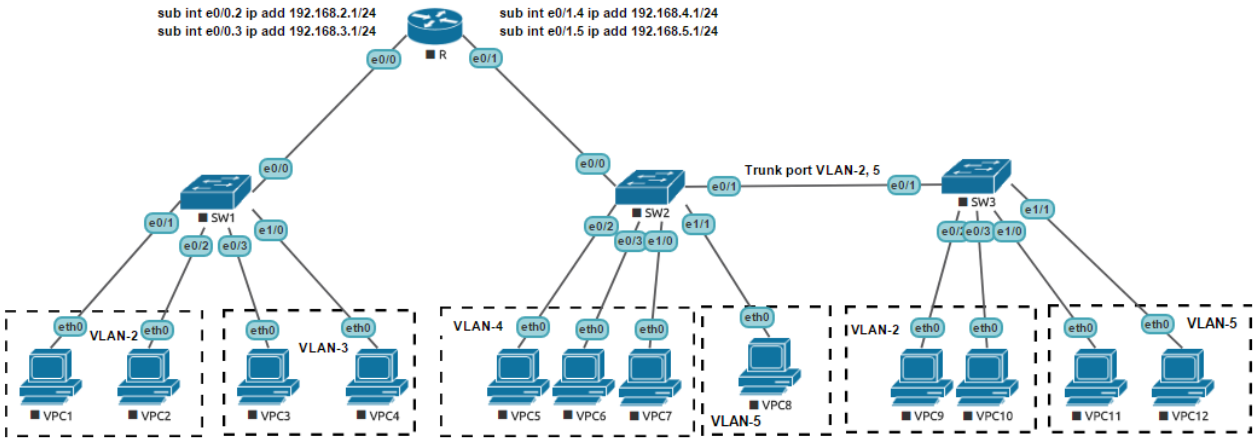

Рисунок 18 - Спроектированная модель вычислительной сети №2

На ней продемонстрирован случай, при котором возникает задача логического объединения вычислительных машин в единую локальную сеть, но физически подключенных к разным коммутаторам. В данном случае, компьютеры, логически находящиеся в пятой локальной сети, но физически подключенные к разным коммутаторам (SW2 и SW3) будут иметь возможность сетевого взаимодействия даже без учета маршрутизатора R. Однако ситуация с компьютерами логически находящихся во второй локальной сети противоположна, взаимодействие возможно только при наличии маршрутизатора. Такое логическое объединение стало возможным путем соединения коммутаторов SW2 и SW3 магистральным портом (Trunk port). Данный магистральный порт служит для передачи трафика локальных сетей (VLAN) между устройствами.

Модель №3, продемонстрированная на рисунке 19, отображает рост предприятия. Увеличивается как количество рабочих станций, так количество сетевых устройств для создания вычислительной сети. Данная концепция включает в себя оба метода подключения рабочих станций из предыдущих

моделей. Также в модели отражено логическое деление компьютеров на локальные сети по отношению к подразделениям на предприятии.

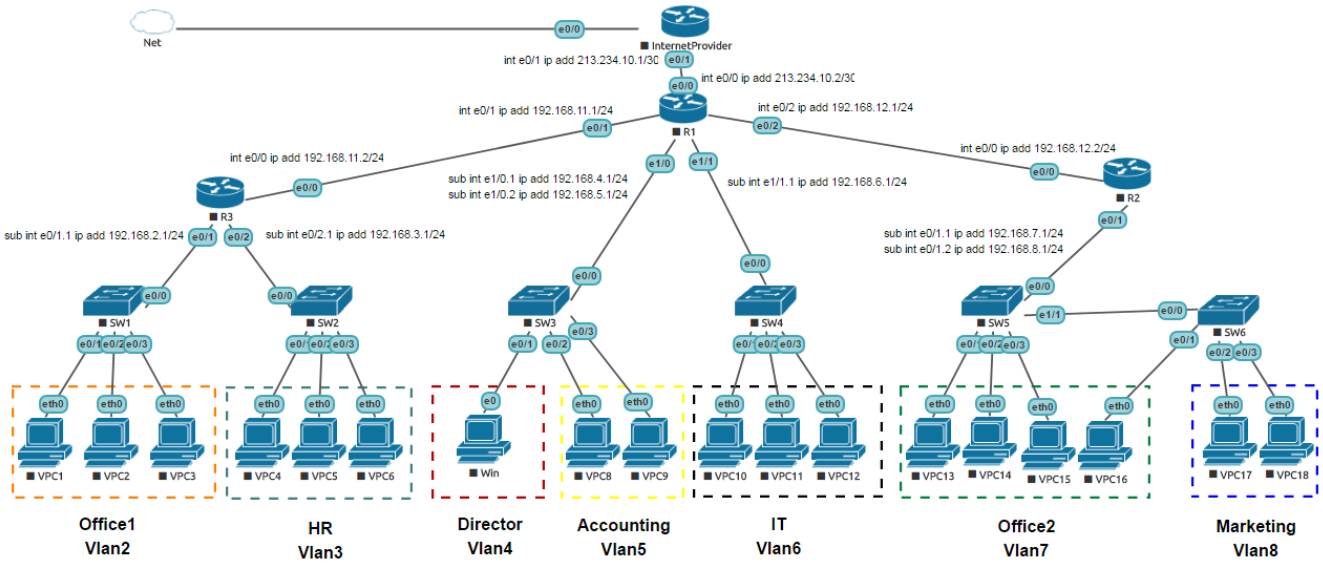

Рисунок 19 - Спроектированная модель вычислительной сети №3

Поскольку в данной модели присутствует три маршрутизатора (R1, R2 и R3), появляется необходимость в маршрутизации протекающего в сети трафика. Для этого был использован протокол динамической маршрутизации EIGRP, работа которого заключается в обмене, соседних маршрутизаторов, информацией об известных им сетям. Настройка данного протокола на маршрутизаторе R1 продемонстрирована на рисунке 20.

```
router eigrp 1
 network 192.168.4.0
 network 192.168.5.0
 network 192.168.6.0
 network 192.168.11.0
 network 192.168.12.0
 network 213.234.10.0
```

Рисунок 20 - Настройки протокола динамической маршрутизации EIGRP на маршрутизаторе R1

В модели также фигурирует провайдер (InternetProvider) – поставщик “белого” IP-адреса. С помощью протокола NAT, через выделенный IP-адрес

провайдером, был открыт доступ всем узлам сети доступ в сеть Интернет. Для этого, на маршрутизаторе R1, был создан лист-доступа с перечнем IP-адресов локальных сетей, необходимых преобразовывать в выделенный провайдером IP-адрес. Т.е. при возникновении обращения в сеть Интернет узлом из локально сети из списка-доступа, происходила трансляция его “серого” IP-адреса в “белый”. Созданный лист-доступа на маршрутизаторе R1 отображен на рисунке 21.

```
ip access-list standard FOR-NAT
 permit 192.168.2.0 0.0.0.255
 permit 192.168.3.0 0.0.0.255
 permit 192.168.4.0 0.0.0.255
 permit 192.168.5.0 0.0.0.255
 permit 192.168.6.0 0.0.0.255
 permit 192.168.7.0 0.0.0.255
 permit 192.168.8.0 0.0.0.255
 permit 192.168.11.0 0.0.0.255
 permit 192.168.12.0 0.0.0.255
```

Рисунок 21 - Лист-доступа с перечнем транслируемых IP-адресов локальных сетей протоколом NAT на маршрутизаторе R1

Модель №4, изображенная на рисунке 22, отображает структурное деление предприятия на территориальные филиалы. Смоделирован случай, когда у компании появляется территориально отдаленный филиал и появляется необходимость в создании общей вычислительной сети для возможности сетевого взаимодействия между объектами разных филиалов.

Поскольку каждый филиал имеет доступ в Интернет, через выделенный IP-адрес своим провайдером, то между этими IP-адресами был создан сообщающий VPN тоннель. Т.е. создавалось явное соединение типа точка-точка между внешними интерфейсами маршрутизаторов R1 и R4. Затем, на созданным VPN тоннель, накладывались политики шифрования из протокола IPSec.

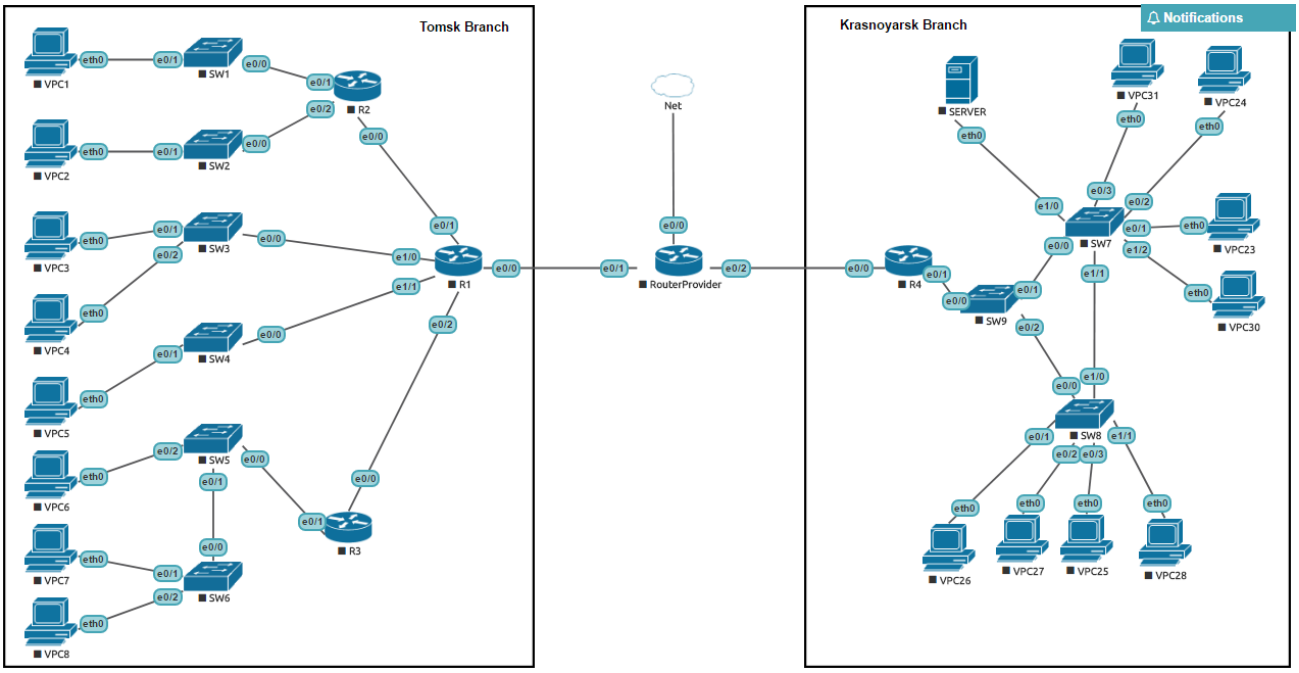

Рисунок 22 - Спроектированная модель вычислительной сети №4

Однако, появляется необходимость маршрутизации трафика, выходящего за пределы локальной сети. Необходимо производить сортировку трафика. Трафик, идущий в локальную сеть филиала, должен быть направлен по VPN тоннелю, а весь остальной трафик необходимо преобразовывать в выделенный провайдером IP-адрес. Для решения этой задачи использовался расширенный список-доступа, в котором явно было указанно, какой трафик необходимо направлять по VPN тоннелю, а какой транслировать в “белый” IP-адрес.

Для обеспечения отказоустойчивого доступа к серверному оборудованию, в топологии вычислительной сети филиала, на коммутаторах SW7, SW8 и SW9 был настроен сетевой протокол STP, а именно его улучшенная версия RSTP, обладающая меньшим временем перестроения топологии, в случае возникновения неисправности.

В заключительной модели №5, изображенной на рисунке 23, был смоделирован другой вариант построения сообщающего тоннеля между филиалами компании.

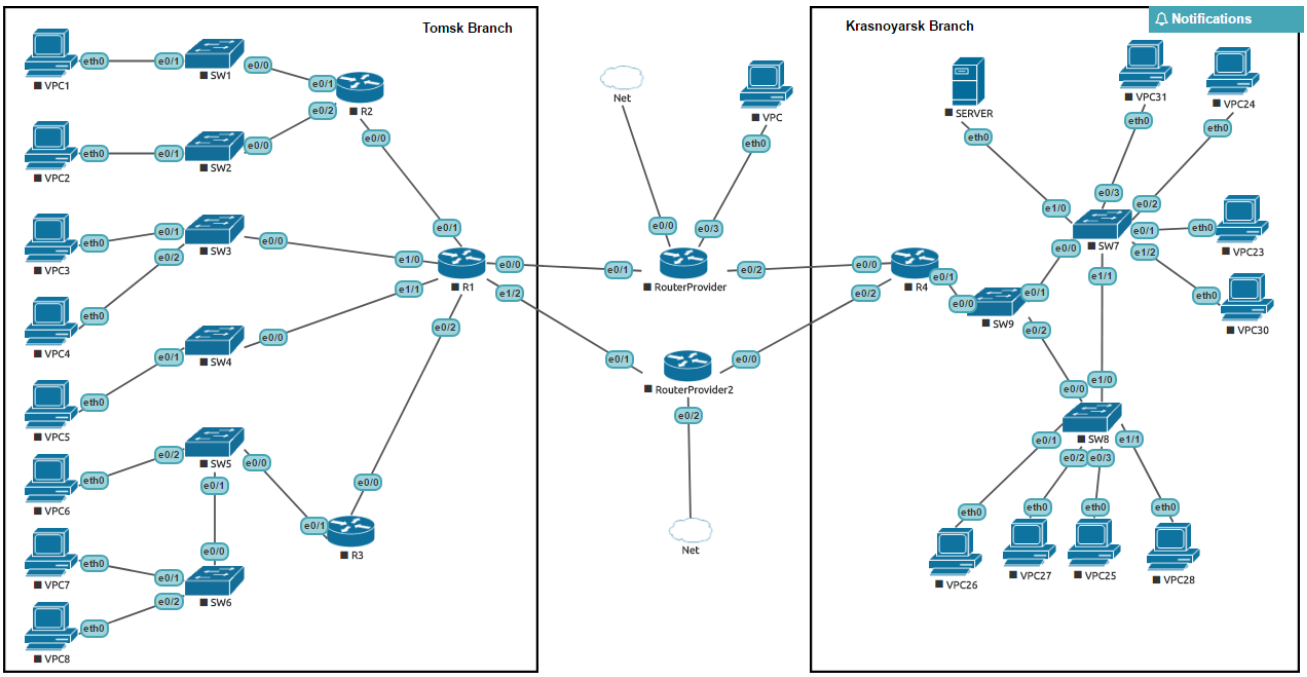

Рисунок 23 - Спроектированная модель вычислительной сети №5

Данный вариант подразумевать, что каждый филиал арендует как минимум два “белых” IP-адреса у провайдеров. Через каждую пару IP-адресов проведены сообщающие GRE тоннели, один основной и один резервный. Для реализации отказоустойчивости тоннелей, на маршрутизаторах филиалов R1 и R4 был настроен, уже ранее использованный, протокол динамической маршрутизации EIGRP. В случае возникновения неисправности основного GRE тоннеля, топология автоматически перестроится и активизируется зарезервированный GRE тоннель.

