МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное
образовательное учреждение высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук
Кафедра «Электронные вычислительные машины»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой ЭВМ
_____ Д.В. Топольский
«___»_____ 2024 г.

Проектирование информационно-коммуникационной сети Министерства здравоохранения Челябинской области с несколькими территориально распределенными филиалами

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

Руководитель работы,
к.п.н., доцент каф. ЭВМ
_____М.А. Алтухова
«___»_____2024 г.

Автор работы,
студент группы КЭ-405
_____Д.Е. Бикмухаметов
«___»_____2024 г.

Нормоконтролёр,
ст. преп. каф. ЭВМ
_____С.В. Сяськов
«___»_____2024 г.

Челябинск-2024

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное
образовательное учреждение высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра «Электронные вычислительные машины»

УТВЕРЖДАЮ
Заведующий кафедрой ЭВМ
_____ Д.В. Топольский
«___»_____2024 г.

ЗАДАНИЕ

на выпускную квалификационную работу бакалавра

студенту группы КЭ-405
Бикмухаметову Даниле Евгеньевичу
обучающемуся по направлению
09.03.01 «Информатика и вычислительная техника»

1. **Тема работы: «**Проектирование информационно-коммуникационной сети Министерства здравоохранения Челябинской области с несколькими территориально распределенными филиалами» утверждена приказом по университету от «22» апреля 2024 г. №764-13/12

2. **Срок сдачи студентом законченной работы:** 4 июня 2024 г.

3. **Исходные данные к работе.**

3.1 В Министерстве здравоохранения Челябинской области имеется действующая информационно-коммуникационная сеть. Необходимо модернизировать сеть в соответствии с поставленными требованиями.

3.2 Основные требования к информационно-коммуникационной сети:

1) сеть должна быть способной обеспечивать одновременную работу до 250 пользователей;

2) требуется обеспечить высокоскоростной обмен данными между центральным офисом Министерства здравоохранения Челябинской области и его филиалами;

3) необходимо обеспечить бесперебойную связь между всеми филиалами;

4) сеть должна быть отказоустойчивой;

5) требуется организация защищенного обмена данными между филиалами и центральным офисом с использованием современных методов шифрования и аутентификации;

6) необходимо предоставить каждому пользователю доступное сетевое хранилище;

7) требуется наличие сервера виртуализации для работы необходимых сервисов;

8) сеть должна поддерживать IP/SIP телефонию;

9) необходимо обеспечить беспроводной доступ к сети для гостей и сотрудников на территории центрального офиса и филиалов;

10) требуется организация удаленного доступа к информационным ресурсам Министерства здравоохранения Челябинской области для его сотрудников.

4. **Перечень подлежащих разработке вопросов:**

1) анализ существующей информационно-коммуникационной сети Министерства здравоохранения Челябинской области;

2) проектирование модернизированной сети;

3) разработка модели в программном симуляторе;

4) тестирование модели.

5. **Дата выдачи задания:** 1 декабря 2023 г.

Руководитель работы _____/ М.А. Алтухова/

Студент _____/ Д.Е. Бикмухаметов/

КАЛЕНДАРНЫЙ ПЛАН

Этап	Срок сдачи	Подпись руководителя
Анализ существующей информационно-коммуникационной сети Министерства здравоохранения Челябинской области	10.03.2023	
Проектирование модернизированной сети	21.03.2024	
Разработка модели в программном симуляторе	04.04.2024	
Тестирование модели	24.04.2024	
Компоновка текста работы и сдача на нормоконтроль	16.05.2024	
Подготовка презентации и доклада	24.05.2024	

Руководитель работы _____/ М.А. Алтухова/

Студент _____/ Д.Е. Бикмухаметов/

АННОТАЦИЯ

Д.Е. Бикмухаметов. Проектирование информационно-коммуникационной сети Министерства здравоохранения Челябинской области с несколькими территориально распределенными филиалами. – Челябинск: ФГАОУ ВО «ЮУрГУ (НИУ)», ВШ ЭКН; 2024, 46 с. библиогр. список – 17 наим.

В рамках выпускной квалификационной работы проводится анализ информационно-коммуникационной сети Министерства здравоохранения Челябинской области и выявляются основные недостатки ее архитектуры и конфигурации оборудования.

В ходе работы проектируется модернизированная информационно-коммуникационная сеть с учетом выявленных недостатков и установленных требований. Выбирается программный симулятор компьютерных сетей, подходящий для реализации необходимых аспектов модели. Разрабатывается функциональная модель спроектированной сети. Проводится тестирование модели на соответствие требованиям.

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

АТС – автоматическая телефонная станция.

ИКС – информационно коммуникационная сеть.

ПАК - программно-аппаратный комплекс.

СХД – система хранения данных.

DHCP – сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в компьютерных сетях.

DNS – от англ. Domain Name System – система доменных имен.

IP – Интернет-протокол, обеспечивающий передачу данных между узлами сети через произвольное число промежуточных узлов.

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

IVR – от англ. Interactive Voice Response – интерактивное голосовое меню, предназначенное для автоматической обработки входящих вызовов.

L2TP – от англ. Layer 2 Tunneling Protocol – это протокол, позволяющий создавать частные виртуальные сети (VPN) через общественные сети.

MAC – от англ. Media Access Control – контроль доступа к среде.

MAC-адрес – это уникальный идентификатор, который присваивается каждой единице сетевого оборудования.

SIP-телефон — это телефон, который позволяет совершать голосовые телефонные вызовы, применяя технологию Voice Over Internet Protocol (VoIP) – передача голоса через интернет.

VLAN – виртуальная локальная компьютерная сеть. Позволяет объединять устройства в один логический широковещательный домен вне зависимости от их физического расположения.

VPN – от англ. Virtual Private Network – виртуальная частная сеть. Позволяет создавать защищенные соединения между удаленными устройствами и локальной сетью.

ВВЕДЕНИЕ

Актуальность темы обусловлена тем, что влияние информационных технологий на культуру и организацию управления в последние десятилетия стремительно растет. Информационные и коммуникационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка [1].

В России наряду с задачей обеспечения всеобщего доступа к информационным и коммуникационным технологиям актуальной является проблема интенсификации использования самих технологий.

Применение в органах государственной власти Российской Федерации новых технологий, обеспечивающих повышение качества государственного управления, является одной из основных задач применения информационных и коммуникационных технологий для развития системы государственного управления, установленных пунктом 40 Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденной Указом Президента РФ от 09.05.2017 № 203.

Информационные системы как среда реализации информационных технологий эволюционируют вместе с этими технологиями [4]. В связи с чем, действующие информационно-коммуникационные системы требуют изменения и доработки.

Целью данной работы является проектирование корпоративной информационно-коммуникационной системы на примере Министерства здравоохранения Челябинской области, обеспечивающее модернизацию действующей сети, выявление возможных проблем, разработку способов повышения эффективности ее работы.

Объектом исследования является информационно-коммуникационная сеть Министерства здравоохранения Челябинской области.

1. АНАЛИЗ СУЩЕСТВУЮЩЕЙ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СЕТИ МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

1.1. Структура и функции Министерства здравоохранения Челябинской области

Министерство здравоохранения Челябинской области является органом исполнительной власти Челябинской области.

Основной задачей министерства является выработка и реализация государственной политики в сфере здравоохранения Челябинской области, направленной на повышение доступности и качества медицинской и лекарственной помощи для населения на основе единого использования всех источников финансирования [2].

Министерство здравоохранения Челябинской области является юридическим лицом.

Министерство в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, нормативными правовыми актами Президента Российской Федерации, Правительства Российской Федерации и Министерства здравоохранения и социального развития Российской Федерации, Уставом (Основным Законом) Челябинской области, законами и иными нормативными правовыми актами Челябинской области, а также Положением о Министерстве здравоохранения Челябинской области, утвержденным постановлением Губернатора Челябинской области от 27 июля 2004 года № 383.

Штатная численность министерства составляет более 210 единиц.

Министерство возглавляет Министр здравоохранения Челябинской области, Министр имеет первого заместителя и заместителей.

В структуру Министерства здравоохранения Челябинской области входят 15 управлений, 31 отдел, 2 службы.

Министерство территориально расположено по трем разным адресам в г. Челябинск: центральный офис, филиал 1 и филиал 2.

