

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий

институт

Вычислительная техника

кафедра

УТВЕРЖДАЮ
Заведующий кафедрой

_____ О. В. Непомнящий
подпись инициалы, фамилия
«___» _____ 2020 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Настройка и оптимизация качества обслуживания
корпоративной сети предприятия

тема

09.04.01 Информатика и вычислительная техника

код и наименование направления

09.04.01.05 Сети ЭВМ и телекоммуникации

код и наименование магистерской программы

Научный
руководитель

подпись, дата

доцент, канд.техн.наук
должность, ученая степень

Н.Ю.Сиротина
инициалы, фамилия

Выпускник

подпись, дата

В.В.Маркелова
инициалы, фамилия

Рецензент

подпись, дата

нач. ИВЦ АО
«НПП «Радиосвязь»
должность, ученая степень

М.В.Дибров
инициалы, фамилия

Нормоконтролер

подпись, дата

Н.Ю.Сиротина
инициалы, фамилия

Красноярск 2020

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Космических и информационных технологий
институт
Вычислительная техника
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой

_____ О. В. Непомнящий
подпись инициалы, фамилия
« ___ » _____ 2020 г.

**ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ
в форме магистерской диссертации**

Студенту _____ Маркеловой Виктории Владимировне
фамилия, имя, отчество

Группа КИ18-01-5М Направление (специальность) 09.04.01
номер код

«Информатика и вычислительная техника»
наименование

Тема выпускной квалификационной работы Настройка и оптимизация
качества обслуживания корпоративной сети предприятия

Утверждена приказом по университету № _____ от _____

Руководитель ВКР Н.Ю. Сиротина, доцент, канд.техн.наук, кафедра ВТ ИКИТ
инициалы, фамилия, должность, учебное звание и место работы

Исходные данные для ВКР: разработать методы для повышения качества
обслуживания корпоративной сети предприятия АО «НПП «Радиосвязь»,
без увеличения пропускной способности каналов связи

Перечень разделов для ВКР: 1 Анализ архитектуры существующей
корпоративной сети предприятия; 2 Аналитический обзор методов решения
поставленной задачи; 3 Разработка структурной и функциональной схем и
алгоритма работы; 4 Применение разработанных методов на существующей сети
передачи данных предприятия

Перечень графического материала: презентация доклада выступления

Руководитель ВКР _____ Н.Ю. Сиротина
подпись инициалы и фамилия

Задание принял к исполнению _____ В.В. Маркелова
подпись инициалы и фамилия

« _____ » _____ 20 ____ г.

РЕФЕРАТ

Выпускная квалификационная работа по теме «Настройка и оптимизация качества обслуживания корпоративной сети предприятия» содержит 45 страниц, 18 иллюстраций, 5 таблиц, 1 список сокращений, 12 использованных источников.

МЕТОДЫ КОНТРОЛЯ КАЧЕСТВА СЕТИ, КОРПОРАТИВНАЯ СЕТЬ ПЕРЕДАЧИ ДАННЫХ, ТЕХНОЛОГИЯ QOS, ТЕХНОЛОГИЯ SDN, МЕТРИКА КАЧЕСТВА СЕТИ RTT, БЛОК ПРИЛОЖЕНИЙ, БЛОК КОНТРОЛЯ, БЛОК ПЕРЕДАЧИ ДАННЫХ, СИСТЕМНЫЙ АДМИНИСТРАТОР.

Цель работы: разработка программно-аппаратной системы для повышения качества обслуживания корпоративной сети предприятия без увеличения пропускной способности каналов связи.

При выполнении данной работы было изучено задание на выпускную квалификационную работу, исследованы существующие методы решения поставленной задачи и сформированы требования, предъявляемые к разрабатываемой системе.