Также в модели настроен доступа к серверу предприятия пользователям из сети Интернет, находящихся за пределами внутренней структуры вычислительной сети предприятия. При обращении пользователем из сети Интернет на IP-адрес, выделенный провайдером на маршрутизаторе R4, с помощью технологии NAT происходит трансляция в IP-адрес сервера. Таким образом, доступ к серверу становится публичным и доступен всем пользователям из сети Интернет.

3.2 Проведение исследований эффективности смоделированных вычислительных сетей

Для проведения исследований эффективности спроектированных моделей вычислительных сетей необходимо провести симуляцию работы этой сети. Для каждой спроектированной модели в UNetLab были проведены исследования эффективности выполнения поставленных задач при разработке их концепций. Если в результате проведенных исследований достигались поставленные задачи, то модель считалась эффективной.

3.2.1 Проведение исследований возможности сетевого взаимодействия между компьютерами

Для моделей №1 и №2, основной задачей которых является объединение в единую сеть вычислительных машин предприятия и создание возможности сетевого взаимодействия между ними, были проведены исследования возможностей этого взаимодействия. Возможность сетевого взаимодействия определялась успешным выполнением сетевой утилиты для проверки целостности и качества сетевого соединения – «*ping*» между компьютерами одной локальной сети и компьютерами, находящихся в разных локальных сетях.

Для начала, проверим успешное функционирование DHCP-сервера, настроенного на маршрутизаторе R в модели №1, применив на рабочей станции команду «*dhcp -r*» для начала аренды IP-адреса у DHCP-сервера. Результат выполнения команды «*dhcp -r*» на рабочей станции продемонстрирован на рисунке 24.

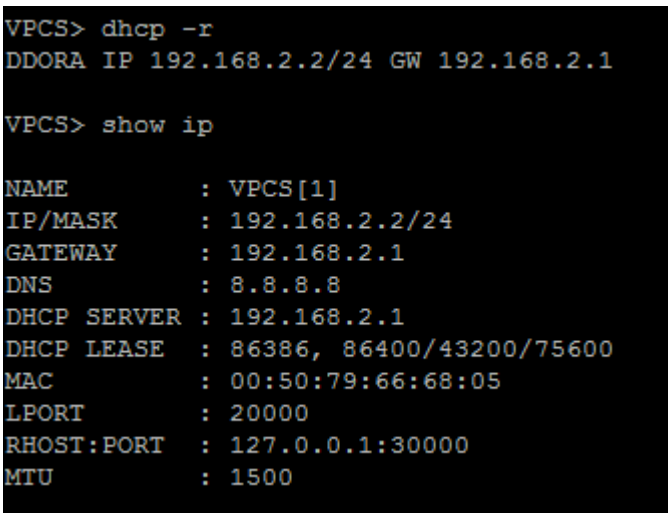

Рисунок 24 - Результат успешной аренды IP-адреса у DHCP-сервера

Из полученных результатов видно, что рабочая станция успешно получила в ответ от DHCP-сервера конфигурацию настроек для работы в сети.

Далее, на примере модели №2, проверим возможность сетевого взаимодействия компьютеров, находящихся в одной локальной сети, в пятой, и в разных, в пятой и второй.

Результаты успешного выполнения сетевого взаимодействия компьютеров, находящихся в одной локальной сети и в разных, продемонстрированы на рисунках 25 и 26 соответственно.

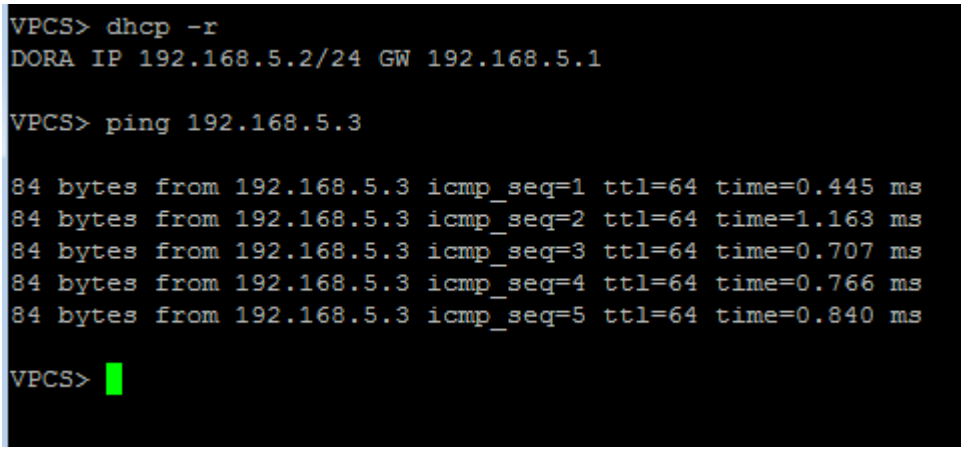

Рисунок 25 - Результат успешного сетевого взаимодействия компьютеров, находящихся в пятой локальной сети

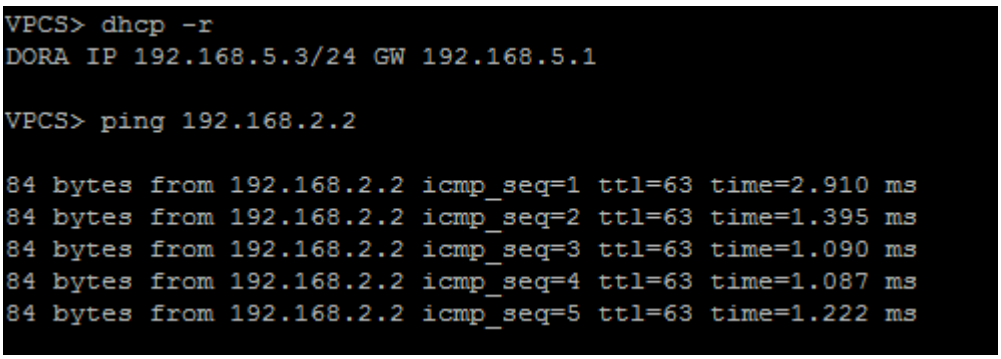

Рисунок 26 - Результат успешного сетевого взаимодействия компьютеров, находящихся в разных локальных сетях

3.2.2 Проведение исследований возможности доступа в сеть Интернет

Для модели №3, основной задачей являлось открытие доступа в сеть Интернет всем рабочим станциям через выделенный провайдером IP-адрес. Провайдер выделил компании “белый” IP-адрес типа 213.234.10.2, через который будет осуществляться доступ в сеть Интернет. Проверим работу, настроенной на маршрутизаторе R1, технологии NAT, попытавшись провести сетевое взаимодействие с рабочей станции компании и узла “Google.ru”. Результат продемонстрирован на рисунке 27.

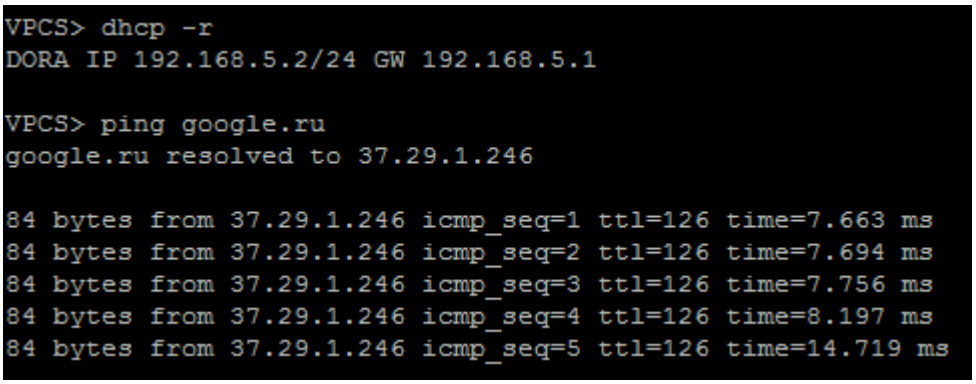

Рисунок 27 - Результат успешного сетевого взаимодействия с узлом “Google.ru”

Проверим результат успешного сетевого взаимодействия с узлом “Google.ru” на маршрутизаторе R1, просмотрев таблицу трансляции IP-адресов технологией NAT.

```
R1#show ip nat translations icmp
Pro Inside global      Inside local       Outside local      Outside global
icmp 213.234.10.2:54501 192.168.5.2:54501 37.29.1.226:54501  37.29.1.226:54501
icmp 213.234.10.2:54757 192.168.5.2:54757 37.29.1.226:54757  37.29.1.226:54757
icmp 213.234.10.2:55013 192.168.5.2:55013 37.29.1.226:55013  37.29.1.226:55013
icmp 213.234.10.2:55269 192.168.5.2:55269 37.29.1.226:55269  37.29.1.226:55269
icmp 213.234.10.2:55525 192.168.5.2:55525 37.29.1.226:55525  37.29.1.226:55525
```

Рисунок 28 - Таблица трансляции IP-адресов на маршрутизаторе R1

На рисунке 28 видно, что при попытке сетевого взаимодействия компьютера предприятия, имеющего IP-адрес 192.168.5.2, с узлом “Google.ru”, произошла трансляция адреса технологией NAT в IP-адрес 213.234.10.2. Что означает, что модель настроена верно.

3.2.3 Проведение исследований эффективности защищенного сообщающего тоннеля и отказоустойчивого доступа к серверному оборудованию

В модели №4 была поставлена задача построения, сообщающего VPN тоннеля между филиалами, а также шифрования, проходящего по нему трафика. Проверим взаимодействия между компьютерами филиалов на примере сетевого взаимодействия между компьютерами находящихся в четвертой локальной сети, Томского филиала, и 9 локальной сети, Красноярского филиала. Результат сетевого взаимодействия изображен на рисунке 29.

```
VPCS> dhcp -r
DORA IP 192.168.4.2/24 GW 192.168.4.1

VPCS> ping 192.168.9.2

84 bytes from 192.168.9.2 icmp_seq=1 ttl=62 time=3.367 ms
84 bytes from 192.168.9.2 icmp_seq=2 ttl=62 time=2.061 ms
84 bytes from 192.168.9.2 icmp_seq=3 ttl=62 time=1.989 ms
84 bytes from 192.168.9.2 icmp_seq=4 ttl=62 time=2.102 ms
84 bytes from 192.168.9.2 icmp_seq=5 ttl=62 time=1.958 ms
```

Рисунок 29 - Результат успешного сетевого взаимодействия между компьютерами филиалов

Для проверки шифрования, проходящего по VPN тоннелю, трафика, было использовано дополнительно ПО WireShark, являющееся программой-анализатором трафика.

Для начала, перехватим трафик, идущий между компьютерами филиалов, изнутри локальной сети Томского филиала, рисунок 30.

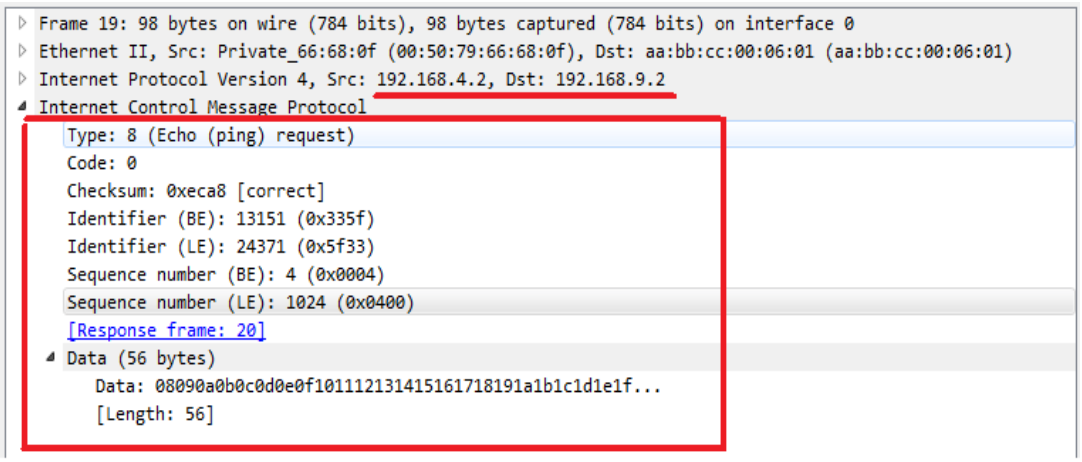

Рисунок 30 - Содержимое информации, передающейся между компьютерами филиалов, в незашифрованном виде

И перехватим трафик, идущий между компьютерами филиалов, извне локальной сети Томского филиала, внутри VPN тоннеля, рисунок 31.