1.2. Анализ существующей сетевой инфраструктуры

Информационно-коммуникационная сеть (ИКС) Министерства здравоохранения Челябинской области предназначена для обеспечения информационного взаимодействия между компьютерами сотрудников организации, серверами, принтерами и другим оборудованием стандарта Ethernet [6]. Также ИКС применяется для подключения к внешним вычислительным сетям, например Интернет. ИКС строится на технологии Ethernet со скоростью 100/1000Мбит/с., что обеспечивает необходимую пропускную способность.

На данный момент информационно-коммуникационная сеть Министерства здравоохранения Челябинской области представляет собой так называемую «Расширенную звезду» [10]. Центральный офис является основным узлом сети, а филиалы подключены к нему через выделенные каналы связи. Топология сети была разработана с учетом территориально распределённой структуры организации, в целях обеспечения связи между центральным офисом и филиалами.

Такая топология сети позволяет минимизировать потенциальные простои и обеспечить бесперебойную работу министерства. В случае отказа одного из узлов сети филиалов, центральный офис продолжит работу. Кроме этого, такую топологию легко масштабировать без существенных изменений в инфраструктуре. Важным преимуществом такой топологии также является то, что управление сетевой инфраструктурой централизировано, что существенно упрощает процесс настройки и обслуживания сети [3].

На рисунке 1 представлена схема ИКС Министерства здравоохранения Челябинской области.

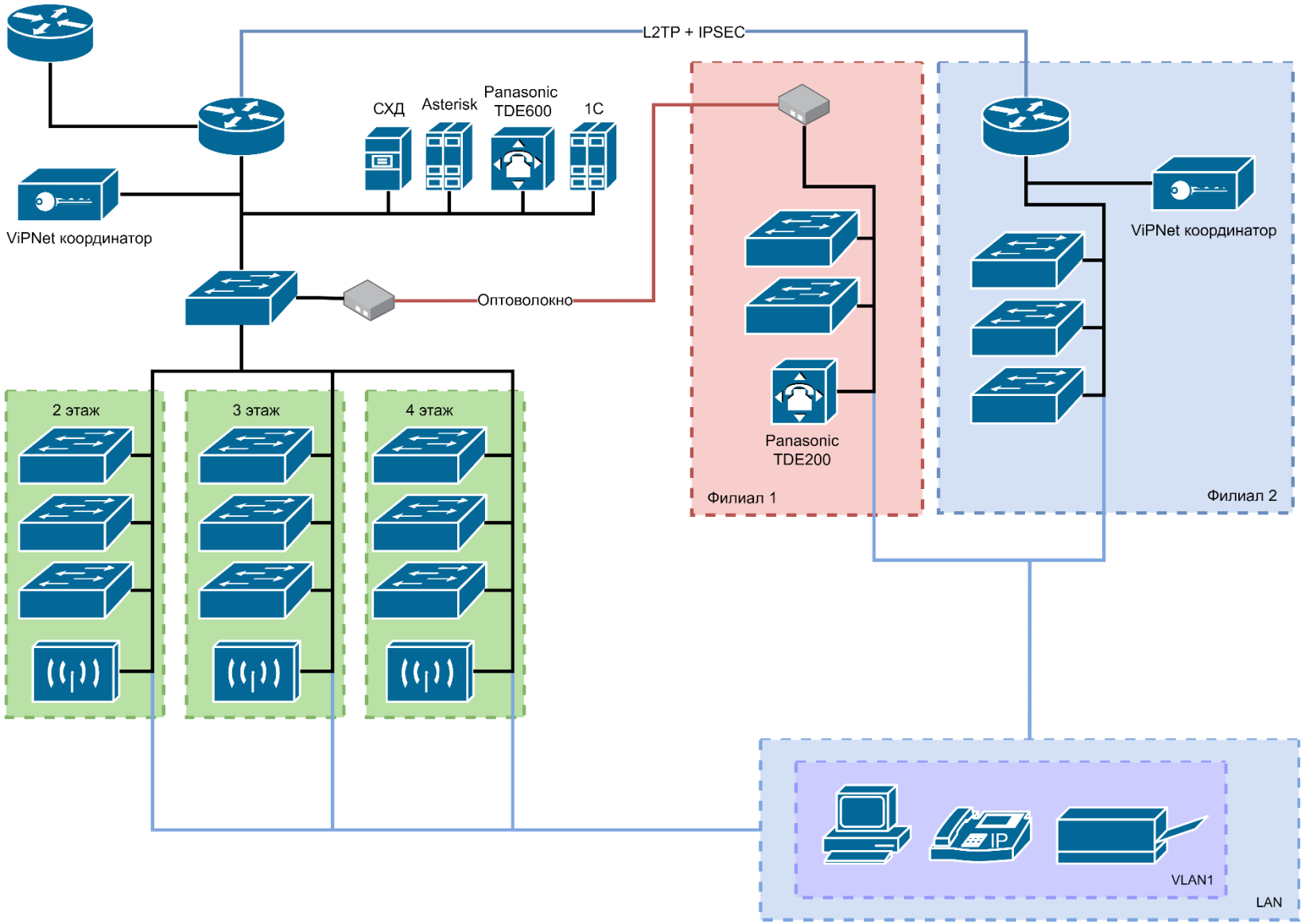

Рисунок 1 – Схема ИКС Министерства здравоохранения Челябинской области

Центральный офис представляет собой трехэтажное здание, обладающее разветвленной и устойчивой сетевой инфраструктурой. Такая инфраструктура необходима для обеспечения работы всем подключенным к сети устройствам. Всего в центральном офисе 150 компьютеров, 150 SIP телефонов и 70 принтеров.

На каждом этаже здания размещены сетевые шкафы, в каждом из которых находятся три коммутатора Eltex MES2428P. Эти коммутаторы имеют по 24 Ethernet порта стандарта 1000BASE-T и пропускную способность до 56 Гбит/с. Они обеспечивают локальную коммутацию трафика. Именно к ним с помощью небольших неуправляемых коммутаторов в кабинетах подключаются компьютеры, телефоны и периферийная техника.

Коммутаторы сетевых шкафов соединены с центральным коммутатором HP Aruba 2530 48 J9781A, который находится в серверной на третьем этаже. Он имеет 48 Ethernet порта стандарта 1000BASE-T и пропускную способность до 96 Гбит/с. Этот коммутатор обеспечивает коммутацию трафика между всеми филиалами.

Центральный коммутатор соединен с корневым маршрутизатором MikroTik CCR1016-12G. Этот промышленный маршрутизатор с 16-ядерным процессором и общей пропускной способностью до 12 Гбит/с является ключевым узлом ИКС министерства и обеспечивает маршрутизацию трафика внутри и между филиалами. Именно благодаря этому маршрутизатору становится возможным централизированное управление конфигурацией ИКС. Кроме того, он обеспечивает ряд дополнительных функций.

Одной из основных задач корневого маршрутизатора является обеспечение доступа в Интернет для сотрудников министерства. Для обеспечения безопасности при выходе в Интернет используются правила брандмауэра, позволяющие тонко настраивать какие именно подключения разрешены и запрещены в сети. Это позволяет защитить сеть от злоумышленников.

Кроме того, маршрутизатор выполняет функцию Network Address Translation, что позволяет преобразовывать локальные IP-адреса устройств в сети для обеспечения межсетевой коммуникации.

На корневом маршрутизаторе функционирует DHCP сервер, который выдает IP-адреса устройствам центрального офиса и первого филиала.

Также, этот маршрутизатор является основным DNS сервером ИКС Министерства здравоохранения Челябинской области.

Интернет центральному офису предоставляется Министерством информационных технологий, связи и цифрового развития Челябинской области. Для этого в серверной был установлен маршрутизатор CISCO, предоставленный провайдером. Этот маршрутизатор соединен с корневым маршрутизатором в сети министерства здравоохранения. Он устанавливает и поддерживает соединение с сетью провайдера и принимает трафик от сотрудников министерства, направленный в интернет.

Основой сетевой структуры в первом филиале являются два неуправляемых коммутатора D-Link DES-1024D. У каждого из них 24 порта стандарта 10/100Base-TX и пропускная способность до 5 Гбит/с. Во втором филиале в общей сложности 30 компьютеров, 30 SIP телефонов и 15 принтеров. Поэтому такой пропускной способности хватает для комфортной одновременной работы всех сотрудников.