В результате анализа требований исследована существующая архитектура корпоративной сети передачи данных, разработаны структурная и функциональная схемы и алгоритм функционирования программно-аппаратной системы в рамках пояснительной записки. Поведение системы исследовано на разработанном стенде и частично внедрено на реальной корпоративной сети предприятия. В рамках работы исследовались изменения метрик качества сети при внедрении разрабатываемых решений.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	4
1 Описание архитектуры существующей корпоративной сети передачи данных предприятия	6
1.1 Общие сведения о предприятии	6
1.2 Архитектура корпоративной сети предприятия	6
1.3 Обзор используемого коммуникационного управляемого оборудования.....	9
1.3.1 Управляемые коммутаторы.....	9
1.3.2 Цифровая автоматическая телефонная станция	11
1.3.3 IP-телефоны	12
1.4 Модель классов обслуживания.....	13
1.5 Выводы.....	15
2 Аналитический обзор методов решения поставленной задачи.....	17
2.1 Метрики качества обслуживания	17
2.2 Метод управления разнородным трафиком	19
2.3 Программно-конфигурируемая сеть	22
2.4 Предлагаемое решение	25
2.5 Выводы.....	26
3 Разработка структурной схемы, функциональной схемы и правил блока приложений.....	27
3.1 Структурная схема разрабатываемой системы.....	27
3.2 Функциональная схема разрабатываемой системы.....	28
3.3 Разработка правил для приложений.....	30
3.4 Выводы.....	32

4	Применение разработанной системы на существующей сети передачи данных предприятия	33
4.1	Применение разработанных правил на сервере блока контроля ...	33
4.2	Исследование сети передачи данных.....	37
4.3	Выводы.....	40
	ЗАКЛЮЧЕНИЕ	41
	СПИСОК СОКРАЩЕНИЙ	43
	СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ.....	44

ВВЕДЕНИЕ

В настоящее время сети передачи данных, обслуживающие предприятия и организации, активно развиваются. Возрастает как объем трафика, так и его разнообразие. Как правило, в сети передается разнородный трафик, включающий обычные текстовые данные, голосовые и видео данные и другие, при этом различные виды данных требуют различных способов обслуживания.

В то же время сама по себе сетевая инфраструктура часто является достаточно консервативной, внесение изменений в нее требуют значительных финансовых и организационных затрат. Одним из способов повышения качества работы сети является увеличение пропускной способности каналов связи, но значительное увеличение скорости передачи данных в каналах связи сети может повлечь огромные расходы для компании [1]. Оборудование с требуемыми характеристиками имеет высокую стоимость, а управление сетью становится всё затруднительным и вынуждает тратить огромные ресурсы на поддержание сети в работоспособном виде. К тому же протоколы маршрутизации не учитывают реальную загруженность сети.

В этой ситуации актуальной задачей является поиск возможных способов повышения качества работы сети за счет внутренних резервов. Одним из таких резервов является оптимизация управления трафиком, которая может обеспечить эффективную работу разнородных систем. Эффективность использования ресурсов канала пакетной передачи данных всегда была актуальной задачей, но ее важность возросла в последние годы в связи с появлением все более жестких требований к качеству обслуживания разнородного трафика, в особенности IP-телефонии и видеосвязи. Негативные последствия неудовлетворительного качества обслуживания могут привести к финансовым проблемам, некачественной коммуникации и увеличению задержек в производстве.

Целью выпускной квалификационной работы является разработка программно-аппаратной системы для повышения качества обслуживания

корпоративной сети предприятия без увеличения пропускной способности каналов связи.

Поставленные задачи:

- исследование и анализ структуры существующей корпоративной сети предприятия;

- исследование существующих методов и систем, обеспечивающих оптимизацию качества обслуживания мультисервисной сети пакетной передачи данных;

- разработка системы по оптимизации качества обслуживания сети применимой к существующей корпоративной сети предприятия;

- применение разработанной системы по оптимизации качества обслуживания сети на существующем оборудовании предприятия.

В результате применения системы выявленные уязвимости и проблемы с качеством передачи данных в корпоративной сети предприятия решены.

Тестирование разработанной системы подтвердило ее работоспособность.