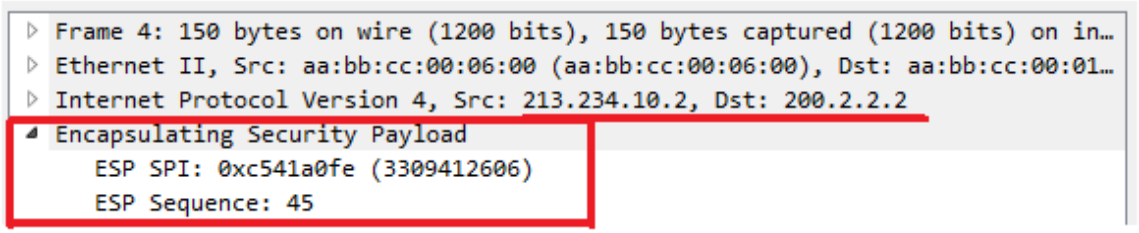

Рисунок 31 - Содержимое информации, передающейся между компьютерами филиалов, в зашифрованном виде

Из полученных результатов видно, что до шифрования была доступна информация о типе протокола и его содержимом, после шифрования, только название алгоритма шифрования.

Отказоустойчивый доступ к серверному оборудованию проверим путем запуска команды «*ping –c 15*» на рабочей станции филиала и одновременно вручную разорвем передающую среду между коммутаторами SW8 и SW9.

```
VPCS> ping 192.168.12.5 -c 15

84 bytes from 192.168.12.5 icmp_seq=1 ttl=63 time=1.689 ms
84 bytes from 192.168.12.5 icmp_seq=2 ttl=63 time=1.594 ms
84 bytes from 192.168.12.5 icmp_seq=3 ttl=63 time=1.494 ms
84 bytes from 192.168.12.5 icmp_seq=4 ttl=63 time=1.452 ms
84 bytes from 192.168.12.5 icmp_seq=5 ttl=63 time=1.571 ms
84 bytes from 192.168.12.5 icmp_seq=6 ttl=63 time=1.667 ms
84 bytes from 192.168.12.5 icmp_seq=7 ttl=63 time=1.747 ms
84 bytes from 192.168.12.5 icmp_seq=8 ttl=63 time=1.741 ms
84 bytes from 192.168.12.5 icmp_seq=9 ttl=63 time=1.593 ms
84 bytes from 192.168.12.5 icmp_seq=10 ttl=63 time=1.879 ms
84 bytes from 192.168.12.5 icmp_seq=11 ttl=63 time=1.601 ms
84 bytes from 192.168.12.5 icmp_seq=12 ttl=63 time=1.599 ms
84 bytes from 192.168.12.5 icmp_seq=13 ttl=63 time=1.488 ms
84 bytes from 192.168.12.5 icmp_seq=14 ttl=63 time=1.654 ms
84 bytes from 192.168.12.5 icmp_seq=15 ttl=63 time=1.897 ms
```

Рисунок 32 - Результат сетевого взаимодействия с серверным оборудованием при принудительном разрыве соединения между коммутаторами SW8 и SW9

Из полученных результатов, продемонстрированных на рисунке 32, видно, что при возникновении неисправности в передающей среде, ни один пакет, при сетевом взаимодействии с серверным оборудованием, не пропал.

3.2.4 Проведение исследований эффективности отказоустойчивого сообщающего тоннеля и доступности сервера из сети Интернет

В модели №5 была поставлена задача построения отказоустойчивого сообщающего тоннеля между филиалами. Отказоустойчивость тоннеля проверим путем запуска продолжительного сетевого взаимодействия, между компьютерами филиалов командой «*ping –c 100*» и одновременно, вручную, разорвем передающую среду тоннеля между маршрутизаторами R1 и R4.

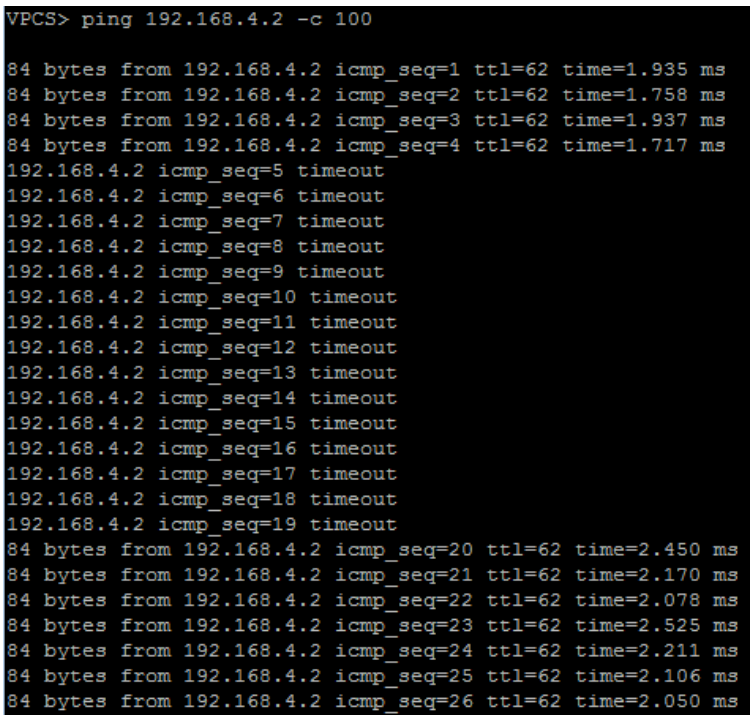

Рисунок 33 - Результат сетевого взаимодействия между компьютерами филиалов при возникновении разрыва сообщающего тоннеля

Из полученных результатов, продемонстрированных на рисунке 33, видно, что процесс перестроения сообщающего тоннеля, в случае возникновения неисправности, занимает примерно 15 секунд. По прошествии данного времени, связь с филиалами восстанавливается.

Далее, проверим доступность сервера для пользователей из сети Интернет. Для этого, на машине под управление операционной системы Windows 7, через веб-браузер, зайдем на IP-адрес 200.2.2.2.

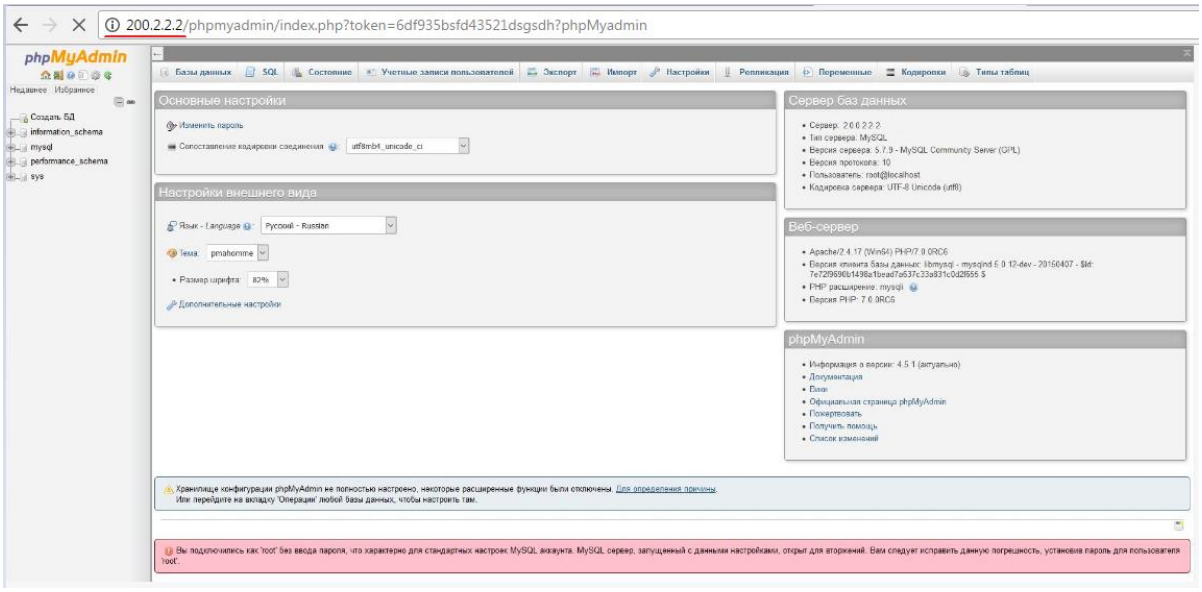

Рисунок 34 - Результат обращений к серверу для пользователя из сети Интернет

Как видно из результатов, рисунок 34, доступность сервера компании для пользователей из сети Интернета достигнута. При обращении на IP-адрес 200.2.2.2, выделенный провайдером, с помощью технологии NAT, произошло транслирование на IP-адрес сервера, на котором развернут веб-сервер.

3.2.5 Проведение исследований нагрузочного тестирования смоделированных вычислительных сетей

Для проведения исследований эффективности спроектированных моделей вычислительных сетей необходимо провести симуляцию работы этой сети, подвергнув её нагрузкам, т.е. произвести генерацию большого объема трафика внутри нее. Для этой задачи, в UNetLab предусмотрен генератор трафика Ostinato, которым мы и воспользуемся. Ostinato представляет собой устройство – дрон, который физически подключается к модели вычислительной сети. Управление же происходит с компьютера пользователя, путем запуска на нем графического интерфейса. Пользователю доступна настройка типа генерируемого трафика, его объема, источника и назначения.

Для проведения исследований, дрон Ostinato был подключен к спроектированным моделям вместо рабочих станций, таким образом, будет происходить имитация работы пользователей в сети путем генерации трафика

дроном Ostinato. Пример подключения дрона Ostinato к модели вычислительной сети продемонстрирован на рисунке 35.

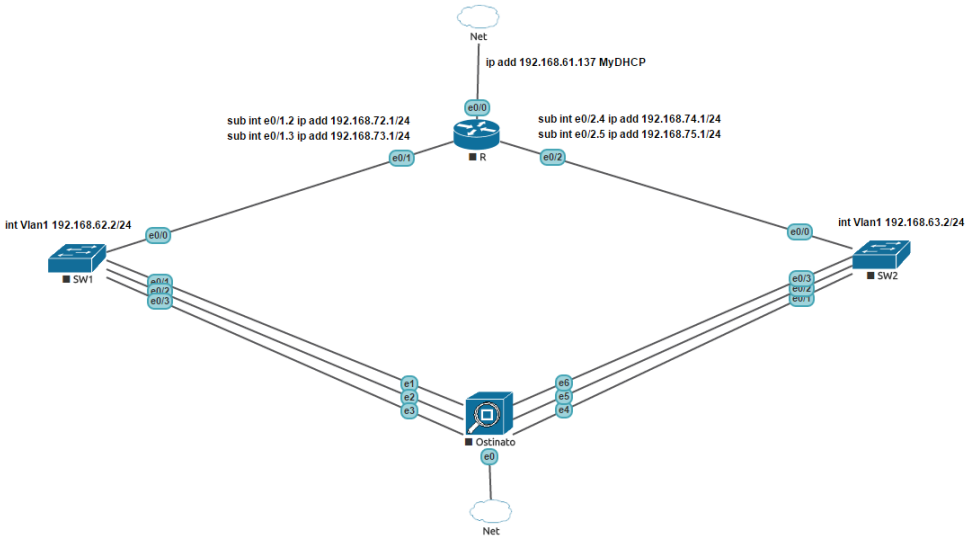

Рисунок 35 - Пример подключения дрона Ostinato к спроектированной модель вычислительной сети.

Для анализа работы моделей вычислительных сетей под нагрузкой необходимо собирать информацию с устройств. Сделать это можно при помощи протокола SNMP (Simple Network Management Protocol, простой протокол сетевого управления). Для этого, было использовано программное обеспечение PRTG Network Monitor, с помощью которого, по протоколу SNMP, собиралась статистика работы сетевого оборудования.

Тестирование проводилось путем генерации бесконечного трафика дроном Ostinato, передаваемого между локальными сетями.

В результате такого нагрузочного тестирования, были получены следующие результаты, рисунки 36 и 37:

- Максимальная загруженность каналов на коммутаторах SW1 и SW2 была равна 173 кб/с;
- Максимальная загруженность каналов на маршрутизаторе была равна 4,83 кб/с;
- Загрузка процессора маршрутизатора не превышала 1%.