Центральный офис соединен с первым филиалом с помощью оптоволоконного канала. Используется одномодовый оптоволоконный кабель. Медиаконвертер, нужный для преобразования сигнала, получаемого по витой паре, в формат, совместимый с оптоволоконным проводом, и обратно, в сервере в центральном офисе подключен в один из портов центрального коммутатора HP Aruba 2530 48. В первом филиале такой же медиаконвертер подключен к одному из коммутаторов D-Link. Такая конфигурация позволяет рассматривать устройства сети, физически находящиеся в первом филиале, как часть локальной сети центрального офиса, что упрощает управление сетью. Соединение по оптоволокну обеспечивает пропускную способность до 1 Гбит/с между филиалами [12].

Второй филиал имеет похожую на центральный офис структуру сети. Этот филиал территориально находится далеко от центрального офиса. Отделам,

расположенным во втором филиале, требуется бесперебойный доступ в Интернет для осуществления своей деятельности. Также, отделы, находящиеся там, должны иметь возможность продолжать работу, даже если произойдет отказ сети в основном офисе. Для обеспечения этих требований во второй филиал компанией-провайдером «Интерсвязь» проведен интернет на скорости 40 Мбит/с. Корневым маршрутизатором в этом филиале также является MikroTik CCR1016-12G. К нему подключены три коммутатора Eltex MES2428P, осуществляющие основную коммутацию трафика в сети. Всего в филиале 70 компьютеров, 70 SIP телефонов, 30 принтеров. На корневом маршрутизаторе этого филиала функционирует свой DHCP-сервер.

Между вторым филиалом и центральным офисом нет прямого физического канала. Связь между филиалами обеспечивается посредством L2TP туннеля.

L2TP (Layer 2 Tunneling Protocol) – это протокол, позволяющий создавать частные виртуальные сети (VPN) через общественные сети, такие как Интернет. Он обеспечивает соединение между двумя конечными точками. С помощью инкапсуляции этот протокол позволяет туннелировать любые данные, независимо от протокола. Для обеспечения безопасности, L2TP используется вместе с протоколом IPsec, который имеет возможности для шифрования трафика. Кроме этого, IPsec также позволяет осуществлять аутентификацию и проверку целостности пакетов [9].

Для того, чтобы создать такой туннель, нужно, чтобы у одной из сторон подключения был статический адрес в общественной сети. Такие адреса называются «белыми» [11]. Для второго филиала у провайдера был приобретен белый IP-адрес в сети Интернет.

В Министерстве здравоохранения Челябинской области L2TP туннель между основным офисом и вторым филиалом настроен с аутентификацией и шифрованием IPsec. Центральный офис является L2TP клиентом и подключается с помощью общего ключа, логина и пароля к L2TP серверу во втором филиале. Настройка клиента и сервера была произведена на маршрутизаторах Miktorik.

Устройства второго филиала доступны как часть локальной сети для основного офиса благодаря L2TP туннелю.

Такое соединение безопасно и обеспечивает достаточную пропускную способность для нужд министерства.

1.3. Анализ конфигурации сетевого оборудования

В данном разделе проводится анализ основных настроек, примененных на оборудовании, использующемся в действующей сети Министерства здравоохранения Челябинской области. Будут рассмотрены такие параметры и настройки, как VLAN, DHCP и брандмауэра. Правильная настройка этих параметров оптимизирует процессы передачи данных, обеспечивает безопасность сети.

1.3.1. VLAN

В действующей информационно-коммуникационной сети Министерства здравоохранения Челябинской области отсутствует разделение на виртуальные локальные сети (VLAN). Все подключенные к сети устройства находятся в одном стандартном VLAN с идентификатором 1.

Такая конфигурация, хоть и позволяет всем устройствам в сети беспрепятственно обмениваться данными, имеет ряд недостатков.

Нахождение всех устройств в одном широковещательном домене существенно повышает риск несанкционированного доступа к важным данным и сетевым ресурсам.

Без разделения на VLAN каждый из узлов сети конкурирует за доступ к сетевым ресурсам, что создает дополнительную нагрузку на сеть. Это приводит к снижению производительности и качества обслуживания для пользователей.

Также, при такой настройке невозможно эффективно контролировать потоки трафика. Это существенно усложняет процесс изменения настроек сетевых устройств и реорганизации сетевой структуры.

Проблемы одного устройства в пределах общего широковещательного домена могут негативно сказаться на работе всей сети, так как отсутствует изоляция сегментов сети.

1.3.2. DHCP

Основной DHCP-сервер сети Министерства здравоохранения Челябинской области расположен на корневом маршрутизаторе в центральном офисе. Он имеет три пула адресов, покрывающие 675 устройств. Этот сервер также раздает адреса устройствам первого филиала.

Во втором филиале есть свой DHCP-сервер на корневом маршрутизаторе. Он имеет один пул адресов, покрывающий 250 устройств.

Так как первый филиал соединен с центральным офисом при помощи арендованного оптического канала, то отказ основного DHCP-сервера или перебой в работе оптического канала, может привести к серьезным проблемам в работе локальной сети первого филиала.

1.3.3. Брандмауэр

Брандмауэр в информационно-коммуникационной сети Министерства здравоохранения настроен на двух маршрутизаторах, непосредственно подключенных к интернету. Это корневые маршрутизаторы в центральном офисе и во втором филиале.

Оба маршрутизатора настроены одинаково. Внутри локальной сети разрешены любые виды соединений. Запрещены New и Invalid соединения из внешней сети, так как эти виды соединений могут быть попытками вторжения. Разрешены Established и Related соединения. Это позволяет обрабатывать

трафик, который является частью уже установленных соединений, или соединений, относящихся к ним. Таким образом, обеспечивается безопасный выход в интернет и беспрепятственный обмен информацией между устройствами локальной сети.

1.4. Средства сетевой защиты

Для обеспечения защищенного обмена данными между центральным офисом и вторым филиалом используется программно-аппаратный комплекс (ПАК) ViPNet Coordinator HW1000. Один такой ПАК установлен в центральном офисе и еще один установлен во втором филиале.

ПАК ViPNet Coordinator HW1000 позволяет создавать защищенные каналы связи и обеспечивать безопасную передачу данных, в том числе и через открытые сети [17]. Достигается это благодаря возможностям шифрования трафика.

Трафик, направленный из центрального офиса во второй филиал, поступает в ПАК ViPNet Coordinator HW1000, шифруется и через PtP туннель направляется в ПАК ViPNet Coordinator HW1000 во втором филиале.

Это позволяет обеспечить безопасность при передаче данных между центральным офисом и вторым филиалом.

Однако, трафик между центральным офисом и первым филиалом передается в незашифрованном виде, так как в первом филиале не установлен ПАК ViPNet Coordinator HW1000. Так как оптический канал между филиалами арендуется у провайдера, отсутствие шифрования трафика создает угрозу безопасности.

1.5. Система хранения данных

Система хранения данных (СХД) —это аппаратно-программное решение с операционной системой, специально предназначенной для хранения

информации [5]. В ИКС Министерства здравоохранения Челябинской области используется СХД файлового типа.

На сервере под управлением Windows Server 2012 развернуто общее файловое хранилище на основе протокола SMB. Размер файлового хранилища – 4 ТБ.

Доступ к различным общим папкам разграничен с помощью локальных учетных записей, созданных на самом сервере. Определенным учетным записям доступны определенные папки. На компьютере пользователя указывается какая именно учетная запись должна быть использована для подключения к файловому серверу.

Также, на сервере для общих ресурсов включена служба теневого копирования, сохраняющая состояние файлов в течение дня, что позволяет минимизировать потерю важных данных.

Такая организация общих файловых ресурсов позволяет каждому сотруднику Министерства здравоохранения Челябинской области безопасно хранить необходимые для работы данные, а также обмениваться ими с другими сотрудниками, не прибегая к использованию сторонних сервисов для обмена файлами.

1.6. Телефония

Правильно организованная работа АТС и IP-телефонии обеспечивает устойчивость коммуникаций и является важным элементом действующей ИКС Министерства здравоохранения Челябинской области.

Аналоговая АТС – аппаратная станция, к которой подключаются внешние линии и абонентские устройства – телефонные аппараты, организована на базе IP-АТС Panasonic KX-TDE600 и KX-TDE200.

Указанные IP-АТС оснащены функциями, которые позволяют обеспечить:

1) сокращение расходов на международную и междугородную связь;

2) поддержку системных IP-телефонов, а также телефонов стандарта SIP;

3) работу с IP-телефонами для связи с сотрудниками, находящимися вне офиса;

4) совместимость с различными интерфейсами, приложениями и сетями;

5) удаленное централизованное администрирование.

IP-телефония, обеспечивающая передачу голоса через Интернет (на основе протокола Voice over IP), организована на базе программной IP АТС «Asterisk».