Анализ изменения структуры трафика сети передачи данных показал, что в связи с ростом чувствительных к задержкам мультимедийных приложений повышаются требования к качеству обслуживания. При использовании разработанной системы можно повысить существующий уровень качества обслуживания, что в свою очередь, позволит подключить дополнительное число пользователей к тому же сегменту сети.

1 Описание архитектуры существующей корпоративной сети передачи данных предприятия

1.1 Общие сведения о предприятии

Данная работа выполнялась для корпоративной сети предприятия АО «НПП «Радиосвязь» г. Красноярск.

Сегодня предприятие имеет мощную научно–техническую и производственную базу, является единственным предприятием в России, разрабатывающим и одновременно серийно изготавливающим помехозащищённые станции спутниковой и тропосферной связи, а также навигационные системы и комплексы, обеспечивающие определение с точностью до единиц угловых минут положение объектов в пространстве [2].

Основные направления работы:

- разработка и производство станций спутниковой связи;
- разработка и производство станций тропосферной связи;
- разработка и производство аппаратуры спутниковой навигации ГЛОНАСС/GPS;
- разработка и производство систем фазовой навигации.

За развитие и поддержку корпоративной сети, обеспечивающей автоматизацию многих отраслей производства, непрерывную коммуникационную связь и охрану территории, отвечает отдел автоматизированных систем управления предприятием (АСУП).

Из выше изложенного можно сделать вывод, что качество обслуживания в данной корпоративной сети должно соответствовать всем потребностям производства, чтобы обеспечивать качественную работу предприятия.

1.2 Архитектура корпоративной сети предприятия

Архитектура корпоративной сети предприятия включает в себя только проводные соединения управляемого оборудования. Магистральные устройства

корпоративной сети соединены по топологии «кольцо» с дополнительными резервными связями.

Топология «кольцо» обеспечивает резервирование каналов и масштабирование сети с наименьшими затратами по сравнению с топологией «звезда». «Кольцо» более выгодно для распределённых сетей. Сделать «звезду» на большую распределённую сеть очень дорого, так как требуются дополнительные резервные каналы. Поэтому для предприятий с несколькими корпусами – это оптимальная топология. Такая топология обеспечивает резервирование без дополнительного соединения. В случае обрыва канала между двумя устройствами маршруты, которые были построены через этот канал просто перестроятся благодаря динамическому протоколу маршрутизации OSPF (Open Shortest Path First). Некоторые пакеты будут маршрутизироваться по более длинному пути, но при этом все сегменты сети останутся работоспособными.

Сеть построена по принципу иерархической модели, которая делит сеть на три основных уровня:

1. Уровень доступа (Access Layer) – предоставляет пользователям и устройствам доступ к сети.
2. Уровень распределения (Distribution Layer) – объединяет сегменты уровня доступа.
3. Уровень ядра (Core Layer) – объединяет сегменты уровня распределения.

На уровне доступа располагаются управляемые коммутаторы уровня L2 и осуществляют сегментирование сети на подсети по технологии VLAN (Virtual Local Area Network). К уровню подключаются компьютеры пользователей, принтеры, IP-телефоны.

Главной задачей уровня распределения является объединение уровня доступа, что позволяет существенно уменьшить количество соединений. Так же к оборудованию этого уровня подключаются сервисы сети, а именно сервера. В архитектуре этого уровня стоят управляемые коммутаторы уровня L3 и поддерживают маршрутизацию.

Иерархическая модель сети представлена на рисунке 1.