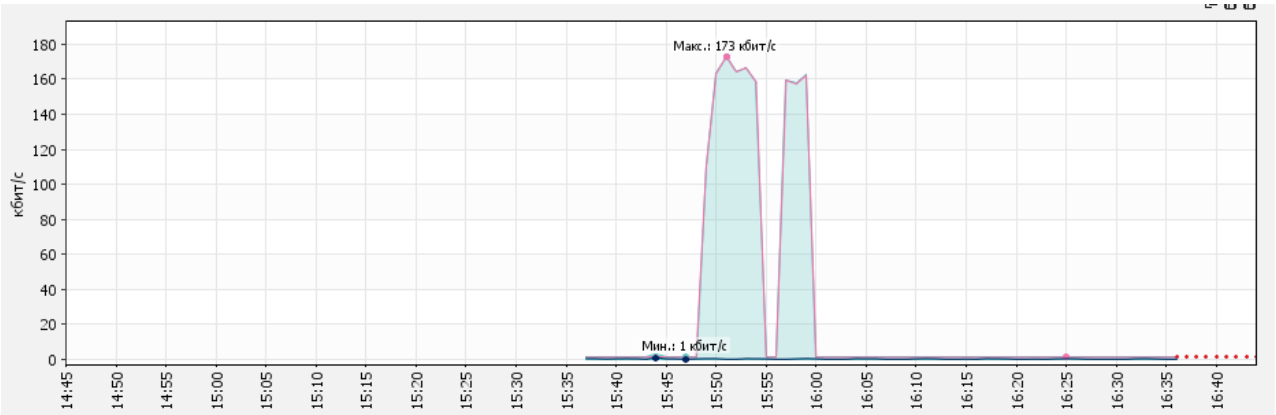

Рисунок 36 - Результаты нагрузочного тестирования для коммутаторов

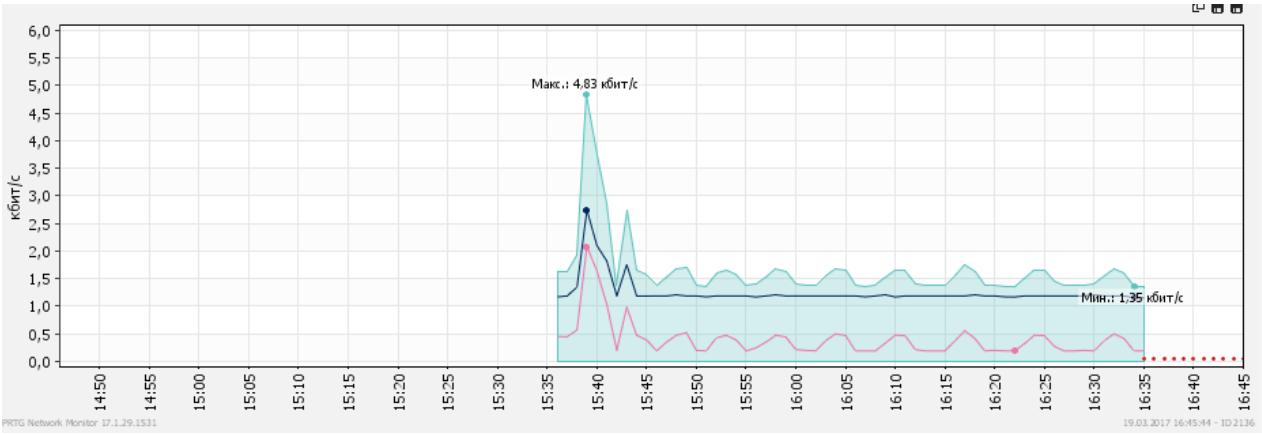

Рисунок 37 - Результаты нагрузочного тестирования для маршрутизатора

Полученные результаты оказались не репрезентативными и даже близко не соответствуют параметрам реального оборудования, заявленных производителем оборудования. Такие результаты обусловлены тем, что сетевое оборудование, выпускаемое компанией Cisco Systems, это прежде всего оборудование, состоящее как из программного обеспечения (Cisco IOS), так и аппаратного обеспечения. При моделировании работы этого оборудования в платформе UNetLab, происходит эмуляция только программного обеспечения, оболочки Cisco IOS, а все эмуляция аппаратного обеспечения ложится на оборудовании вычислительной машины, на которой данная платформа установлена.

Таким образом, при физическом воссоздании спроектированных моделей в UNetLab, выбор типа и серии оборудования, может быть обусловлено заданными характеристиками при моделировании работы и необходимым количеством портов для подключения оборудования.

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
8ИМ5А	Окуневу Дмитрию Александровичу

Институт	Кибернетики	Кафедра	ИСТ
Уровень образования	магистратура	Направление/специальность	Информационные системы и технологии

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. *Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих*	*Должностные оклады, ставки социального налога, тарифы на электроэнергию и т.д.*
2. *Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования*	*Ставка НДС*
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. *Оценка коммерческого и инновационного потенциала НТИ*	*Коммерческий потенциал*
Перечень графического материала *(с точным указанием обязательных чертежей):*	
1. *Сегментирование рынка* 2. *График проведения и бюджет НТИ* 3. *Оценка ресурсной, финансовой и экономической эффективности НТИ*	

Дата выдачи задания для раздела по линейному графику	1.05.2017

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. менеджмента	Попова С.Н.	к.э.н		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ИМ5А	Окунев Дмитрий Александрович		

4 Финансовый менеджмент, ресурсоэффективность и ресурсосбережение

Целью данного раздела является определение оценки коммерческого потенциала, перспективности и альтернатив проведения научных исследований с позиции ресурсоэффективности и ресурсосбережения, а также планирование и формирование бюджета научных исследований, определение ресурсной (ресурсосберегающей), финансовой, бюджетной, социальной и экономической эффективности исследования.

Научно-исследовательская работа направлена на разработку моделей сложных вычислительных сетей на основе современной онлайн-платформе UnetLab.

4.1 Оценка коммерческого потенциала и перспективности проведения научных исследований с позиции ресурсоэффективности и ресурсосбережения

4.1.1 Потенциальные потребители результатов исследования

Целевой аудиторией проектируемых моделей вычислительных сетей являются физические и юридические лица, связанные с потребностями пользователей в информационном обеспечении, а также преподаватели или студенты, занимающиеся изучением современных методов моделирования вычислительных систем.

Целевым рынком для данной разработки является рынок информационного обеспечения с применением современных средств и протоколов для создания сетевой инфраструктуры.

Исходя из вышеизложенного, сегментацию рынка можно произвести по следующим критериям:

Сегментация целевого рынка для данной разработки по виду потребителей:

- Образовательные учреждения;

- Коммерческие предприятия;

Сегментация коммерческих потребителей по масштабу:

- Крупные предприятия;
- Средние предприятия;
- Малые предприятия;
- Отдельные индивидуальные предприятия.

Сегментация по масштабу системы:

- Крупная;
- Средняя;
- Малая;

Карта сегментации рынка на основании наиболее значимых критериев для рынка представлена в таблице 2.

Таблица 2 - Карта сегментирования рынка по наиболее важным критериям

		Размер кампании-заказчика			
		Крупные	Средние	Мелкие	Отдельные ИП
Масш таб	Крупная				
	Средняя				
	Малая				

Примечание к таблице 2:

- области, где имеются готовые решения по информационному обеспечению.

Исходя из вышеприведенных данных, можно сделать выводы, определяющие результаты сегментирования рынка:

Основным сегментом рынка выбрана область разработки моделей с малым масштабом для мелкого размера компании и отдельных ИП;

Сегменты, на которые необходимо ориентироваться: разработка и дальнейшее исследование возможностей проектируемых моделей вычислительных сетей;

Сегменты рынка, которые привлекательны для развития разработок в будущем: создание моделей вычислительных сетей инфраструктуры подразделений средних и крупных организаций.

4.2 Организация и планирование работ

При организации работ в рамках магистерской работы необходимо планировать занятость каждого участника проекта в работе. На данном этапе определяется полный перечень работ, распределение времени работ между всеми участниками. В качестве структуры, показывающей необходимые данные, используется линейный график работ, представленный в таблице 3.

Таблица 3 – Перечень этапов работ и распределение исполнителей

Основные этапы	№ раб	Содержание работ	Должность исполнителя
Выбор задания, утверждение темы	1	Выбор и утверждение задания и темы работы	Студент – 30%, Научный руководитель - 70%
Выбор направления исследований	2	Подбор и изучение материалов по данной теме, изучение предметной области	Студент - 70%, Научный руководитель – 30%
	3	Календарное планирование работ по теме	Студент – 20%, Научный руководитель – 80%
	4	Исследование существующих систем эмуляции сетевого оборудования	Студент - 70%, Научный руководитель - 30%
Теоретические и экспериментальные исследования	5	Описание концепций вычислительных сетей	Студент - 100%
	6	Разработка моделей вычислительных сетей	Студент - 100%
Обобщение и оценка результатов	7	Проведение исследований эффективности	Студент – 70%, Научный руководитель – 30%
	8	Оценка эффективности полученных результатов	Студент – 50%, Научный руководитель – 50%
Оформление пояснительной записки по ВКР	9	Оформление расчётно-пояснительной записки по ВКР	Студент – 100%

4.3 Продолжительность этапов работ

Расчет продолжительности этапов работ может осуществляется опытно-статистическим методом. Для расчета ожидаемого значения продолжительности работ $t_{ож}$ применяются две оценки: $t_{\min}$ и $t_{\max}$ (метод двух оценок).

$$t_{ожс} = \frac{3t_{\min} + 2t_{\max}}{5},$$

где $t_{\min}$ – минимальная трудоемкость работ, чел/дн;

$t_{\max}$ – максимальная трудоемкость работ, чел/дн.

Для выполнения перечисленных в таблице 3 работ требуются специалисты: научный руководитель (НР) и студент (С).

Для построения линейного графика рассчитывается длительность этапов в рабочих днях, а затем осуществляется её перевод в календарные дни. Расчёт продолжительности выполнения каждого этапа в рабочих днях ($T_{РД}$) выполняется по формуле:

$$T_{РД} = \frac{t_{ожс}}{K_{ВН}} \cdot K_{Д},$$

где $t_{ожс}$ – продолжительность работы, дн.;

$K_{ВН}$ – коэффициент выполнения работ ($K_{ВН} = 1$);

$K_{Д}$ – коэффициент, учитывающий дополнительное время на компенсацию непредвиденных задержек и согласование работ ($K_{Д} = 1,2$).

Расчёт продолжительности этапа в календарных днях осуществляется по формуле:

$$T_{КД} = T_{РД} \cdot T_{К},$$

где $T_{КД}$ – продолжительность выполнения этапа в календарных днях;

$T_{РД}$ – продолжительность выполнения этапа в рабочих днях;

$T_{К}$ – коэффициент календарности.

Коэффициент календарности рассчитывается по формуле:

$$T_{К} = \frac{T_{КАЛ}}{T_{КАЛ} - T_{ВД} - T_{ПД}},$$

где $T_{КАЛ}$ – календарные дни, $T_{КАЛ} = 365$;

$T_{\text{ВД}}$ – выходные дни, $T_{\text{ВД}} = 52$;

$T_{\text{ПД}}$ – праздничные дни, $T_{\text{ПД}} = 10$.

Подставив значения в формулу, получим следующий результат:

$$T_K = \frac{365}{365 - 52 - 10} = 1{,}205.$$

В таблице 4 приведена длительность этапов работ и число исполнителей, занятых на каждом этапе.

Таблица 4 – Временные показатели проведения научного исследования

Этап	**Исполнители**	**Продолжительность работ, дни**			**Длительность работ, чел/дн.**			
					$T_{РД}$		$T_{КД}$	
		t_{min}	t_{max}	$t_{ож}$	**НР**	**С**	**НР**	**С**
1. Выбор и утверждение задания и темы работы	Студент, Научный руководитель	2	5	3	3,24	1,08	3,9	1,3
2. Подбор и изучение материалов по данной теме, изучение предметной области.	Студент, Научный руководитель	3	6	5	1,8	4,2	2,17	5,1
3. Календарное планирование работ по теме	Студент, Научный руководитель	4	7	6	5,76	1,44	6,9	1,7
4. Исследование существующих систем эмуляции сетевого оборудования	Студент, Научный руководитель	5	7	7	2,52	5,88	3,04	7,09
5. Описание концепций вычислительных сетей	Студент	10	17	16	0	19,2	0	23,14
6. Разработка моделей вычислительных сетей	Студент	15	20	17	0	20,4	0	24,28
7. Проведение исследований эффективности	Студент, Научный руководитель	12	17	14	5,04	11,76	6,07	14,17
8. Оценка эффективности полученных результатов	Студент, Научный руководитель	4	7	4	2,4	2,4	2,89	2,89
9. Оформление расчётно-пояснительной записки по ВКР	Студент	10	15	12	0	14,4	0	13,73
Итого:		**65**	**101**	**84**	**20,76**	**80,76**	**25,02**	**97,32**

4.4 Разработка графика проведения научного исследования

Для наглядного отображения графика и распределения работ между участниками проекта использована диаграмма Ганта. Диаграмма Ганта представляет собой ленточный график, на котором работы по теме представляются протяженными во времени отрезками, характеризующиеся датами начала и окончания выполнения того или иного этапа работ.

Календарный план-график проведения работ представлен в таблице 5.

Таблица 5 – Календарный план-график проведения работ

№ раб	Вид работ	$T_{кд}$ НР	$T_{кд}$ С	Продолжительность выполнения работ													
				Февраль		Март			Апрель			Май			Июнь		
				2	3	1	2	3	1	2	3	1	2	3	1	2	3
1	Выбор и утверждение задания и темы работы	3,9	1,3														
2	Подбор и изучение материалов по данной теме, изучение предметной области.	2,17	5,1														
3	Календарное планирование работ по теме	6,9	1,7														
4	Исследование существующих систем эмуляции сетевого оборудования	3,04	7,09														
5	Описание концепций вычислительных сетей	0	23,14														
6	Разработка моделей вычислительных сетей	0	24,28														
7	Проведение исследований эффективности	6,07	14,17														
8	Оценка эффективности полученных результатов	2,89	2,89														
9	Оформление расчётно-пояснительной записки по ВКР	0	13,73														

Примечание к таблице 5: - Научный руководитель

- Студент

4.5 Бюджет научно-технического исследования

В состав бюджета выполнения работ по научно-технической работе включает вся себя стоимость всех расходов, необходимых для их выполнения. При формировании бюджета используется группировка затрат по следующим статьям:

- материалы и покупные изделия;
- заработная плата;
- социальный налог;
- расходы на электроэнергию (без освещения);
- амортизационные отчисления;
- оплата услуг связи;
- прочие (накладные расходы) расходы.

4.5.1 Расчет материальных затрат

Так как все работы выполнялись преимущественно на компьютерном оборудовании, то они не потребовали затрат на материалы. Но потребовались затраты на канцелярские принадлежности и флэш карту. Все материальные затраты отображены в таблице 6.

Таблица 6 – Материальные затраты

Наименование	**Ед. изм.**	**Количество**	**Цена за ед., руб.**	**Затраты на материалы, ($З_м$), руб.**
Бумага формата А4	Уп.	1	150	150
Чернила	Шт.	1	250	250
Флэш-карта	Шт.	1	500	500
Итого				**900**

Транспортно-заготовительные расходы (ТРЗ) составляют 5% от отпускной цены материалов. Расходы на материалы с учётом ТРЗ:

$$C_{MAT} = 900 \cdot 1{,}05 = 945 \text{ руб.}$$

4.5.2 Расчет заработной платы

Данная статья расходов включает заработную плату научного руководителя и студента, а также премии, входящие в фонд заработной платы. Расчет основной заработной платы выполняется на основе трудоёмкости выполнения каждого этапа и величины месячного оклада исполнителя.