Asterisk обеспечивает поддержку различных видов оборудования для Voice over IP (VoIP), и соответственно, необходимых VoIP протоколов; обладает всеми возможностями классической АТС, предоставляет функции голосовой почты, конференций, интерактивного голосового меню (IVR), центра обработки вызовов (постановка звонков в очередь и распределение их по агентам используя различные алгоритмы), запись CDR и прочие функции. Преимуществом Asterisk является отсутствие ограничений по количеству функциональных возможностей каналов и абонентов.

Любой IP телефон, подключаемый к ЛВС Министерства здравоохранения Челябинской области, получает необходимые для начальной настройки параметры с помощью особой опции, настроенной на DHCP серверах корневых маршрутизаторов. Опция 66 DHCP отсылает телефоны к программной АТС Asterisk, на которой в определенной директории лежат файлы конфигурации для каждого подключаемого телефона. При первом включении IP телефон получает с помощью этой опции адрес программной АТС, затем подключается к ней и запрашивает файл конфигурации. АТС выбирает какой файл конфигурации. Это позволяет упростить процесс масштабирования телефонной сети.

1.7. Беспроводной доступ

Для обеспечения беспроводного доступа к Интернету и локальной сети на территории центрального офиса Министерства здравоохранения Челябинской области на каждом из трех этажей установлено по одному маршрутизатору MikroTik с WIFI антенной. Отдельно созданы сети для сотрудников и для гостей.

Сеть для сотрудников имеет доступ к локальной сети. Это нужно, например, чтобы пользоваться принтером с ноутбука, не имеющего Ethernet порта. Гостевая же сеть имеет лишь доступ к сети Интернет.

Эти маршрутизаторы настроены одинаково, однако, из-за отсутствия в сети централизированного контроллера точек доступа, каждый из них необходимо настраивать отдельно. Это существенно усложняет процесс конфигурации беспроводного доступа.

1.8. Удаленный доступ

Удаленный доступ к локальной сети Министерства здравоохранения осуществляется с помощью L2TP подключения. Для обеспечения безопасности подключения используется IPSec с общим ключом. Также, каждому сотруднику выдается логин и пароль, без которого подключение невозможно.

IPSec обеспечивает высокий уровень безопасности подключения с помощью технологии шифрования, что минимизирует риск несанкционированного доступа [7].

Такая организация удаленного доступа безопасна и позволяет контролировать возможность доступа сотрудников к локальной сети.

1.9. Серверы

В Министерстве здравоохранения Челябинской области для работы каждого сервиса используется отдельный сервер. Это позволяет изолировать их работу, а также повысить отказоустойчивость сегментов сети. Однако такой подход связан с дополнительными затратами на закупку и поддержку оборудования. Кроме того, каждый сервер необходимо конфигурировать отдельно, что повышает сложность управления сетью, а также создает проблемы при масштабировании и внедрении новых сервисов.

1.10. Вывод

В целом, действующая ИКС Министерства здравоохранения Челябинской области соответствует большинству поставленных требований. Текущая инфраструктура позволяет обеспечить одновременную работу 250 сотрудников. Реализованы различные методы обеспечения бесперебойной связи между филиалами и повышения отказоустойчивости сети. Каждому пользователю предоставлен доступ к сетевому хранилищу. Кроме того, в сети присутствует поддержка IP/SIP телефонии. Также, реализован беспроводной доступ к сетевым ресурсам для гостей и сотрудников на территории филиалов и центрального офиса. Обеспечен удаленный доступ к информационным ресурсам для сотрудников.

Однако, в действующей информационно-коммуникационной сети Министерства здравоохранения Челябинской области отсутствует сервер виртуализации, наличие которого необходимо согласно поставленным требованиям. Внедрение сервера виртуализации позволит оптимизировать использование аппаратного обеспечения, повысит отказоустойчивость и гибкость системы, а также упростит процесс развертывания и управления сервисами.

Также, ИКС не обеспечивает защищенный обмен данных между центральным офисом и первым филиалом. Отсутствие в первом филиале шифрования трафика, идущего через оптический канал в центральный офис, повышает уязвимость сети к атакам. Установка программно-аппаратного комплекса (ПАК) ViPNet Coordinator HW1000 в первом филиале позволит шифровать трафик через оптический канал. Это существенно уменьшит уязвимость сети к атакам и обеспечит безопасность при передаче данных между филиалами.

Кроме того, были выделены другие недостатки нынешней ИКС Министерства здравоохранения Челябинской области.

В отсутствие VLAN весь трафик перемещается в рамках одного широковещательного домена. Неприменение VLAN может приводить к возникновению широковещательных штормов, снижению безопасности сети, повышению сложности управления сетью. К тому же, существенно повышается нагрузка на сетевое оборудование. Интеграция VLAN помогает оптимизировать трафик и улучшить производительность сети, повысить отказоустойчивость.

Отсутствие DHCP-сервера в первом филиале может привести к нарушениям в работе его локальной сети при отказе основного DHCP-сервера или арендованного оптического канала. Распределение функций DHCP между несколькими серверами позволит снизить нагрузку на основной DHCP-сервер и улучшить отзывчивость сети в целом. Кроме того, наличие локального DHCP-сервера позволит управлять и настраивать параметры сети в соответствии с потребностями конкретного филиала, что способствует более гибкому и эффективному управлению сетью в целом.

Необходимо спроектировать модернизированную сеть, которая исправит недостатки действующей сети, а также будет соответствовать всем поставленным требованиям.

2. ПРОЕКТИРОВАНИЕ МОДЕРНИЗИРОВАННОЙ СЕТИ

2.1. Конфигурация VLAN

Виртуальные локальные сети (Virtual Local Area Network) или VLAN представляют собой механизм разделения локальных сетей на логические группы [8]. Эти группы управляются на уровне коммутаторов и маршрутизаторов.

Использование VLAN повышает безопасность и производительность сети, позволяет контролировать потоки трафика.

Создание VLAN возможно на основе физических портов коммутаторов или маршрутизаторов, MAC-адресов устройств и протоколов передачи данных. Взаимодействие подсетей возможно только через маршрутизатор.

В Министерстве здравоохранения Челябинской области активно используется VOIP-телефония по протоколу SIP. Почти у каждого сотрудника есть свой личный рабочий телефон. Трафик протокола SIP является большой частью всего трафика организации.

При этом, телефонам необходимо взаимодействовать только с другими телефонами. Поэтому, в модернизированной сети необходимо выделить VOIP трафик в отдельную логическую группу на основе протокола.

Это позволит отделить телефонную сеть от остальной сети, что повысит производительность и отказоустойчивость сети в целом.

2.2. DHCP-сервер в первом филиале

DHCP (Dynamic Host Configuration Protocol) – сетевой протокол, который позволяет автоматически назначать IP-адреса и другие параметры, такие как шлюз по умолчанию, адрес DNS-сервера и т.д., устройствам в локальной сети. Это позволяет централизованно управлять сетевой конфигурацией и упрощает подключение новых устройств.

Оборудование, установленное в первом филиале, не имеет возможности работать в роли DHCP сервера. Поэтому необходимо внедрить маршрутизатор в сеть первого филиала. В качестве маршрутизатора был выбран MikroTik hAP ax2. Его возможностей хватит для обеспечения стабильной работы сотрудников первого филиала.

При создании DHCP-сервера в первом филиале будет использован один из трех пулов адресов DHCP-сервера в центральном офисе. Остальные два пула останутся для устройств центрального офиса.

Внедрение маршрутизатора с собственным DHCP-сервером в первом филиале позволит разгрузить DHCP-сервер центрального офиса, а также повысит отказоустойчивость сети в целом.

2.3. Шифрование трафика в первом филиале

Для организации защищенного обмена данными между первым филиалом и центральным офисом необходимо обеспечить шифрование трафика, идущего по оптическому каналу между этими двумя филиалами. В центральном офисе уже установлен ПАК ViPNet Coordinator HW1000 с возможностью шифрования трафика. Необходимо внедрить аналогичный ПАК ViPNet Coordinator HW1000 в первом филиале. Это позволит принимать шифровать трафик, отправляемый в центральный офис, а также получать и расшифровывать трафик, приходящий из центрального офиса.