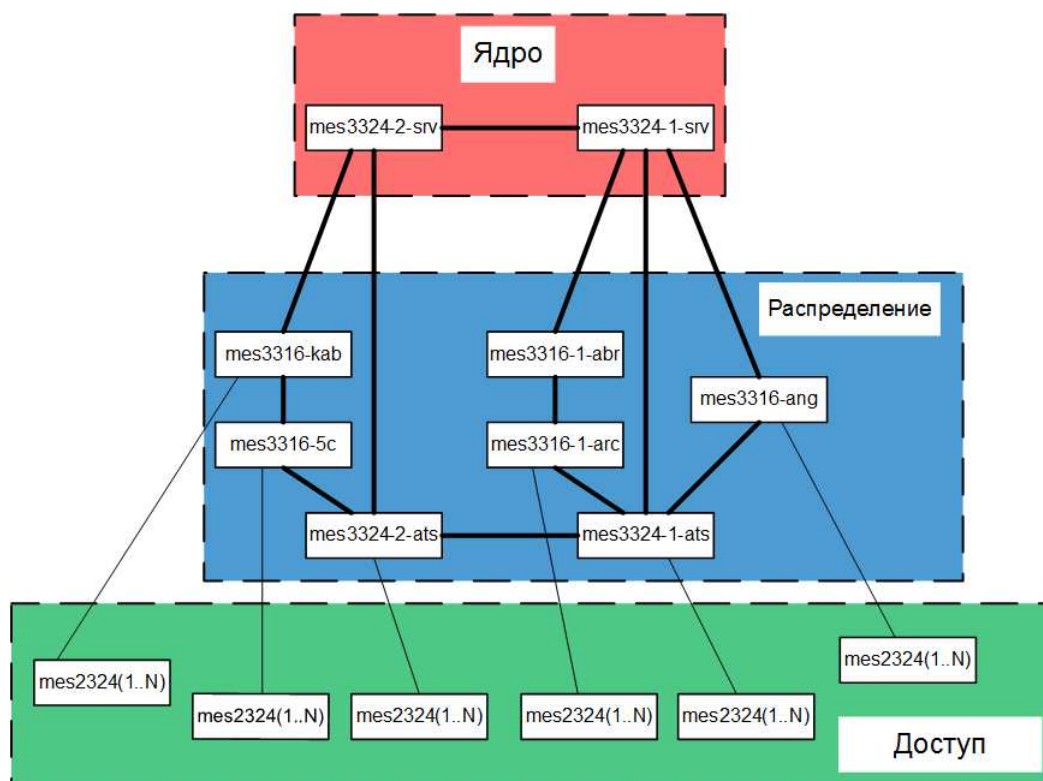


Рисунок 1 – Иерархическая модель СПД

Сеть передачи данных была бы ненужной без ресурсов сети. В данной работе под ресурсами сети понимается различного вида данные, которые передаются по сети передачи данных от одних узлов к другим и обратно.

К ресурсам сети относятся сервера сервисных приложений, баз данных, различных автоматизированных систем, вычислительных ресурсов и производственных приложений.

Для обеспечения сотрудников телефонной связью предприятие оборудовано цифровой автоматической телефонной станцией (АТС) и IP-телефонами, которые используют локальную сеть для передачи пакетов. Для автоматизированного управления телефонами организован сервер автоматических централизованных обновлений конфигурации и программного обеспечения.

Для обеспечения безопасности предприятия и контроля над территорией введены система видеонаблюдения и система автоматизированного контроля доступом в помещения. Используются IP-видеокамеры различных производителей и специализированные серверные приложения для записи видео и управлением системой видеонаблюдения. Система контроля доступа (СКД) также использует локальную сеть для передачи данных с приборов, находящихся на различных точках доступа в помещения, а также серверное программное обеспечение для управления СКД.

В пользовательской сети преобладает трафик производственных приложений, организованных по принципу клиент-сервер. Они представляют собой веб-приложения, использующих базы данных, и располагаются на серверах. Со стороны клиента доступ к приложениям организован через пользовательские рабочие станции с помощью веб-браузера.

Так же существуют обязательные для любой сети серверы такие как: серверы администрирования пользовательскими рабочими станциями и серверами; серверы, защищающие от различных сетевых угроз, а также вычислительные серверы.

В качестве сетевой операционной системы (ОС) на большинстве рабочих станций установлена ОС Microsoft Windows 7 (RUS), а также небольшое количество станций с ОС Microsoft Windows 10 (RUS). Для серверов – ОС Microsoft Windows Server 2016 (RUS).