Величина месячного оклада научного руководителя (МОНР) получена из открытых данных, размещенных на официальном сайте Национального исследовательского Томского политехнического университета. Величина месячного оклада инженеров (МОИ) берется как месячный оклад инженера кафедры.

Основной расчет фонда заработной платы выполняется по формуле:

$$\text{ЗП}_{\text{дн}-\text{т}} = \text{МО}/N,$$

где МО – месячный оклад, руб.;

N – количество рабочих дней в месяц, при шестидневной рабочей неделе – $N = 24{,}91$, а при пятидневной рабочей неделе – $N = 20{,}58$.

Среднедневная заработная плата научного руководителя равна:

$$\text{ЗП}_{\text{дн}-\text{т}} = \frac{26\,300}{24{,}91} = 1\,055{,}8 \ \frac{\text{руб.}}{\text{раб. день}}.$$

Для расчёта среднедневной заработной платы студента, возьмем базовый оклад инженера. А среднедневная тарифная заработная плата инженеров равна

$$\text{ЗП}_{\text{дн}-\text{т}} = \frac{9800}{20{,}58} = 476{,}19 \ \frac{\text{руб.}}{\text{раб. день}}.$$

Затраты времени по каждому исполнителю в рабочих днях взяты из таблицы 5. Для перехода от тарифной суммы заработка исполнителя, связанной с участием в проекте, к соответствующему полному заработку необходимо будет тарифную сумму заработка исполнителя, связанной с участием в проекте умножить на интегральный коэффициент. Интегральный коэффициент находится по формуле:

$$К_{и} = К_{пр} \cdot К_{доп.ЗП} \cdot К_{р},$$

где $К_{пр}$ – коэффициент премий, $К_{пр}$ = 1,1;

$К_{доп.ЗП}$ – коэффициент дополнительной зарплаты, при шестидневной рабочей неделе $К_{доп.ЗП}$ = 1,188, а при пятидневной рабочей неделе $К_{доп.ЗП}$ = 1,113;

$К_{р}$ – коэффициент районной надбавки, $К_{р}$ = 1,3.

Результаты вычислений представлены в таблице 7.

Таблица 7 - Основная заработная плата исполнителей системы

Исполнитель	**Оклад, руб./мес**	$ЗП_{дн-т}$, **руб./раб.день**	**Затраты времени, раб.дни**	**Коэффициент**	**Фонд з/платы, руб.**
НР	26300	1055,8	21	1,699	37669,89
С	9800	476,19	81	1,59	61328,57
Итого:					98998,46

4.5.3 Расчет затрат на социальные нужды

Взнос в социальные фонды установлен в размере 30,2% от заработной платы. Размер взноса рассчитываются по формуле:

$$С_{соц} = С_{ЗП} \cdot 0{,}302,$$

где $С_{ЗП}$ – размер заработной платы.

Подставив необходимые значения в формулу и получим:

$$С_{соц} = 98998{,}46 \cdot 0{,}302 = 29897{,}53 \text{ руб.}$$

4.5.4 Расчет затрат на электроэнергию

Затраты на электроэнергию рассчитываются по формуле:

$$С_{эл.об.} = Р_{об} \cdot t_{об} \cdot Ц_{э},$$

где $Р_{об}$ – мощность, потребляемая оборудованием, кВт;

$t_{об}$ –время работы оборудования, час;

$Ц_{э}$ – тариф на 1 кВт·час. Для ТПУ, $Ц_{э} = 5{,}8$ руб./кВт · час.

Время работы оборудования вычисляется на основе итоговых данных таблицы 3 для инженера ($Т_{рд}$) из расчета, что продолжительность рабочего дня равна 8 часов.

$$t_{об} = Т_{РД} \cdot K_t,$$

где K_t – коэффициент использования оборудования по времени, $K_t = 0{,}9$.

Мощность, потребляемая оборудованием, определяется по формуле:

$$Р_{об} = Р_{ном} \cdot K_C,$$

где K_C – коэффициент загрузки;

$Р_{ном}$ – номинальная мощность оборудования, кВт. Для технологического оборудования малой мощности $K_С = 1$.

Таблица 8 – Затраты на электроэнергию технологическую

Наименование оборудования	**Время работы оборудования tоб, час**	**Потребляемая мощность Роб, кВт**	**Затраты Эоб, руб.**
Персональный компьютер	791,6	0,09	372,89
Итого:			**372,89**

4.5.5 Расчет амортизационных расходов

Для расчета амортизационных расходов используется формула:

$$С_{АМ} = \frac{Н_А \cdot Ц_{ОБ} \cdot t_{рф} \cdot n}{F_Д},$$

где $Н_А$ – годовая норма амортизации единицы оборудования;

$Ц_{ОБ}$ – балансовая стоимость единицы оборудования с учетов ТЗР, стоимость ПК инженера – 25 000 руб.;

$t_{рф}$ – фактическое время работы оборудования в ходе выполнения проекта, $t_{рф} = 80{,}76 \cdot 8 = 646{,}08$ часов;

n – число задействованных однотипных единиц оборудования;

$F_Д$ – действительный годовой фонд времени работы соответствующего оборудования, $F_Д = 298 * 8 = 2384$ часа.

$Н_А$ определяется по формуле:

$$Н_А = \frac{1}{СА},$$

где СА – срок амортизации, который можно получить из постановления правительства РФ «О классификации основных средств, включенных в амортизационные группы» Для электронно-вычислительной техники СА свыше 2 лет до 3 лет включительно. В данной работе примем СА=2,5 года. Тогда

$$Н_А = \frac{1}{2{,}5} = 0{,}4.$$

Таким образом,

$$С_{АМ}(ПК) = \frac{0{,}4 \cdot 25\,000 \cdot 646{,}08 \cdot 1}{2384} = 2710{,}07 \text{ руб}$$

Итого начислено амортизации: 2710,07 руб.

4.5.6 Расчет расходов на услуги связи

Расходы на услуги связи определены наличием подключения к сети Интернет на компьютере, использованном в данной работе.

Ежемесячная оплата, согласно тарифу TPUnet, составляет 350 рублей. В соответствии с таблицей 3, трудоемкость выполняемой задачи составляет четыре календарных месяца. Таким образом, сумма расходов на услуги связи составляет 4*350 = 1400 руб. Общая сумма расходов $С_{св} = 1400$

4.5.7 Расчет прочих расходов

Прочие расходы следует принять равными 10% от суммы всех предыдущих расходов. Они находятся по формуле:

$$С_{проч} = (С_{мат} + С_{ЗП} + С_{соц} + С_{эл.об.} + С_{АМ} + С_{св}) \cdot 0{,}1,$$

Где $С_{мат}$ – расходы на материалы, руб.;

$С_{ЗП}$ – основная заработная плата, руб.;

$С_{соц}$ – расходы на единый социальный налог, руб.;

$C_{эл.об.}$ – расходы на электроэнергию, руб.;

$C_{АМ}$ – амортизационные расходы, руб.;

$C_{св}$ – расходы на услуги связи, руб.

Подставив полученные выше результаты, получим:

$C_{проч}$ = (945 + 98998,46 + 29897,53 + 372,89 + 2710,07 + 1400) ·0,1 = 13432,39 руб.

4.5.8 Расчет общей себестоимости разработки

Проведя расчет по всем статьям сметы затрат на разработку, можно определить общую себестоимость проекта.

Таблица 9 – Смета затрат на разработку проекта

Статья затрат	**Условное обозначение**	**Сумма, руб.**
Материалы и покупные изделия	$C_{мат}$	945
Основная заработная плата	$C_{ЗП}$	98998,46
Отчисления в социальные фонды	$C_{соц}$	29897,53
Расходы на электроэнергию	$C_{эл.об.}$.	372,89
Амортизационные отчисления	$C_{АМ}$	2710,07
Расходы на услуги связи	$C_{св}$	1400
Прочие расходы	$C_{проч}$	13432,39
Итого:		**147756,35**

Таким образом, затраты на разработку составили С = 147756,35 руб.

4.6 Оценка экономической эффективности

Выполнение научно-исследовательских работ оценивается уровнями достижения экономического, научного, научно-технического и социального эффектов.

Для итоговой оценки результатов проекта в зависимости от поставленных целей в качестве критерия эффективности принимается один из видов эффекта, а остальные используются в качестве дополнительных характеристик.

На данном этапе внедрение нет возможности оценить экономический эффект в количественных показателях. Так как данная разработка является моделью сложной вычислительной сети для дальнейшей модификации при решении конкретно поставленной модели. Следовательно, в дальнейшем необходимо рассчитывать данный показатель исходя из заявленных параметров и условий. Поэтому в качестве критерия эффективности проекта оценим научно-технический уровень НИР.

4.6.1 Оценка научно-технического уровня НИР

Научно-технический уровень характеризует влияние проекта на уровень и динамику обеспечения научно-технического прогресса в данной области. Для оценки научной ценности, технической значимости и эффективности, планируемых и выполняемых НИР, используется метод балльных оценок. Каждому фактору по принятой шкале присваивается определенное количество баллов. Обобщенная оценка проводится по сумме баллов по всем показателям. На её основе делается вывод о целесообразности НИР.

Интегральный показатель научно технического уровня НИР определяется по формуле:

$$I_{\text{НТУ}} = \sum_{i=1}^{3} R_i \cdot n_i,$$

где $I_{\text{НТУ}}$ – интегральный индекс научно-технического уровня;

R_i – весовой коэффициент *i*-го признака научно-технического эффекта;

n_i – количественная оценка *i*-го признака научно-технического эффекта, в баллах.

Весовые коэффициенты признаков НТУ приведены в таблице 10.

Таблица 10 – Весовые коэффициенты признаков НТУ

Признаки научно-технического эффекта НИР	**Характеристика признака НИР**	R_i
Уровень новизны	Систематизируются и обобщаются сведения, определяются пути дальнейших исследований	0,40
Теоретический уровень	Разработка способа (алгоритма)	0,10
Возможность реализации	Время реализации в течение первых лет	0,50

Баллы для оценок уровня новизны, теоретического уровня и возможности реализации приведены в таблицах 11 – 13.

Таблица 11 – Баллы для оценки уровня новизны

Уровень новизны	**Характеристика уровня новизны**	**Баллы**
Принципиально новая	Новое направление в науке и технике, новые факты и закономерности, новая теория, вещество, способ	8–10
Новая	По-новому объясняются те же факты, закономерности, новые понятия дополняют ранее полученные результаты	5–7
Относительно новая	Систематизируются, обобщаются имеющиеся сведения, новые связи между известными	2–4
Не обладает новизной	Результат, который ранее был известен	0

Таблица 12 – Баллы значимости теоретических уровней

Теоретический уровень полученных результатов	**Баллы**
Установка закона, разработка новой теории	10
Глубокая разработка проблемы, многоспектральный анализ взаимодействия между факторами с наличием объяснений	8
Разработка способа (алгоритм, программа)	6
Элементарный анализ связей между фактами (наличие гипотезы, объяснения версии, практических рекомендаций)	2
Описание отдельных элементарных факторов, изложение наблюдений, опыта, результатов измерений	0,5

Таблица 13 – Возможность реализации результатов по времени

Время реализации	**Баллы**
В течение первых лет	10
От 5 до 10 лет	4
Свыше 10 лет	2

В таблице 14 указано соответствие качественных уровней НИР значениям показателя.

Таблица 14 – Оценка научно-технического уровня НИР

Фактор НТУ	**Значимость**	**Уровень фактора**	**Выбранный балл**	**Обоснование выбранного балла**
Уровень новизны	0,4	Новая	5	Облегчит разработку других моделей
Теоретический уровень	0,1	Разработка способа	6	Описание принципа работы вычислительных сетей
Возможность реализации	0,5	В течение первых лет	10	Быстрая разработка с помощью различных инструментальных средств

Интегральный показатель научно-технического уровня составляет:

$$I_{НТУ} = 0{,}4 \cdot 5 + 0{,}1 \cdot 6 + 0{,}5 \cdot 10 = 7.6 .$$

Таблица 15 – Оценка уровня научно-технического эффекта

Уровень НТЭ	**Показатель НТЭ**
Низкий	1–4
Средний	4–7
Высокий	8–10

Таким образом, согласно таблице 15, научно-исследовательская работа, на тему «Разработка моделей вычислительных сетей на основе платформы UnetLab» имеет средний уровень научно-технического эффекта.