2.4. Сервер виртуализации

Необходимые для работы Министерства здравоохранения Челябинской области сервисы, такие как, например, внутренний мессенджер и базы данных 1С, в действующей сети развернуты на отдельных физически изолированных серверах. Такой подход повышает безопасность и отказоустойчивость, но требует очень много ресурсов для поддержания и создает проблемы при

масштабировании. Поэтому необходимо внедрить в ИКС сервер виртуализации, который позволит централизировано разворачивать сервисы, управлять ими, а также получать информацию об их состоянии. Сервер виртуализации, к тому же, упростит процесс создания резервных копий важных данных сервисов, т.к. все данные будут собраны в одном месте.

В качестве платформы для сервера виртуализации был выбран Proxmox. Proxmox – это открытая бесплатная платформа виртуализации. Она позволяет управлять виртуализированными окружениями и создавать виртуальные машины на одном сервере. В состав платформы также входят инструменты мониторинга, управления ресурсами и резервного копирования. Все это в совокупности делает Proxmox хорошим выбором платформы для сервера виртуализации.

Платформа Proxmox будет установлена на один из использующихся физических серверов. После этого постепенно другие сервисы будут перенесены со своих серверов на виртуальные машины под управлением Proxmox. Постепенный переход позволит обеспечить наименьшие задержки в работе сотрудников.

2.5. Схема модернизированной сети

В результате проектирования модернизированной сети были подобраны новые параметры конфигурации сети, включая создание VLAN для VOIP трафика, внедрение маршрутизатора с DHCP-сервером и ПАК ViPNet Coordinator HW1000 в первом филиале, а также внедрения сервера виртуализации на платформе Proxmox.

Изменения, внесенные в результате проектирования модернизированной сети, соответствуют требованиям, поставленным перед сетью Министерства здравоохранения Челябинской области.

Создание VLAN для VOIP трафика позволит разделить голосовой трафик от остального сетевого трафика, что улучшит качество связи и предотвратит его конфликт с другими данными в сети. Такой шаг соответствует требованию обеспечения высокоскоростной IP/SIP телефонии и требованию об отказоустойчивости сети.

Внедрение маршрутизатора с DHCP-сервером и ПАК ViPNet Coordinator HW1000 в первом филиале позволит повысить отказоустойчивость сети за счет наличия резервного DHCP-сервера и обеспечит защищенный обмен данными между филиалами с помощью ПАК ViPNet Coordinator HW1000.

Внедрение сервера виртуализации на платформе Proxmox позволит снизить затраты на оборудование, упростить управление сетевой инфраструктурой и повысить гибкость системы. Применение виртуализации также соответствует требованию об отказоустойчивости сети.

Таким образом, внесенные изменения в конфигурацию сети соответствуют поставленным требованиям и способствуют улучшению ее производительности, безопасности и управляемости.

На рисунке 2 представлена схема модернизированной ИКС Министерства здравоохранения Челябинской области.

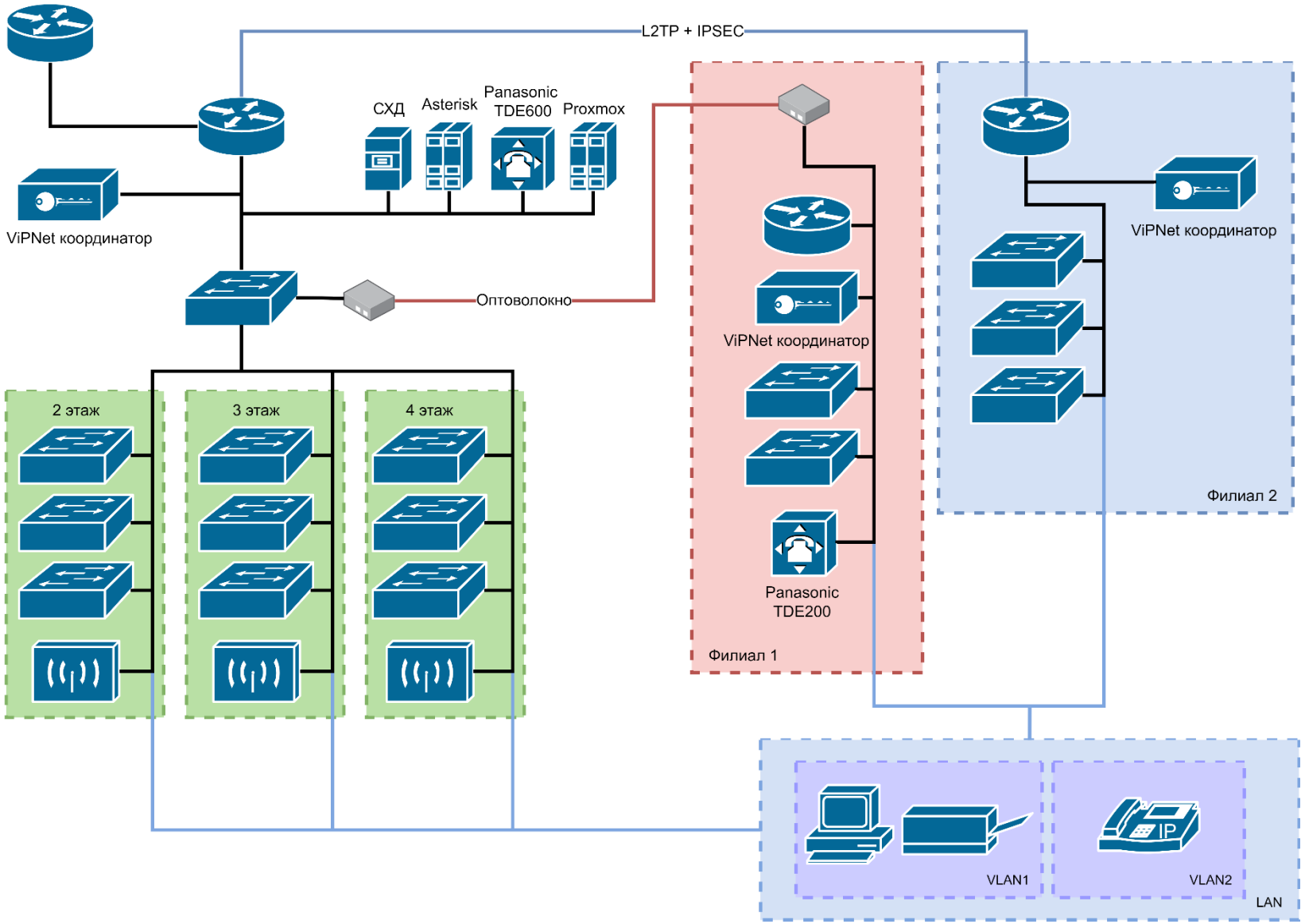

Рисунок 2 – Схема модернизированной ИКС Министерства здравоохранения Челябинской области

3. РАЗРАБОТКА МОДЕЛИ В ПРОГРАММНОМ СИМУЛЯТОРЕ

3.1. Выбор программного симулятора

В процессе проектирования и модернизации компьютерных сетей важное значение имеет выбор программного симулятора, позволяющего создать виртуальную модель ИКС, изучить и оценить в действии результаты оптимизации сети.

В качестве критериев выбора программного симулятора автором использованы функциональные возможности, гибкость и производительность инструментов, применяемых для моделирования и тестирования сетевых топологий. Данные, полученные в ходе изучения программных симуляторов, позволят определить наиболее подходящий инструмент для моделирования модернизированной ИКС.

3.1.1 GNS3

Графический симулятор сети GNS3 позволяет создавать виртуальные сетевые топологии. С его помощью пользователи могут создавать на своем компьютере модели различных устройств – маршрутизаторов, коммутаторов, АТС и других, изучать и тестировать их в виртуальной среде. В связи с чем, платформа GNS3 популярна как среди студентов, так и среди профессиональных сетевых инженеров, используется для получения знаний и практического опыта в области настройки и управления сетями [16].

Возможность работы с реальными образами сетевых устройств обеспечивает высокую степень реализма при моделировании, настройке и управлении сетями, а также исключает риски повреждения реального оборудования, что является существенным преимуществом GNS3, являющимся по сути, эмулятором сети. Виртуализация позволяет снизить затраты на

приобретение и поддержку аппаратного обеспечения, а также эксплуатационные расходы.

GNS3 является бесплатным программным обеспечением с открытым кодом доступа, что позволяет пользователям не только свободно использовать инструмент, но и создавать собственные расширения и модули, тем самым вносить свой вклад в развитие симулятора.

К достоинствам GNS3 относится также способность поддерживать интеграцию с реальным сетевым оборудованием и создавать тем самым гибридные среды тестирования.