1.3 Обзор используемого коммуникационного управляемого оборудования

1.3.1 Управляемые коммутаторы

Для организации IP-телефонии на заданном предприятии использовано оборудование компании «ELTEX» – ведущего российского разработчика и производителя коммуникационного оборудования. Данное оборудование

обеспечивает бюджетные и функциональные решения для развёртывания как малой корпоративной сети, так и сеть крупного предприятия.

На рисунке 1 представлен магистральный сегмент корпоративной сети предприятия на основе коммутаторов MES3316F и MES3324. Коммутаторы данной серии обеспечивают высокую производительность, гибкость, безопасность, многоуровневое качество обслуживания QoS (Quality of Service) [3].

Коммутатор уровня L3 MES3316F имеет в себе развитые функции L2, поддержку статической и динамической маршрутизации, наличие 12 интерфейсов 1 Гбит/с (SPF), 4 комбо-интерфесов 1 Гбит/с, 4 интерфейсов 10 Гбит/с (SFP+), пропускная способность 112 Гбит/с возможность объединения в стек до 8 устройств, резервирование источников питания с возможностью горячей замены. Имеет значительный запас по производительности благодаря универсальным интерфейсам, работающим на скорости 10Гбит/с или 1Гбит/с [3].

Устройство поддерживает приоритезацию исходящего трафика по очередям на каждом порту. Распределение пакетов по очередям может производиться в результате классификации пакетов по различным полям в заголовках пакетов. Стандарт 802.1p специфицирует метод указания приоритета кадра и алгоритм использования приоритета в целях своевременной доставки чувствительного к временным задержкам трафика. Стандарт 802.1p определяет восемь уровней приоритетов. Коммутаторы могут использовать значение приоритета 802.1p для распределения кадров по приоритетным очередям [4].

Коммутатор MES3324 отличается от предыдущего большим количеством SFP интерфейсов (24 интерфейса 1 Гбит/с (SPF)) и высокой пропускной способностью (128 Гбит/с). Коммутаторы представлены на рисунке 2.



Рисунок 2 – Внешний вид коммутаторов MES3316F и MES3324

1.3.2 Цифровая автоматическая телефонная станция

Опции платформы SMG-2016 позволяют использовать платформу в качестве полнофункциональной IP-АТС до 3 000 SIP-абонентов. Программный модуль IP-АТС ECSS-10 предназначен для быстрого развёртывания VoIP-узла связи с минимальными капитальными затратами (CAPEX): «АТС+ДВО» – пакет для использования SMG-2016 в качестве офисной АТС [5].

Платформа позволяет настраивать QoS и контролировать полосу пропускания. Настраиваемые функции обеспечения качества обслуживания:

- приоритет VLAN;
- режим QoS – режим использования QoS;
- режим ограничения входящих пакетов – режим ограничения трафика, поступающего на порт;
- ограничение скорости для входящих пакетов в очереди 0-3 – ограничение полосы пропускания трафика, поступающего на порт для 0-3 очереди.

Гибридная платформа SMG-2016 на предприятии используется в качестве IP-АТС (цифровая автоматическая телефонная станция) с поддержкой функций дополнительного вида обслуживания (ДВО).

SMG-2016 представлена на рисунке 3.



Рисунок 3 – Внешний вид гибридной платформы SMG-2016

1.3.3 IP-телефоны

Yealink SIP-T19P E2 – это качественный IP-телефон начального уровня, обладающий функциональностью и производительностью, как у более продвинутых моделей телефонов. Аппарат поддерживает одну учётную запись VoIP, технологии PoE, VLAN, QoS и обширное количество поддерживаемых услуг ДВО [6]. Самая распространённая модель IP-телефона на предприятии (рисунок 4).

Так же имеются модели Yealink SIP-T21P, T27P, T29G (рисунок 5) с более продвинутым интерфейсом, большим количеством функций и поддержкой нескольких аккаунтов.