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
8ИМ5А	Окуневу Дмитрий Александровичу

Институт	Кибернетики	Кафедра	ИСТ
Уровень образования	магистратура	Направление/специальность	Информационные системы и технологии

Исходные данные к разделу «Социальная ответственность»:	
Характеристика объекта исследования (вещество, материал, прибор, алгоритм, методика, рабочая зона) и области его применения.	*Разработка моделей сложных вычислительных сетей на основе современной онлайн-платформе UnetLab. Разработанные модели отображают путь становления компании от небольшого офиса до крупной компании, имеющей территориально отдаленные филиалы, нуждающейся в высоких вычислительных ресурсах и их защите.*
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Производственная безопасность *1.1. Анализ вредных факторов, которые могут возникнуть на рабочем месте при проведении исследований.* *1.2. Анализ опасных факторов, которые могут возникнуть на рабочем месте при проведении исследований.*	*1.1. Вредные факторы, которые могут возникнуть на рабочем месте при проведении исследований:* *−микроклимат;* *−шум;* *−электромагнитные поля;* *−освещение;* *−поражение электрическим током.* *1.2. Опасные факторы, которые могут возникнуть на рабочем месте при проведении исследований:* *−опасность пожара;* *−поражение электрическим током;* *1.3. Обоснование мероприятий по защите исследователя от действия опасных и вредных факторов.*
2. Экологическая безопасность: *2.1. Анализ влияния объекта исследования на окружающую среду.*	*2.1 Влияние объекта исследования на литосферу:* *-вопросы утилизации техники;* *-вопросы утилизации отходов;* *2.2 Проводимые мероприятия по защите окружающей среды.*
3. Безопасность в чрезвычайных ситуациях: – *перечень возможных ЧС при разработке и эксплуатации проектируемого решения;* – *выбор наиболее типичной ЧС;* – *разработка превентивных мер по предупреждению ЧС;*	*3.1 Анализ возможных чрезвычайных ситуаций, которые могут возникнуть на рабочем месте инженера:* *- пожар;* *-поражение электрическим током;*

разработка действий в результате возникшей ЧС и мер по ликвидации её последствий.	*3.2 Мероприятия по предотвращению наиболее типичных ЧС*
4. Правовые и организационные вопросы обеспечения безопасности: – *специальные (характерные при эксплуатации объекта исследования, проектируемой рабочей зоны) правовые нормы трудового законодательства;* – *организационные мероприятия при компоновке рабочей зоны.*	*4.1 Основные проводимые правовые и организационные мероприятия по обеспечению безопасности инженера в учебных аудиториях.* *4.2 Влияние реализации разрабатываемой системы на конечных пользователей.*

Дата выдачи задания для раздела по линейному графику	1.05.2017

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ассистент каф. ЭБЖ	Акулов П.А	-		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ИМ5А	Окунев Дмитрий Александрович		

5 Социальная ответственность

Раздел социальной ответственности предназначен для освещения вопросов, касающихся охраны труда, окружающей среды и обеспечения безопасности в чрезвычайных ситуациях. В этом разделе будет произведен анализ вредных и опасных производственных факторов, даны рекомендации по их снижению, а также будут рассмотрены чрезвычайные ситуации характерные для рассматриваемого производственного объекта.

5.1 Описание проводимых работ

В рамка выполнения магистерской диссертации на основе выбранной онлайн-платформы виртуализации UNetLab, были разработаны моделей сложных вычислительных сетей. Разработанные модели отображают путь становления компании от небольшого офиса до крупной компании, имеющей территориально отдаленные филиалы, нуждающейся в высоких вычислительных ресурсах и их защите.

На основе спроектированных моделях были проведены исследования эффективности разработанных вычислительных сетей. Основной целью разрабатываемых моделей было создание единой инфраструктуры для предприятия и его территориально отдаленных филиалов. Были рассмотрены вопросы создания возможности сетевого взаимодействия между вычислительными машинами предприятия, доступа в сеть Интернет, создание защищенных сообщающих тоннелей между филиалами, а также был рассмотрен вопрос создания отказоустойчивости.

Одной из важнейших задач являлась создание защищенного сообщающего тоннеля для коммуникации между филиалами компании. На сегодняшний день, задача информационной безопасности актуальна как никогда. Потеря предприятием конфиденциальной информации может привести к огромным финансовым потеря и даже к краху.

Во время разработки сложных моделей вычислительных сетей выполнялись работы, связанные со сбором и анализом данных, разработкой

концепций, проектированием топологий и моделированием. Данный вид работ непосредственно связан с вычислительной техникой: персональным компьютером, периферическими устройствами, системами ввода и вывода информации. Данное взаимодействие соответственно связывает человека с дополнительным, вредным воздействием целой группы факторов, что существенно снижает производительность его труда. Большую угрозу несет монитор компьютера, так как он является источником электромагнитного поля.

Описанные выше работы проводились в специализированной учебно-научной лаборатории, находящейся на кафедре «Информационных систем м технологий» Института Кибернетики, аудитория 402 десятого учебного корпуса Томского Политехнического Университета.

5.2 Характеристики рабочего места

Научно-исследовательская работа выполнялась в рабочем кабинете, оснащенном персональными электронно-вычислительными машинами (ПЭВМ). В процессе работы на программиста действуют различные опасные и вредные факторы. Задача охраны труда свести действие этих факторов к минимуму и создать оптимальные условия труда. Работа с ЭВМ регламентируется санитарными правила и нормами [19].

Рабочее место находится на четвертом этаже здания и представляет собой комнату длиной – 10 м., шириной – 6 м. и высотой – 3 м. Естественное освещение кабинета осуществляется посредством двух окон размерами 1,7 м. х 1,5 м. Дверь – деревянная, одностворчатая, коричневого цвета. Высота двери – 2 м., ширина - 1 м. Стены комнаты окрашены водоэмульсионной краской бежевого цвета. Потолок подвесной, плиточный. Пол покрыт линолеумом. Площадь кабинета составляет 60 $м^2$, объем – 180 $м^3$.

В данном помещении находится 14 рабочих мест. Во время работы использовалось современное компьютерное оборудование марок Intel, Gigabyte и Logitech, соответствующее международным требованиям безопасности. В качестве мониторов используются широкоформатные жидкокристаллические

мониторы BenQ. Требования, которые определены к минимальной площади и объему на одно рабочее место (4 м^2 на человека) – выполняются [9].

5.3 Техногенная безопасность

Для данной рабочей зоны необходимо проанализировать следующие факторы. К вредным факторам относятся:

- микроклимат;
- шум;
- электромагнитные поля;
- освещение.

К опасным фактором рабочей зоны относятся:

- опасность пожара;
- опасность поражения электрическим током.

Чрезвычайные ситуации характерные для данного объекта:

- пожар.

5.4 Анализ выявленных вредных факторов рабочего помещения

5.4.1 Микроклимат производственного помещения

Микроклимат является важной характеристикой производственных помещений. В организме человека происходит непрерывное выделение тепла. Одновременно с процессами выделения тепла происходит непрерывная теплоотдача в окружающую среду. Равновесие между выделением тепла и теплоотдачей регулируется процессами терморегуляции, т.е. способностью организма поддерживать постоянство теплообмена с сохранением постоянной температуры тела. Отдача тепла происходит различными видами: излучением, конвекцией, испарение влаги.

Нарушение теплового баланса в условиях высокой температуры может привести к перегреву тела, и как следствие к тепловым ударам с потерей

сознания. В условиях низкой температуры воздуха возможно переохлаждение организма, могут возникнуть простудные болезни, радикулит, бронхит и другие заболевания.

К параметрам микроклимата относятся: температура воздуха, температура поверхностей, относительная влажность воздуха, скорость движения воздуха.

Оптимальные значения этих характеристик зависят от сезона (холодный, тёплый), а также от категории физической тяжести работы. Для инженера-программиста она является лёгкой (1а), так как работа проводится сидя, без систематических физических нагрузок.

Согласно требованиям, оптимальные параметры микроклимата в офисах приведены в таблице 16 [19].

Таблица 16 – Оптимальные значения характеристик микроклимата

Период года	**Температура воздуха, °С**	**Температура поверхностей, °С**	**Относительная влажность, %**	**Скорость движения воздуха, м/с**
Холодный	22-24	21-25	40-60	0,1
Тёплый	23-25	22-26	40-60	0,1

Для создания благоприятных условий труда и повышения производительности, необходимо поддерживать оптимальные параметры микроклимата производственных помещений. Для этого предусмотрены следующие средства: центральное отопление, вентиляция (искусственная и естественная), искусственное кондиционирование.

5.4.2 Производственное освещение

Около 80% общего объема информации человек получает через зрительный канал. Качество поступающей информации во многом зависит от освещения, неудовлетворительное качество которого вызывает утомление организма в целом. При неудовлетворительном освещении снижается

производительность труда и увеличивается количество допускаемых программистом ошибок.

Освещение – получение, распределение и использование световой энергии для обеспечения благоприятных условий видения предметов и объектов [28].

В рабочем помещении сочетаются естественное освещение (через окна) и искусственное освещение (использование ламп при недостатке естественного освещения).

Светильники в помещении располагаются равномерно по площади потолка, тем самым обеспечивая равномерное освещение рабочих мест.

Разряд зрительных работ программиста относится к разряду III подразряду Г (высокой точности), параметры искусственного освещения указаны в таблице 17 [21].

Таблица 17 - Нормативные значения освещённости

Характеристика зрительной работы	Наименьший или эквивалентный размер объекта различения, мм	Разряд зрительной работы	Подразряд зрительной работы	Контраст объекта с фоном	Характеристика фона	Искусственное освещение		
						Освещённость, Лк		
						При комб. освещении		При общ. освещении
						всего	В том числе от общего	
Высокой точности	От 0,3 до 0,5	III	Г	Средний << Большой	Светлый << Средний	400	200	200

Рассчитаем фактическую освещенность рассматриваемой учебной аудитории. Длина и ширина аудитории равны соответственно 10 и 6 м, высота – 3 м. Рассчитаем индекс помещения:

$$i = \frac{S}{h \cdot (A + B)},$$

где:

i – индекс помещения;

S – площадь помещения, м^2;

h – высота помещения, м;

A – длина помещения, м;

B – ширина помещения.

Получили индекс помещения i = 1,25.

Исходя из значения индекса помещения можно определить, что коэффициент использования рассматриваемого светового светильника с люминесцентными лампами равен 38%. Рассчитаем освещенность по формуле, учитывая, что в аудитории 4 светильника по 4 лампы в каждом:

$$E_{факт} = \frac{N \cdot n \cdot \Phi_{ст} \cdot \eta}{S \cdot K_з \cdot Z},$$

где:

N – число светильников в помещении;

n – число ламп в светильнике;

$\Phi_{ст}$ – величина стандартного светового потока, лм;

η – коэффициент использования светового потока;

S – площадь помещения;

$K_з$ – коэффициент запаса;

Z – коэффициент неравномерности освещения.

Зная, что $\Phi_{ст}$ = 1650 лм для люминесцентных ламп дневной цветности (СНиП 23-05-95), $K_з$ для помещений с малым выделением пыли равен 1,5, а Z для люминесцентных ламп равен 1,1, рассчитаем значение фактической освещенности. Оно равно 101 Лк. Данное значение не совпадает с нормативным. Рассчитаем численную оценку разности между фактическим значением освещенности и нормативным.

$$\Delta E = \frac{(E_{факт} - E_{н})}{E_{н}} \cdot 100\%,$$

где:

ΔЕ – показатель разности между фактической освещенностью и нормативной;

$Е_{факт}$ – фактическое значение освещенности;

$Е_{н}$ – нормативное значение освещенности.

Подставив значения в формулу, вычислим ΔЕ = 24%. Таким образом, можно сделать вывод о том, что фактическая освещенность не удовлетворяет нормативным показателям в 200 Лк, поэтому для улучшения освещения аудитории следует добавить еще один светильник с 4 люминесцентными лампами.

5.4.3 Производственные шумы

Одной из важных характеристик производственных помещений является уровень шума.

Шум определяется как звук, оцениваемый негативно и наносящий вред здоровью [28].

Основными источниками шума в помещении являются:

- система охлаждения центральных процессоров;
- жесткие диски;
- шум с улицы.

При выполнении основной работы на ПЭВМ уровень шума на рабочем месте не должен превышать 50 дБ. Допустимые уровни звукового давления в помещениях для персонала, осуществляющего эксплуатацию ЭВМ при разных значениях частот, приведены в таблице 3 [22].

Таблица 18 - Допустимые уровни звука на рабочем месте

Вид трудовой деятельности, рабочее место	Уровни звукового давления, дБ, в октавных полосах со среднегеометрическими частотами, Гц									Уровни звука и эквивалентного звука (в дБА)
	31,5	63	125	250	500	1000	2000	4000	8000	
Конструкторские бюро, программисты, лаборатории	86	71	61	54	49	45	42	40	38	50

Для снижения уровня шума, производимого персональными компьютерами, рекомендуется регулярно проводить их техническое обслуживание: чистка от пыли, замена смазывающих веществ; также применяются звукопоглощающие материалы.

5.4.4 Электромагнитное излучение

Воздействие электромагнитного излучения на человека зависит от напряженностей электрического и магнитного полей, потока энергии, частоты колебаний, размера облучаемого тела [28].

Нарушения в организме человека при воздействии электромагнитных полей незначительных напряженностей носят необратимый характер. При воздействии полей, имеющих напряженность выше предельно допустимого уровня, развиваются нарушения со стороны нервной, сердечно-сосудистых систем, органов пищеварения и некоторых биологических показателей крови.

Работа проводилась на современном компьютере, где значения электромагнитного излучения малы и отвечают требованиям, которые приведены в таблице 19 [23].

Таблица 19 - Допустимые уровни электромагнитных полей

Наименование параметров	Допустимые значения
Напряженность электромагнитного поля на расстоянии 50 см. вокруг ВДТ по электрической составляющей должна быть не более: • в диапазоне частот 5 Гц – 2 кГц • в диапазоне частот 2 – 400 кГц	 25 В/м 2.5 В/м
Плотность магнитного потока должна быть не более: • в диапазоне частот 5 Гц – 2 кГц • в диапазоне частот 2 – 400 кГц	 250 нТл 25 нТл
Напряженность электростатического поля:	20 кВ/м

Основной способ снижения вредного воздействия – это увеличение расстояния от источника (не менее 50 см от пользователя). При работе за компьютером специальные экраны и другие средств индивидуальной защиты применены не были.

5.5 Опасные факторы

5.5.1 Электробезопасность

В связи с наличием электрооборудования для данного производственного объекта характерным является возможность поражения электрическим током. Для снижения данного риска необходимо соблюдать нормы электробезопасности.

Электробезопасность — это система организационных и технических мероприятий и средств, обеспечивающих защиту людей от вредного и опасного для жизни воздействия электрического тока, электрической дуги, электромагнитного поля и статического электричества [24].