В качестве недостатков GNS3 следует отметить требование наличия значительных ресурсов компьютера, в том числе процессора и оперативной памяти, необходимых для запуска крупных сетевых топологий. Данный фактор является ограничивающим доступность платформы для пользователей, имеющих старое оборудование или незначительные ресурсы.

Кроме того, у новичков в сетевых технологиях GNS3 может вызвать сложности в установке и настройке образов устройств, конфигурации сетевых параметров, поскольку требует специализированных знаний для успешного запуска и эффективного использования данной платформы.

При прогнозировании конкретных сценариев использования GNS3 следует учитывать все вышеперечисленные факторы.

3.1.2 Cisco Packet Tracer

Cisco Packet Tracer относится к инструментам моделирования сетей Cisco, специально разработанным для обучения и практических занятий начинающих пользователей по технологии виртуальных сетей [14].

Cisco Packet Tracer отличается достаточно простым и понятным интерфейсом, позволяющим пользователям - начинающим и опытным сетевым специалистам - легко моделировать и преобразовывать сетевые топологии, проводить их тестирования и эксперименты.

Пакет Cisco Packet Tracer ориентирован на сетевое оборудование Cisco и включает в себя широкую линейку сетевых устройств, таких как коммутаторы, маршрутизаторы, межсетевые экраны и т.д., что позволяет пользователям создавать различные сценарии сетевого взаимодействия, выполнять настройку и конфигурацию оборудования указанного производителя.

Симулятор Cisco Packet Tracer предоставляет возможности создавать и изучать различные сетевые протоколы, технологии и сервисы; тестировать настройку VLAN и VPN, протоколов маршрутизации и многое другое. Пользователям доступны также инструменты исследования сети, способные выявить и исправить возможные проблемы сетевой инфраструктуры.

Преимуществом Cisco Packet Tracer является его доступность – симулятор предоставляется бесплатно для студентов, преподавателей и образовательных учреждений, осуществляющих обучение по программам высшего профессионального образования, что дает возможность для изучения сетевых топологий без дополнительных затрат на лицензирование. При этом, следует отметить, исходный код у программы закрытый.

Cisco Packet Tracer, в отличие от реального оборудования, имеет недостатки, связанные с тем, что некоторые продвинутые функции или конфигурации могут быть недоступными или работать некорректно, сужая тем самым возможность реализации определенных сценариев. Кроме этого, затруднения у пользователей в изучении отдельных аспектов сетевой конфигурации могут вызвать ограничения некоторых настроек и параметров Cisco Packet Tracer, по сравнению с реальным оборудованием Cisco.

В версии Cisco Packet Tracer присутствуют не все модели сетевого оборудования, представленных в реальных сетях Cisco, что ограничивает возможности пользователей, нацеленных на практическое изучение определенных типов оборудования и конфигураций

К недостаткам Cisco Packet Tracer также относится ориентация именно на сетевое оборудование Cisco, что исключает возможность для пользователей

изучить с помощью данного симулятора оборудование и стандарты других производителей.

3.1.3 EVE-NG

Программное обеспечение EVE-NG (Emulated Virtual Environment Next Generation) представляет собой набор инструментов для виртуализации сетевых сред, позволяющий создавать сетевые топологии с интеграцией оборудования разных производителей [15].

EVE-NG обладает значительным набором возможностей моделирования сетевых топологий, в том числе, доступом к официальным образам операционных систем ведущих производителей сетевого оборудования, обеспечивающим виртуализацию сетевых топологий с максимальной степенью реалистичности. Это позволяет пользователям практиковаться с различными типами оборудования и операционными системами, тестировать разные конфигурации, исключая риски повреждения реального оборудования.

Особенностью EVE-NG является персонифицированный подход к исследовательской и экспериментальной деятельности, который основан на предоставлении пользователям полного контроля над создаваемой сетевой инфраструктурой, возможности настроек конфигурации устройств и параметров сети.

EVE-NG имеет открытый исходный код и поддержку активного сообщества пользователей, благодаря чему постоянно обновляется, наполняется новыми функциями, в целом развивается и совершенствуется.

Из недостатков отмечается требование EVE-NG значительных ресурсов процессора и оперативной памяти для запуска крупных сетевых топологий, что служит ограничительным фактором доступа к платформе пользователей, имеющих ограниченные ресурсы.

Кроме того, для новичков в сетевых технологиях может вызвать сложности настройка EVE-NG, требующая создания и настройки образов устройств, конфигурации параметров сети.

Отдельные расширенные возможности и функции программного обеспечения EVE-NG доступны только в коммерческих версиях, - на безвозмездной основе предоставлен доступ только к базовой версии, что ограничивает возможность их применения значительному числу пользователей.

Отсутствие необходимой для настройки и использования EVE-NG технической документации и руководства пользователей является серьезным препятствием, особенно при работе с расширенными функциями платформы или сложными сценариями, поскольку затрудняет понимание отдельных аспектов работы и может сказаться на результативности процесса изучения и применения данного симулятора.

3.1.4 UNetLab

Сетевой эмулятор Unified Networking Lab (UNetLab, UNL) представляет собой платформу для моделирования и создания виртуальных сетевых топологий и лабораторий, поддерживающую значительный перечень оборудования различных производителей, в том числе Cisco, Juniper и других, что обеспечивает возможность использования программы между разными платформами и является особенностью данного продукта [13].

Благодаря удобному интерфейсу управления образами устройств на платформе UNetLab значительно упрощена загрузка и настройка необходимого сетевого оборудования, а также управление им.

UNetLab предоставляет возможности для настройки и запуска неограниченного количества видов и типов сетевого оборудования (коммутаторов, роутеров, устройств безопасности и т.д.), что позволяет создавать топологии с учётом конкретных потребностей и сценариев пользователей.

Платформа обладает возможностью наращивания дополнительных ресурсов без ощутимого снижения производительности, что является показателем хорошей масштабируемости и позволяет создавать крупные и сложные сетевые топологии.

UNetLab относится к бесплатным инструментам с открытым исходным кодом доступа, что расширяет круг пользователей, заинтересованных в моделировании виртуальных сетевых лабораторий на базе широкой линейки оборудования от различных вендоров. Вместе с тем, необходимо отметить, что разработка программы была приостановлена, что означает отсутствие обновлений и возможные сложности в поддержке.

Для настройки UNetLab требуется определенный уровень подготовки в области сетевых топологий, что может вызвать сложности для начинающих пользователей.

Ограниченные аппаратные возможности рабочего места пользователя также могут повлиять на предоставляемый платформой доступ к запуску большого количества экземпляров сетевого оборудования.

К минусам платформы относится и недостаток документации, что что может вызвать затруднения в поиске и получение информации, необходимой для работы с UNetLab, а также решение возникающих в ходе работы вопросов.

3.1.5 Сравнение преимуществ и недостатков

В таблице 1 приведено сравнение преимуществ и недостатков рассмотренных программных симуляторов компьютерных сетей.

Таблица 1 – Сравнение преимуществ и недостатков рассмотренных программных симуляторов

Программный симулятор	Цена	Исходный код	Возможность работы с образами реального оборудования	Разработка
GNS3	Бесплатный	Открытый	Есть	Продолжается
Cisco Packet Tracer	Бесплатный для студентов	Закрытый	Нет	Продолжается
EVE-NG	Ограниченная бесплатная версия	Открытый	Есть	Продолжается
UNetLab	Бесплатный	Открытый	Есть	Прекращена

После тщательного изучения различных программных симуляторов компьютерных сетей и анализа их преимуществ и недостатков, был сделан выбор в пользу программы GNS3. В ИКС Министерства здравоохранения Челябинской области используется оборудование разных производителей. Поэтому, необходимо, чтобы программный симулятор поддерживал работу с реальными образами оборудования. Также GNS3 полностью бесплатна и имеет открытый исходный код, активную поддержку и полную документацию.

3.2. Реализация основных элементов сети

3.2.1 Маршрутизаторы

В ИКС Министерства здравоохранения Челябинской области используются только маршрутизаторы производителя MikroTik. Все маршрутизаторы указанной компании используют одну и ту же операционную систему RouterOS. Компания-производитель предоставляет версию образа

операционной системы, известную как CHR (Cloud Hosted Router), специально для использования в виртуальных машинах.

В симуляторе GNS3 были созданы виртуальные маршрутизаторы на основе этого образа с необходимым количеством портов Ethernet. Затем в виртуальные маршрутизаторы были загружены резервные копии конфигураций маршрутизаторов, использующихся в Министерстве здравоохранения Челябинской области. Для корректной работы были изменены параметры IP-адресации в соответствии с новым окружением и особенностями программы. Также были внесены изменения в настройки VLAN для поддержки отдельной подсети для VOIP трафика.