Рисунок 4 – Модель IP-телефона Yealink T19P



Рисунок 5 – Модели IP-телефонов Yealink T21P, T27G

IP-телефоны «Yealink» – это полнофункциональные телефоны, которые можно подключить напрямую к IP-сети и могут быть легко использованы без ручной настройки.

Для этого они поддерживают функцию автоматического обеспечения (Auto Provision) с помощью протокола TFTP (Trivial File Transfer Protocol). С помощью конфигурационного файла на сервере TFTP настраиваются все необходимые настройки. Затем при подключении телефона в сеть, автоматически подгружаются все сконфигурированные настройки. Настройки могут быть индивидуальными для каждого телефона, определяемые по MAC-адресу устройства, так и общими применимыми ко всем телефонам сразу.

1.4 Модель классов обслуживания

Сеть передачи данных предприятия логически разделена на классы обслуживания. Каждый класс обслуживания имеет свои параметры и выдвигает свои требования к обслуживанию, так как используются различные приложения с различными характеристиками и способами применения.

В сети предприятия классы поделены с помощью адресного пространства.

Каждому классу выделен свой пул адресов:

- 10.0.0.0/12 – удалённое управление устройствами;

- 10.16.0.0/12 – транспорт (соединения между коммутаторами);
- 10.32.0.0/12 – пользовательская сеть;
- 10.48.0.0/12 – сеть IP-телефонии;
- 10.64.0.0/12 – сеть серверов;
- 10.80.0.0/12 – видеонаблюдение;
- 10.96.0.0/12 – сеть системы контроля доступом на предприятии (СКД).

В таблице 1 представлены характеристики и требования к классам обслуживания и соответствующие им категории приложений.

Таблица 1 – Характеристики и требования к классам обслуживания

Категория приложения	Класс обслуживания	Характеристики	Требования
Контроль приложений	Удалённое управление устройствами	Удалённое подключение к оборудованию, его конфигурация и мониторинг	Наивысший приоритет, трафик чувствительный к задержкам
	Транспорт	Служебный трафик, маршрутизация данных	Высокий приоритет, чувствительный к задержкам
Медиа-ориентированные приложения	Сеть IP-телефонии	Трафик реального времени, телефонные разговоры, конференцсвязь	Высокий приоритет, очень чувствительный к задержкам
	Пользовательская сеть	Рабочие места операторов видеонаблюдения	Средний/низкий приоритет, средняя/низкая чувствительность к задержкам
	Видеонаблюдение	Данные цифровых камер видеонаблюдения	Средний приоритет, чувствительность к задержкам средняя

Категория приложения	Класс обслуживания	Характеристики	Требования
Данные	Пользовательская сеть	Производственные приложения	Приоритет средний/низкий, средняя/низкая чувствительность задержкам
Данные	Сеть серверов	Серверы пользовательских приложений, серверы администрирования, сервер видеонаблюдения	Приоритет выше среднего/средний, средняя/низкая чувствительность задержкам
	Сеть СКД	Приборы и сервер СКД, рабочие места операторов для мониторинга и администрирования системы СКД	Средний приоритет, низкая чувствительность задержкам

В соответствии с характеристиками и требованиями к классам обслуживания можно определить способы обеспечения оптимального качества обслуживания различного вида трафика в сети передачи данных.

1.5 Выводы

В главе 1 выполнено обоснование необходимости разработки системы для оптимизации качества обслуживания корпоративной сети предприятия. С этой целью проведено исследование архитектуры существующей корпоративной сети.

Произведён обзор использованного оборудования и программного обеспечения, на основании которого можно сделать вывод, что оборудование поддерживает упомянутую технологию QoS, которая необходима для

достижения поставленной цели. Программное обеспечение устройств позволяет создать централизованное управление настройками рабочего оборудования.