Персональный компьютер питается от сети 220В переменного тока с частотой 50Гц. Помещение с ПЭВМ, где проводились описанные выше работы,

относится к помещениям без повышенной опасности, так как отсутствуют следующие факторы:

- сырость;
- токопроводящая пыль;
- токопроводящие полы;
- высокая температура;
- возможность одновременного прикосновения человека к имеющим соединение с землёй металлоконструкциям зданий, технологическим аппаратам и механизмам, и металлическим корпусам электрооборудования.

К мероприятиям по предотвращению возможности поражения электрическим током относятся

- при включенном сетевом напряжении работы на задней панели должны быть запрещены;
- все работы по устранению неисправностей должен производить квалифицированный персонал;
- необходимо постоянно следить за исправностью электропроводки.

5.5.2 Пожарная безопасность

В помещениях с ПЭВМ повышен риск возникновения пожара. Неисправность электрооборудования, освещения, неправильная их эксплуатация, наличие статического электричества неудовлетворительный надзор за пожарными устройствами и производственным оборудованием может послужить причиной пожара. Пожар на предприятии наносит большой материальный ущерб и часто сопровождается несчастными случаями с людьми.

Пожарная безопасность включает в себя комплекс организационных и технических мероприятий, направленных на обеспечение безопасности людей, предотвращения пожара, ограничение его распространения, а также создание условии для успешного тушения пожара [26].

Пожарная опасность персональных электронно-вычислительных машин, обусловлена наличием в применяемом электрооборудовании горючих

изоляционных материалов. Горючими являются изоляция обмоток трансформаторов, различных электромагнитов, проводов и кабелей.

Помещение, где проводились описанные выше работы, по пожарной и взрывной опасности относят к категории Д (пониженная пожароопасность), характеризующейся отсутствием легковоспламеняющихся веществ и материалов в горячем состоянии. Здание десятого корпуса, в котором находится помещение, относится к несгораемым [25].

Для того что бы избежать возникновения пожара необходимо проводить следующие профилактические работы, направленные на устранение возможных источников возникновения пожара:

- периодическая проверка проводки;
- отключение оборудования при покидании рабочего места;
- проведение инструктажа работников о пожаробезопасности.

Для предотвращения пожара помещение с ПЭВМ должно быть оборудовано первичными средствами пожаротушения: углекислотным огнетушителем типа ОУ-2 или ОУ-5. Также помещение должно быть оснащено пожарной сигнализацией. Рекомендуемый тип — система на основе оптических пожарных извещателей ДИП-3СУ и пульта Сигнал-20П SMD.C-2000. Рекомендуется также оборудовать помещение автоматической установкой объемного газового пожаротушения, например, системой азотного пожаротушения «Гарсис».

5.6 Охрана окружающей среды

Под охраной окружающей среды характеризуется различного рода мероприятиями, влияющие на следующие природные зоны:

- атмосфера;
- гидросфера;
- литосфера.

Помещение с персональным компьютером относится к пятому классу, размер санитарно-защитной зоны которого равен 50 метров, так как работа на персональном компьютере не является экологически опасной [27].

5.6.1 Загрязнение атмосферного воздуха

Атмосфера всегда содержит определенное количество примесей, поступающих от естественных и антропогенных источников. К числу примесей, выделяемых естественными источниками, относят: пыль (растительного и вулканического, космического происхождения), туман, дымы, газы от лесных и степных пожаров и др.

Основное антропогенное загрязнение атмосферного воздуха создают ряд отраслей промышленности.

Выполнение магистерской диссертации не осуществляет выбросов вредных веществ в атмосферу. Загрязнение атмосферного воздуха может возникнуть в случае возникновения пожара в помещении, в этом случае дым и газы от пожара будут являться антропогенным загрязнением атмосферного воздуха.

5.6.2 Загрязнение гидросферы

Загрязнение гидросферы огромны и происходят довольно давно. Основными источниками загрязнений являются промышленность и сельское хозяйство. Внутренние водоемы загрязняются сточными водами различных отраслей промышленности.

Сточная вода – это вода, бывшая в бытовом или производственном употреблении, а также прошедшая через какую-либо загрязненную территорию.

В ходе выполнения магистерской диссертации образовывались хозяйственно – бытовые воды.

Бытовые сточные воды помещения образовываются при эксплуатации туалетов, столовой, а также при мытье рук и т.п. Данные воды отправляются на городскую станцию очистки.

5.6.3 Отходы

Основные виды загрязнения литосферы – твердые бытовые и промышленные отходы.

В ходе выполнения магистерской диссертации, образовывались различные твердые отходы. К ним можно отнести: бумагу, лампочки, использованные картриджи, отходы от продуктов питания и личной гигиены, отходы от канцелярских принадлежностей и т.д.

Защита почвенного покрова и недр от твердых отходов реализуется за счет сбора, сортирования и утилизации отходов и их организованного захоронения

5.7 Защита в чрезвычайных ситуациях

Наиболее характерной ЧС для описываемой аудитории является пожар. При невозможности самостоятельно потушить пожар с помощью имеющихся средств (пункт 5.4.2), необходимо предпринять меры по эвакуации из помещения в соответствии с планом эвакуации, которые расположены на каждом этаже десятого учебного корпуса.

После эвакуации необходимо вызвать пожарную команду, после чего поставить в известность о случившемся инженера по техники безопасности.

5.8 Правовые и организационные вопросы обеспечения безопасности Защита в чрезвычайных ситуациях

Работа программиста связана с постоянной работой за компьютером, следовательно, могут возникать проблемы, связанные со зрением, также неправильная рабочая поза может оказывать негативное влияние на здоровье. Таким образом, неправильная организация рабочего места может послужить причиной нарушения здоровья и появлением психологических расстройств.

Согласно СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы»:

- яркость дисплея не должна быть слишком низкой или слишком высокой;
- размеры монитора и символов на дисплее должны быть оптимальными;
- цветовые параметры должны быть отрегулированы таким образом, чтобы не возникало утомления глаз и головной боли.
- опоры для рук не должны мешать работе на клавиатуре;
- верхний край монитора должен находиться на одном уровне с глазом, нижний – примерно на 20° ниже уровня глаза;
- дисплей должен находиться на расстоянии 45-60 см от глаз;
- локтевой сустав при работе с клавиатурой нужно держать под углом 90°;
- каждые 10 минут нужно отводить взгляд от дисплея примерно на 5-10 секунд;
- монитор должен иметь антибликовое покрытие;
- работа за компьютером не должна длиться более 6 часов, при этом необходимо каждые 2 часа делать перерывы по 15-20 минут;
- высота стола и рабочего кресла должны быть комфортными.

Заключение

При выполнении выпускной квалификационной работы была поставлена цель на основе современной онлайн-платформы виртуализации сетевого оборудования UNetLab, разработать модели сложных вычислительных сетей. Выданы задачи произвести анализ существующих систем виртуализации сетевого оборудования, спроектировать концепции сложных вычислительных сетей и разработать их модели. На основе разработанных моделей провести исследования их эффективности.

В результате выполнения выпускной квалификационной работы, поставленная задачи были выполнены, цель достигнута. Был проведен анализ существующих систем эмуляции сетевого оборудования, произведено сравнение этих платформ друг с другом для выявления наилучшей. Исходя из анализа систем, данной платформой стал UNetLab.

На основе выбранной платформы были разработаны модели вычислительных сетей, отображающие развитие предприятия. На каждом этапе развития ставились определенные задачи, решаемые с помощью моделей вычислительных сетей.

На основе построенных моделей, были проведены исследования эффективности работы таких вычислительных сетей. Из полученных результатов исследований эффективности, можно сделать вывод, что разработанные модели являются эффективными и решают поставленные задачи.

В финансовой части работы была проведена оценка потенциальных потребителей результатов исследований, сформирован бюджет затрат.

Также были рассмотрены аспекты, связанные с безопасностью труда на рабочем месте, включая вредные и опасные факторы, режимы работы и защита в чрезвычайных ситуациях.

Список использованных источников

1. Компьютерные сети. Принципы, технологии, протоколы. / В.Г. Олифер, Н.А. Олифе – Учебник. – СПб: Изд-во «Питер», 2016. – 992 с.
2. Локальные сети: архитектура, алгоритмы, проектирование. / Ю.В. Новиков, С.В. Кондратенко – М.: ЭКОМ, 2001. – 312 с.
3. Компьютерные сети. Книга 2: Networking Essentials. Энциклопедия пользователя: пер. с англ. / А. Марк, Д. Спортак и др. – К.: Изд-во «ДиаСофт», 1999. – 468 с.
4. Вычислительные сети и сетевые протоколы / Д. Девис, Д. Барбер, У. Прайс – М.: Мир, 1982. – 562с.
5. Компьютерные сети. Книга 1: High-Performance Networking. Энциклопедия пользователя: пер. с англ. / А. Марк, Д. Спортак и др. – К.: Изд-во «ДиаСофт», 1999. – 432 с.
6. Корпоративные сети связи / Т.И. Иванова. Пособие. – Москва 2001, – 297 с.
7. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-е издание. / А. Мысник – М.: Издательский дом «Вильямс», 2005. – 1168 с.
8. CCNP маршрутизация / Т.Лэммсл, Ш.Одом, К. Уоллес. Изд. «Лори», 2015. – 444 с.
9. Компьютерные сети / Э. Таненбаум – СПБ.: «Питер», 2002. – 248 с.
10. Основы построения виртуальных частных сетей. / С.В. Запечников. – М.: Мир, 2003. – 249 с.
11. Информационная безопасность компьютерных систем и сетей. / В. Шаньгин. – Изд.: Инфра-М, 2011. – 416 с.
12. Использование программных средств эмуляции оборудования в обучении сетевым технологиям / Е.Ф. Попов, А.А. Захаров // Сборник научных трудов по материалам Международной заочной научно-практической конференции «Теоретические и прикладные проблемы науки и образования в 21 веке». Часть 8. – Тамбов, Изд-во ТРОО «Бизнес-Наука-Общество», 2012.
13. Использование программных средств эмуляции оборудования при модификации сетевой инфраструктуры / Е.Ф. Попов// Сборник научных трудов по материалам всероссийскую научно-практической конференции студентов, аспирантов и молодых ученых «Новые технологии – нефтегазовому региону». Тюмень, 2012.
14. Тестирование и применение эмуляторов Cisco для моделирования гетерогенной IPсети / А.М. Горячев // Гагаринские чтения – 2016: XLII Международная молодежная научная коференция: Сборник тезисов докладов Т.ё. Московский авиационный институт (национальный исследовательский университет). – 2016. – стр.277-278

15. UNetLab: List of supported images [Электронный ресурс] / A. Dainese. URL: http://www.unetlab.com/documentation/supported-images/index.html – свободный. – Загл. с экрана. – Яз. Англ. Дата обращения: 16.03.2017 г.
16. Razvan Beuran, Intorduction to network emulation – Taylor & Francis Group, 2012. -389стр.
17. Introduction to Cisco IOS Netflow:A Technical Overview / URL: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html – свободный. – Загл. с экрана. – Яз. Англ. Дата обращения: 16.03.2017 г.
18. CiscoIOSFlexibleNetFlow [Электронныйресурс] / URL: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnf-fnetflow.html – свободный. – Загл. с экрана. – Яз. Англ. Дата обращения: 16.03.2017 г.
19. СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы»
20. СанПиН 2.2.4.548 – 96. «Гигиенические требования к микроклимату производственных помещений»
21. СНиП 23-05-95. «Естественное и искусственное освещение»
22. СН 2.2.4/2.1.8.562-96 «Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории жилой, застройки»
23. СанПиН 2.2.4.1191-03. «Электромагнитные поля в производственных условиях».
24. ГОСТ 12.1.009-76 «Электробезопасность. Термины и определения»
25. НПБ 105-95. «Определение категорий помещений и зданий по взрывопожарной и пожарной опасности»
26. СНиП 21-01-97. «Пожарная безопасность зданий и сооружений».
27. СНиП III-42-80. «Охрана окружающей среды»
28. Безопасность жизнедеятельности: Учебник для вузов / Под ред. К.З. Ушакова. – М.: Изд-во Московского гос. горного университета, 2000.– 430 с.

Приложение А

Раздел 1.3

Choice of network equipment emulator

Студент:

Группа	ФИО	Подпись	Дата
8ИМ5А	Окунев Дмитрий Александрович		

Консультант кафедры ИСТ

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. ИСТ	Мирошниченко Е.А.	к.т.н.		

Консультант – лингвист кафедры ИЯИК

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель каф. ИЯИК	Горбатова Т.Н.	-		

1.3 Choice of network equipment emulator

Let’s consider in detail the most popular emulators, which make it possible to create virtual copies of the Cisco Systems network equipment.

Cisco Packet Tracer

The most popular network equipment emulator is Cisco Packet Tracer, it's an emulator developed by Cisco Systems itself to teach beginners. The Packet Tracer has become very popular due to the need to use it for training within Cisco Network Academy programs. Tens of thousands of beginners are trained annually at Cisco Network Academy [6].

The creation of a network infrastructure and further modification takes place through a graphical interface. It is the most convenient graphical management interface provided by the software of the network equipment emulation. The interface is well adapted for beginners and greatly simplifies the process of creating new network infrastructures or launching and configuring the services necessary for conducting practical classes. An example of the interface is given in figure 1.