В конфигурацию DHCP-сервера виртуальных маршрутизаторов центрального офиса и первого филиала были внесены поправки таким образом, чтобы разделить DHCP-сервера работу корневого маршрутизатора центрального офиса между двумя этими маршрутизаторами. Один пул адресов был удален из виртуального маршрутизатора центрального офиса и добавлен в созданный в виртуальном маршрутизаторе первого филиала DHCP-сервер.

Теперь виртуальные маршрутизаторы MikroTik полностью функционируют в среде GNS3, что позволяет тестировать и отлаживать различные сетевые конфигурации.

3.2.2. Коммутаторы

Производители коммутаторов, используемых в действующей сети, не предоставляют образы операционных систем своего оборудования. Поэтому для создания виртуальных коммутаторов был использован образ Open vSwitch. Open vSwitch – это гибкий в настройке коммутатор с открытым исходным кодом, поддерживающий все присутствующие в задействованном в Министерстве здравоохранения Челябинской области оборудовании.

Для каждого виртуального коммутатора была проведена ручная настройка с переносом всех необходимых для обеспечения полного соответствия реальному

оборудованию параметров и конфигураций. Это включало в себя настройку портов, VLAN и других параметров.

Далее для этих коммутаторов была добавлена конфигурация для создания отдельного VLAN для VOIP трафика. Настройка была проведена в соответствии с настройкой виртуальных маршрутизаторов для обеспечения совместной работы виртуального оборудования.

3.2.3. Серверы

Чтобы воссоздать в GNS3 программную АТС Asterisk, использующуюся в Министерстве здравоохранения Челябинской области, была использована виртуальная машина с операционной системой Debian 7.11 Wheezy. Было установлено программное обеспечение Asterisk 14.3. Также, был осуществлен перенос и адаптация конфигурации с физического сервера Asterisk в действующей ИКС. Виртуальная машина была интегрирована в новое окружение и подготовлена к работе с другими устройствами в модели.

Для реализации виртуальной СХД был использован образ системы Windows Server 2012. Были проведены необходимые настройки, в том числе выбор ролей и функций, таких как служба файлов и папок. Основные настройки политик безопасности и прав доступа к папкам были перенесены с физической СХД.

Платформа виртуализации Proxmox была установлена на виртуальную машину в GNS3. Была произведена конфигурация основных сетевых интерфейсов для обеспечения возможности работы с другими устройствами в модели. Для проверки возможностей виртуализации платформы в Proxmox была создана виртуальная машина под управлением Ubuntu Server 18.04. Для нее также была проведена конфигурация сетевых интерфейсов для работы с другими устройствами модели.

3.2.4. SIP-Телефоны

Для создания виртуальных SIP-телефонов в программном симуляторе GNS3 была использована виртуальная машина с операционной системной Debian 12.5 с установленным VOIP клиентом Blink, который поддерживает работу по протоколу SIP.

VOIP клиент Blink был настроен для взаимодействия с виртуальной машиной, на которой была воссоздана программная АТС Asterisk Министерства здравоохранения Челябинской области. Для этого были произведены настройки подключения к серверу АТС, настройки аутентификации на сервере и настройки других параметров соединения, таких как используемые кодеки.

Использование виртуальной машины с VOIP клиентом Blink позволило полностью воссоздать функциональность реальных телефонов в виртуальной среде GNS3.

3.2.5. ПАК ViPNet Coordinator HW1000

У операционной системы ПАК ViPNet Coordinator HW1000 закрытый исходный код и производителем не предоставляется образ системы для использования в виртуальных машинах.

Поскольку принцип работы ПАК ViPNet Coordinator HW1000 похож на принцип работы обычного маршрутизатора, то для его представления в модели была создана виртуальная машина на основе CHR образа RouterOS от компании MikroTik. Виртуальный маршрутизатор был настроен так, чтобы принимать трафик, применять к нему source NAT с адресом другого нужного виртуального ПАК ViPNet Coordinator HW1000 и отправлять этот трафик на шлюз.

3.2.6. Компьютеры пользователей

Для симуляции в модели компьютеров пользователей был использован инструмент под названием VPCS. VPCS – это небольшой симулятор виртуальных компьютеров, который позволяет проверять работоспособность конфигураций сети, а также моделировать поведение пользователей. Симулятор умеет отправлять разные виды трафика через порты виртуальных компьютеров, что позволяет отслеживать потоки данных в сети. Симулятор позволяет моделировать такие действия пользователя, как отправка запросов и получение данных. Кроме того, виртуальные компьютеры имеют возможность получать параметры конфигурации сетевых интерфейсов от DHCP-серверов, что даст возможность протестировать работоспособность нового DHCP-сервера в сети.

3.3. Построение модели

В процессе разработки модели модернизированной сети были воссозданы основные элементы действующей ИКС Министерства здравоохранения Челябинской области. Были перенесены основные настройки и конфигурации оборудования. В соответствии с результатами проектирования модернизированной сети, в модель было внедрено необходимое новое оборудование. Также, были внесены изменения в конфигурацию уже существующего оборудования для исправления обнаруженных недостатков сети и для обеспечения соответствия поставленным требованиям.

Схема модели сети представлена на рисунке 3.

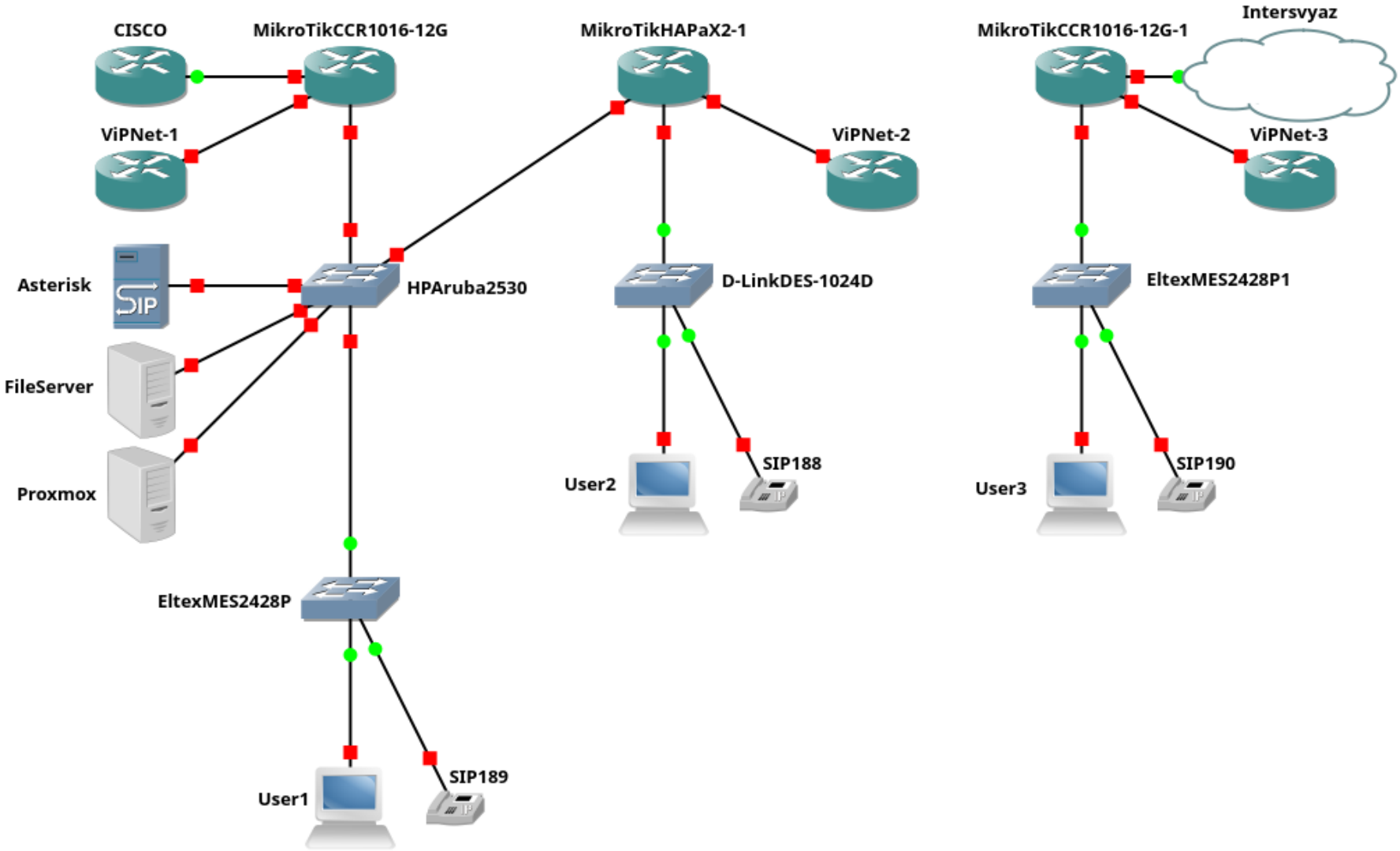

Рисунок 3 – Схема модели модернизированной ИКС Министерства здравоохранения Челябинской области

4. ТЕСТИРОВАНИЕ МОДЕЛИ

Для тестирования модели был использован метод функционального тестирования. Такой вид тестирования подразумевает составление на основе спецификации системы и функциональных требований к ней перечня тестов, в которых проверяется работоспособность ключевых функций системы путем сравнения ожидаемого результата работы функции и полученного непосредственно при использовании системы. Проведение функционального тестирования позволяет убедиться в том, что система соответствует требованиям заказчика и работает корректно.