Также при исследовании структуры сети определено, что трафик, проходящий по сети передачи данных, поделён на классы обслуживания. На основании этого был сделан вывод о возможности определения способов обеспечения оптимального качества обслуживания различного вида трафика в сети передачи данных.

2 Аналитический обзор методов решения поставленной задачи

2.1 Метрики качества обслуживания

Для исследования методов решения по оптимизации качества обслуживания, а также для оценки состояния сети передачи данных предприятия необходимо определить параметры, характеризующие качество сети, называемые, метриками сети.

К основным метрикам качества сети относятся:

- потери пакетов;
- задержки;
- джиттер.

Потери пакетов говорят о том, сколько из отправленных источником пакетов дошло до адресата. Как правило, как справляется с потерями зависит от приложения. В случае с веб-приложениями, использующих протокол TCP, пакет отправляется заново, а в случае телефонного разговора (протокол UDP) – пакет отбрасывается.

Задержка – это время, которое необходимо данным, чтобы добраться от источника до получателя. Задержка создает неудобство при ведении диалога, приводит к перекрытию разговоров и возникновению эхо.

Можно выделить следующие источники задержки при пакетной передаче речи.

1. Задержка накопления – величина задержки определяется типом речевого кодера и изменяется от микросекунд до нескольких миллисекунд;
2. Задержка обработки – процесс кодирования и сбора закодированных отсчетов в пакеты для передачи через пакетную сеть создает определенные задержки. Задержка кодирования или обработки зависит от времени работы процессора и используемого типа алгоритма обработки;

3. Сетевая задержка – задержка обусловлена физической средой и протоколами, используемыми для передачи речевых данных, а также буферами, используемыми для удаления джиттера пакетов на приемном конце [10].

Чаще всего для оценки занятости канала используют круговую задержку RTT (Round Trip Time). Это интервал времени между отправкой пакета и окончанием его обработки на принимающей стороне. В основном данную метрику отслеживают с помощью ICMP протокола (Internet Control Message Protocol).

Разница в задержках между доставкой последовательных пакетов называется джиттером [11]. Опять же зависит от приложения существенность данной метрики. Большинству приложений достаточно, чтобы пакет был доставлен и неважно была ли там задержка. Но для той же IP-телефонии это играет важную роль. Джиттер приводит к специфическим нарушениям передачи речи, слышимым как трески и щелчки.

Различают три формы джиттера:

1. Джиттер, зависимый от данных - происходит в случае ограниченной полосы пропускания или при нарушениях в сетевых компонентах;
2. Искажение рабочего цикла - обусловлено задержкой распространения между передачей снизу-вверх и сверху-вниз;
3. Случайный джиттер - является результатом теплового шума.

Для оценки любого вида трафика наиболее показательной и удобной в применении является круговая задержка RTT. Для её измерения существует множество программ в том числе и в свободном доступе.

В рамках данной работы измерения производились с помощью программы-анализатора трафика Wireshark актуальной на время исследований версии 3.2.4.

2.2 Метод управления разнородным трафиком

Методом контроля и управления разнородным трафиком, который позволяет повысить производительность сети, не требуя роста пропускной способности канала, является технология QoS (Quality of Service), определяющая методы качества обслуживания сети. QoS (уровень сервиса или обслуживания) — технология указания приоритетов обслуживания разным типам трафика. То есть QoS — технология, которая может гарантировать пропуск в полном объеме определенному виду трафика в заданных технологических рамках [7].

Существует три модели обеспечения QoS:

- Best Effort: не гарантирует качества передачи трафика, все потоки равны;
- IntServ: гарантирует качество для каждого потока, заблаговременно резервирует ресурсы от источника до получателя;
- DiffServ: за определение качества отвечает каждый узел, по которым идёт передача, отсутствует резервирование.

В настоящее время в сетях чаще всего используются механизмы DiffServ, так как механизмы IntServ требуют огромных ресурсов от вычислительных процессоров передающих устройств, в связи с постоянным заблаговременным резервированием ресурсов.