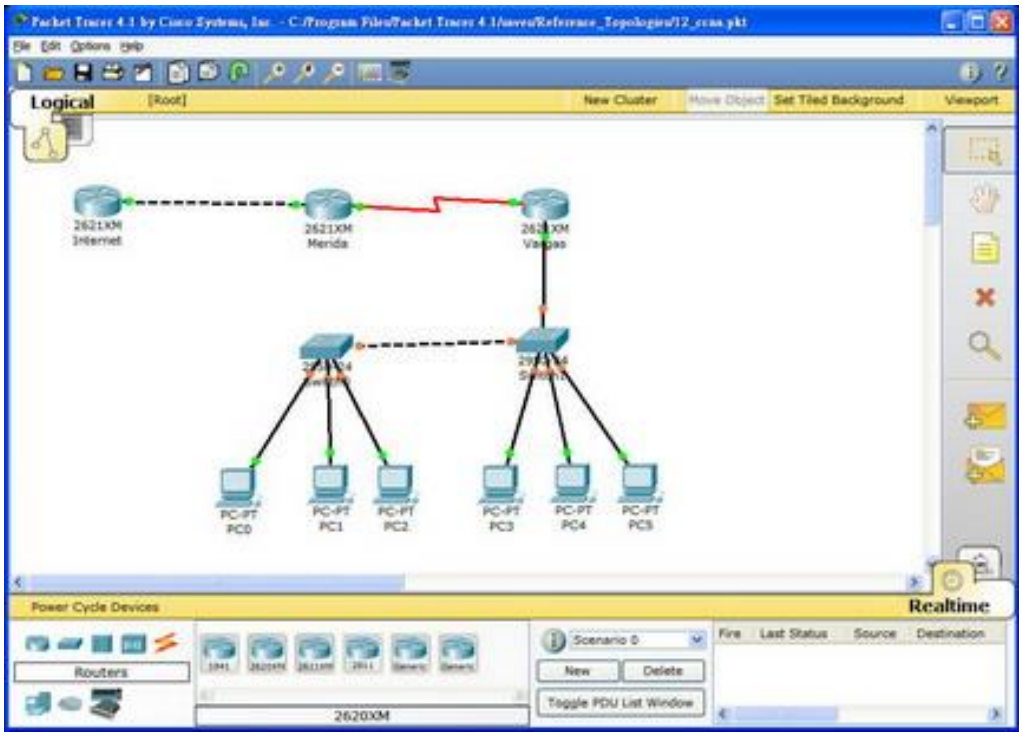

Figure 1 - Graphical interface of the Cisco Packet Tracer emulator

The main purpose of software is to create virtual networks for practical work within preparation for the Cisco Certified Network Associate (CCNA) certification and CCNA Security (Cisco Certified Network Associate Security) exams. In addition to standard routers and switches, Packet Tracer supports emulation of IP phones, wireless access points and servers with a set of standard services [7].

The Packet Tracer includes many tools that simplify the study of the network infrastructure, such as sniffers, which provide detailed information about all the data blocks transmitted to a particular device. Network traffic generators that can artificially create a loading and data flow mapping tools that allow you to trace the route of passage Network by any package or the process of changing the package when passing through various devices.

Packet Tracer is a convenient tool for emulating network equipment, not only for a learner, but also for a teacher. Tools for automatic verification of the task are built-in into the emulator. A teacher can develop a lab for the Packet Tracer. It will check the degree of completion of the task automatically, instead of manual verification on the correct operation of all protocols and the correctness of the entered commands. It is enough to use an automatic check that will determine the percentage of the task completion and the operability of the main services [9].

Cisco Packet Tracer emulates both hardware and software parts of network equipment. But emulated devices do not support a very large number of technologies used in real large networks. Many functions supported in real devices are simply not available.

The main advantage of Cisco Packet Tracer is that this software is free [6,7].

Cisco Packet Tracer is the optimal tool for conducting hands-on training in Cisco basic courses and preparing for examinations at the specialist level. However, to solve complex tasks of modeling computer networks, this software is not suitable, because it is a simulator which does not provide all the capabilities of real equipment, and will not be considered further.

GNS3

GNS3 (Graphical Network Simulator 3) is an independent free software emulator for Cisco devices. GNS3 is available on most Linux, Windows and Mac OS X operating systems, while this software emulator makes it possible to emulate the hardware of Cisco routers by downloading and using the real image of the Cisco IOS operating system [8].

GNS3 is a graphical environment that combines a number of different emulation software tools. The example of graphic interface of the emulation environment is given in figure 2, is not adapted for beginners; it is more likely for those who already have experience with emulation tools, network equipment and familiar with the basic principles of the operation of network devices. However, the availability of graphical controls greatly facilitates the process of creating a network infrastructure and makes working with it more convenient.

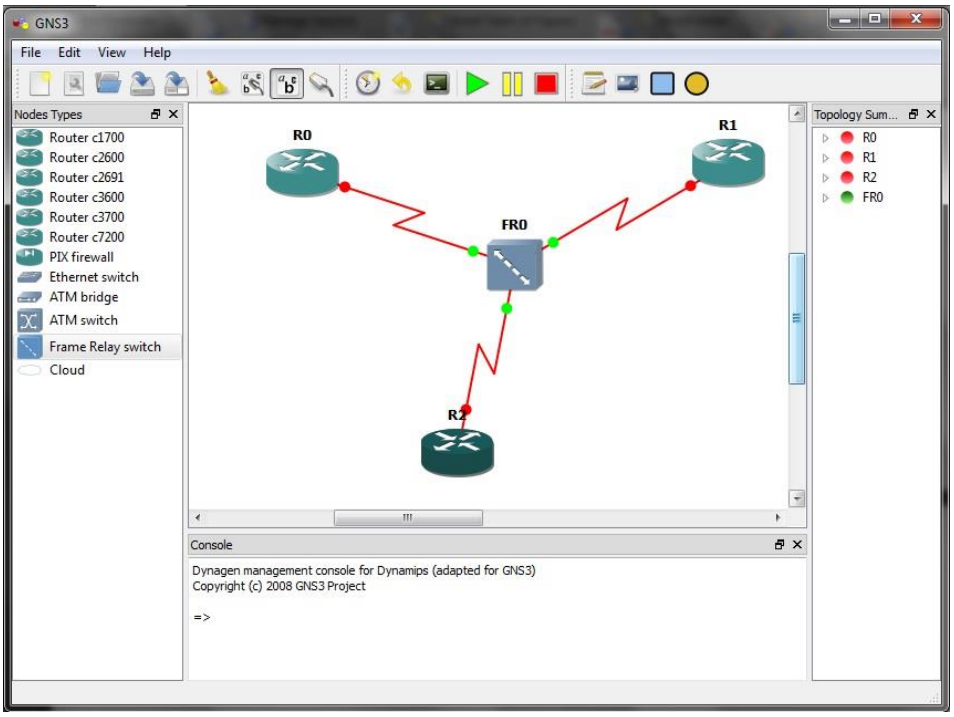

Figure 2 - Graphical interface of the GNS3 emulator

GNS3 includes three separate software emulators. The first one is Dynamips. Many specialists who study network technologies use Dynamips exclusively in the GNS3 environment, since there is no need to work with configuration files and the

command line. The second is Qemu, which allows you to emulate Cisco PIX and ASA firewalls and Cisco IPS intrusion prevention systems, the availability of supporting for these devices greatly expands the ability of GNS3 to use for training in the areas related to the security of network infrastructures [5].

The third element is VirtualBox, which allows integrating virtual servers or virtual personal computers from emulated devices into the network infrastructure. It will give an opportunity to recreate the real information infrastructure, and thus study a large number of technologies.

GNS3 is a very resource-demanding emulation system. Since several independent emulation systems run simultaneously, and above them, a monitoring environment that provides a graphical interface that constantly displays changes in the state of the infrastructure, serious computing power is required. Although GNS3 gives the functionality to create a fairly accurate copy of real information infrastructures with their network, server equipment and end-user computers, the computing power of a personal computer is enough to emulate only a very small information infrastructure. As a result, practical exercises on GNS3 can be conducted on artificially created segments of the network, but not on copies of real infrastructures [6, 8].

UNetLab

Unified Networking Lab (UNetLab, UNL) is multi-user platform for modeling and creating virtual networks, various laboratories, supporting an impressive list of telecommunications equipment. Thus, the conceptual novelty of the product UNetLab is the ability to run and use the program between different platforms and different device manufacturers. An example of a graphical interface is given in figure 3.

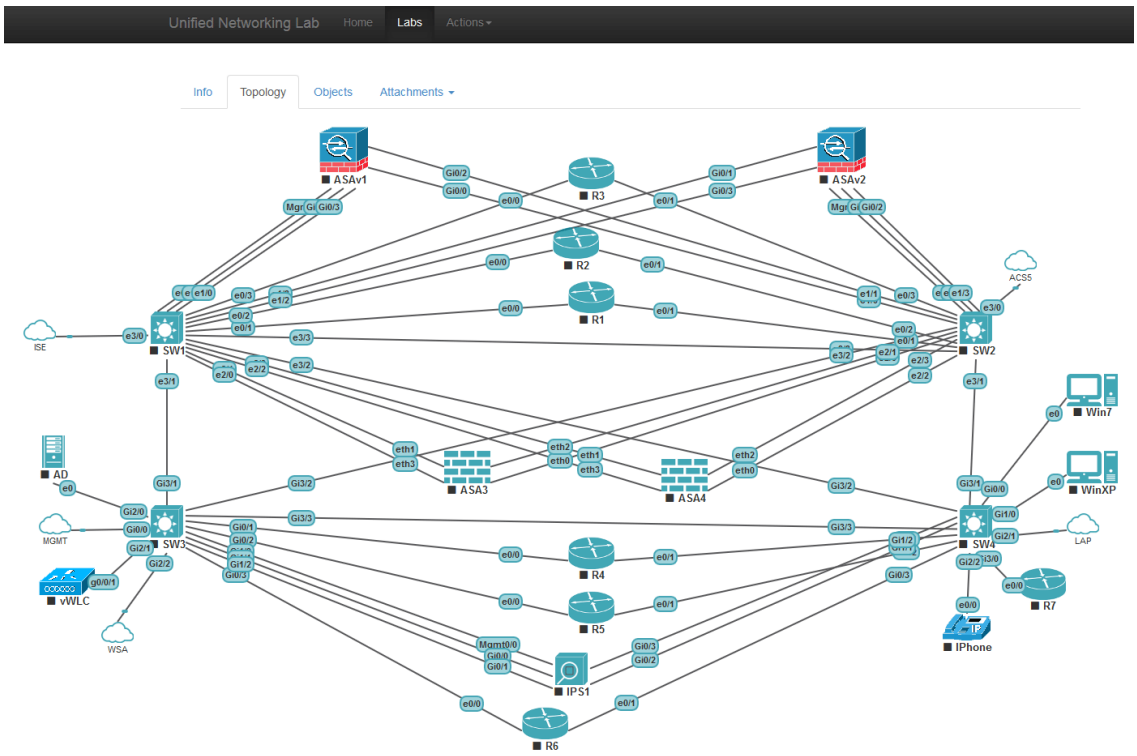

Figure 3 - The GUI of the UNL emulator

Currently, the UNetLab emulator is not only a platform for modeling virtual networks, but also a tool for preparing for various Cisco certifications (for CCNA / CCNP novices and CCIE Routing and Switching professionals, CCIE Security, etc.). In addition, UNL is used in network engineering, and for a systematic approach in identifying and eliminating the causes of network troubleshooting [8]. The UNetLab project started in March 2014, but in such a short time, it became a serious competitor for such famous emulators as GNS3 and Cisco Packet Tracer, having a number of huge advantages. At the same time, product development is carried out up to now, errors are detected and various updates are being released to expand the program functionality and the list of supported devices [7].

Using this approach allows UNL to deviate from the concept of using stand-alone virtual machines to emulate the appropriate network devices and create digital network laboratories based on IOU / IOL, Dynamips and QEMU software emulators, integrating all necessary program modules and scripts in one file within one platform.

The advantage of the UNetLab emulator is that it is completely free, and therefore can be used not only for commercial purposes, but also for training by ordinary users.

The next merit is the ability to run an unlimited number of instances of equipment (routers, switches, security devices, etc.), the amount is limited only by the hardware capabilities of the workplace.

The equipment support in UNetLab is very wide. UNL provides the ability to run images from VIRL (vIOS-L2 and vIOS-L3), ASA images, Cisco IOL images, Cisco IPS images, XRv images and CSR1000v images, Dynamips images from the GNS emulator, Cisco vWLC images and vWSA images. In addition to the above images, there is an impressive list of equipment from other supported vendors: Aruba ClearPass, Alcatel 7750 SR, Arista vEOS, Brocade Virtual ADX, Citrix Netscaler VPX virtual, Checkpoint Firewall, HP VSR1000, Juniper Olive, Juniper Networks vMX router, Juniper vSRX, S-Terra Firewall, MS Windows, and others [15].

Based on the comparative analysis of the software platforms of the network equipment emulator, UNetLab and GNS3 are the most relevant and effective. It should be noted, that UNetLab has a number of technical advantages in comparison with GNS3. A comparative analysis of the functional characteristics of the UNL and GNS3 network equipment emulator platforms is given in table. 1 [4,6,7].

Table 1 - Comparative analysis of the functional characteristics of platforms

	UNetLab	GNS3
GUI	A convenient single graphical user interface based on WEB technology is automatically installed together with the platform.	The GUI in the form of a specialized platform client is installed by the user on the PC and separately from the platform.
Specialized software	There is no need for individual customers to use the platform.	Requires the installation of a specialized client for the subsequent use of the platform.
Functionality	Full support for channel and network layer emulation (L2 and L3) without restrictions.	Partial support for channel and network layer emulation (L2 and L3).
Multiuser support	Multi-user functionality.	Strictly single-user system.
Limitations of RAM	There are no limitations of RAM for emulating QEMU-devices.	QEMU supports up to 2 GB of RAM.
Number of connections	No restrictions on the number of connections between devices in a virtualization environment QEMU.	Limitations in 16 connections between devices in the framework of virtualization QEMU.
Scalability	Images are started and run within the same virtual machine or physical server.	The need to create separate virtual machines to run images in GNS3.
Native support for graphic symbols	The user interface provides native support for user-defined device graphics.	Support for the organization of own values of devices is partially present.

Based on the analysis of all the software products mentioned above, UNetLab is the favorite one, because of its free distribution, huge functionality, a large number of supported emulated devices, and the convenience of creating test equipment for network equipment. UNetLab will be chosen as a software emulator of network equipment for the development of models of computer networks.