4.1. Выбор функций для тестирования

Функции для тестирования модели были выбраны с учетом установленных требований к сети, а также внесенных в модернизированную сеть изменений.

Одним из изменений в сети было введение VLAN. Для проверки разделения сети на виртуальные подсети VLAN в модели необходимо осуществить тестовый звонок с использованием двух VOIP телефонов, а затем с помощью инструментов анализа трафика убедиться, что SIP трафик в сети имеет отличный от других устройств VLAN-тэг.

Другим изменением было внедрение DHCP-сервера в первом филиале. Для проверки этой функции необходимо в модели сети выбрать устройство, которое относится к первому филиалу, узнать его IP-адрес и проверить, соответствует ли полученный устройством IP-адрес конфигурации пула адресов DHCP-сервера на маршрутизаторе в первом филиале.

Также, в проекте модернизированной сети в первом филиале был внедрен ПАК ViPNet Coordinator HW1000 для обеспечения шифрования трафика, идущего от первого филиала в центральный офис и возможности приема шифрованного трафика из центрального офиса. Для проверки этой функции необходимо выбрать в модели компьютер, относящийся к первому филиалу,

отправить запрос, адресованный устройству, находящемуся в центральном офисе, и с помощью инструментов анализа трафика убедиться, что трафик маршрутизируется через виртуальный ПАК ViPNet Coordinator HW1000.

Проект модернизированной сети подразумевает наличие в сети сервера виртуализации на платформе Proxmox. Для тестирования возможности взаимодействия с виртуальными машинами, запущенными на сервере, необходимо с любого компьютера в модели попытаться с помощью встроенных команд проверить доступность любой из запущенных виртуальных машин по ее IP-адресу.

4.2. Проведение тестирования

На основе выбранных для тестирования функций были составлены и проведены тесты. Перечень проведенных тестов приведен в таблице 2.

Таблица 2 – Перечень проведенных тестов

Тестируемая функция	Описание тестирования	Ожидаемый результат	Полученный результат
Выделение VOIP трафика в отдельный VLAN.	1) Запустить все устройства модели. 2) Начать вызов с одного SIP-телефона на другой. 3) С помощью инструмента анализа трафика проверить VLAN-тэг трафика от телефона.	VLAN-тег трафика соответствует выделенному для SIP-трафика тэгу VLAN	Соответствует ожидаемому.
Работа DHCP сервера в первом филиале.	1) Включить все устройства модели. 2) Подключить к компьютеру, относящемуся к первому филиалу. 3) С помощью встроенных команд определить IP-адрес компьютера.	Компьютер пользователя получает IP-адрес из пула DHCP-сервера первого филиала.	Соответствует ожидаемому.

Шифрование трафика между центральным офисом и первым филиалом.	1) Включить все устройства модели. 2) Подключиться к компьютеру, относящемуся к первому филиалу. 3) Отправить запрос TCP компьютеру, относящемуся к центральному офису. 4) С помощью инструмента анализа трафика определить маршрут трафика.	Трафик проходит через ПАК ViPNet Coordinator HW1000 первого филиала и направляется в ПАК ViPNet Coordinator HW1000 центрального офиса прежде, чем дойдет до второго компьютера.	Соответствует ожидаемому.
Доступность виртуальной машины, созданной в Proxmox.	1) Включить все устройства модели. 2) Зайти в панель управления Proxmox. 3) Запустить, виртуальную машину Ubuntu Server 18.04. 4) С любого компьютера в сети с помощью встроенных команд проверить доступность виртуальной машины.	Виртуальная машина доступна с компьютера пользователя.	Соответствует ожидаемому.

Тестирование разработанной модели модернизированной ИКС показало, что ключевые функции системы функционируют согласно поставленным требованиям.

ЗАКЛЮЧЕНИЕ

В ходе выпускной квалификационной работы была спроектирована модернизированная ИКС Министерства здравоохранения Челябинской области. Также, была разработана модель модернизированной сети в программном симуляторе.

Был проведен анализ действующей информационно-коммуникационной сети Министерства здравоохранения Челябинской области, в ходе которого были выявлены основные недостатки сети. Также, была составлена схема действующей сети.

Была спроектирована модернизированная ИКС, с учетом всех поставленных требований, а также выявленных недостатков действующей сети. Была составлена схема модернизированной сети.

Был проведен выбор программного симулятора компьютерных сетей, в ходе которого был выбран симулятор для разработки модели модернизированной ИКС. Была разработана модель модернизированной ИКС, отражающая реально использующиеся конфигурации оборудования.

Было проведено тестирование модели модернизированной информационно-коммуникационной сети, в ходе которого была проведена проверка соответствия разработанной модели поставленным требованиям.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента РФ от 09.05.2017 № 203 «Об утверждении Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»

2. Постановление Губернатора Челябинской области от 27 июля 2004 года №383 «Об утверждении Положения о Министерстве здравоохранения Челябинской области» [Электронный ресурс] – Режим доступа: https://docs.cntd.ru/document/802013889

3. Приказ Министерства здравоохранения Челябинской области от 26 июня 2008 года № 560 Методические рекомендации по проектированию информационно-коммуникационной инфраструктуры в учреждениях здравоохранения Челябинской области [Электронный ресурс] – Режим доступа: https://docs.cntd.ru/document/444939722

4. Белов, В.В. Проектирование информационных систем: Учебник / В.В. Белов. – М.: Академия, 2018. – 255 с.

5. Виртуальные локальные сети VLAN [Электронный ресурс] – Режим доступа: https://edu.mmcs.sfedu.ru

6. Гадасин Д.В., Рахмани Д., Докучаев В.А., Маклачкова В.В., Шалагинов А.В., Шведов А.В. / Под ред. д.т.н., проф. В.А. Докучаева. Системы хранения данных: учебное пособие/ МТУСИ. – М., 2022. – 150с

7. Гвоздева, Т.В. Проектирование информационных систем. Стандартизация: Учебное пособие / Т.В. Гвоздева, Б.А. Баллод. – СПб.: Лань, 2019. – 252 с.

8. Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014)

9. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2013. – 334 с.

10. Перлова, О.Н. Проектирование и разработка информационных систем: Учебник / О.Н. Перлова, О.П. Ляпина, А.В. Гусева. – М.: Academia, 2017. – 416 с.

11. Таненбаум, Э.С. Компьютерные сети / Э. С. Таненбаум. – СПб.: Питер, 2012. – 992 с.

12. Финогеев, А.Г. Сетевые технологии: Учебное пособие 3 часть. Углубленный уровень подготовки / А. Г. Финогеев, А. С. Бождай. – Пенза, 2013. – 192 с.

13. Средства моделирования сетей для целей обучения [Электронный ресурс] – Режим доступа:

https://yamadharma.github.io/ru/post/2022/05/06/network-modeling-tools/

14. CISCO [Электронный ресурс] – Режим доступа: https://www.cisco.com/site/us/en/products/networking/software/index.html

15. EVE [Электронный ресурс] – Режим доступа: https://eve-ng.ru/

16. GNS3.Documentation [Электронный ресурс] – Режим доступа: https://docs.gns3.com/docs/

17. KARMA-GROUP [Электронный ресурс] – Режим доступа: https://www.karma-group.ru/catalog/vipnet-coordinator/coordinator-hw/hw1000/