Принцип DiffServ в следующем: трафик делится на классы. Затем пакет на входе в каждый узел классифицируется и к нему применяется набор инструментов, который по-разному обрабатывает пакеты разных классов, таким образом обеспечивая им разный уровень сервиса [8].

В сети системный администратор определяет классы сервиса, которые он может предоставлять трафику и сопоставляет им некоторое цифровое значение DSCP (DiffServ Code Point), иначе называемый приоритетом. Под одной меткой в поле DSCP агрегированы различные категории трафика, которые ожидают одинакового по отношению к себе поведения. Например, все SIP-сессии будут агрегированы в один класс. Количество возможных классов сервиса ограничено.

Как поделить классы сервиса решает системный администратор, но также существуют рекомендации от IETF (Internet Engineering Task Force) в RFC 4594 «Рекомендации по настройке для классов обслуживания DiffServ». В нём определены основные категории приложений и их классы сервиса.

В терминологии Diffserv поведение пересылки, которое назначается значением DSCP, называется моделью поведения PHB (Per-Hop Behavior). PHB определяет приоритет пересылки, который помеченный пакет получает по отношению к другому трафику в системе с поддержкой Diffserv.

Модели поведения:

- Default Forwarding (DF). Стандартная пересылка. Возможны отбрасывания пакетов, перемешивание порядка приёма пакета, непредсказуемые задержки. Такая модель подходит для нетребовательных приложений.

- Assured Forwarding (AF). Гарантированная пересылка. Отбрасывания и задержки могут быть, но в меньшей степени в сравнении со стандартной пересылкой. Уменьшение переупорядочивания пакетов. Подходит для важных приложений и мультимедиа.

- Expedited Forwarding (EF). Экстренная пересылка. Это модель для приложений, которым нужны отсутствие потерь, короткие задержки. Подходит для IP-телефонии.

- Class Selector (CS). Обеспечивает уровень сервиса, который исключит отбрасывания пакетов и задержки даже в случае экстремальной перегрузки интерфейсов оборудования. Обычно эта модель поведения по умолчанию определена для трафика конфигурирования, контроля и мониторинга коммуникационного оборудования.

В таблице 2 определены классы моделей поведения и соответствующие им значения DSCP и наиболее подходящие под модель поведения классы приложений.

Таблица 2 – Классы модели поведения и соответствующие им значения DSCP и подходящие классы приложений

Класс модели поведения	Значение DSCP	Класс приложения
CS6, CS7	48, 56	Сетевой служебный трафик
EF	46	IP-телефония
CS5	40	Сигнальный трафик IP-телефонии
AF41, AF42, AF43	34, 36, 38	Видеоконференции, видеоигры
CS4	32	
AF31, AF32, AF33	26, 28, 30	Потоковое видео и аудио (видеокамеры)
CS3	24	Широковещательное телевидение и прямые трансляции
AF21, AF22, AF23	18, 20, 22	Клиент-серверные приложения
CS2	16	Администрирование
AF11, AF12, AF13	10, 12, 14	Хранение данных
CS1	8	Любые приложения, в которых необязательна гарантированная пересылка
CS0	0	Прочие приложения

В большинстве случаев механизмы DiffServ отвечают требованиям локальных сетей. Но методы QoS не всегда справляются с задачами на должном уровне, так как некоторые потоки трафика могут оставаться с неучтённым приоритетом и обрабатываются с приоритетом Best Effort.

2.3 Программно-конфигурируемая сеть

Побороть недостаток технологии QoS способна новая актуальная в настоящее время концепция SDN (Software-Defined Networking). Программно-конфигурируемая сеть (SDN) – сеть передачи данных, в которой уровень управления сетью отделен от устройств передачи данных и реализуется программно, одна из форм виртуализации вычислительных ресурсов [9]. Технология, позволяет подстраиваться под нужды пользователей и регулировать загруженность там, где она возникает. SDN перемещает управление сетевыми ресурсами в выделенный элемент сети, а именно – контроллер SDN, который обеспечивает средство для программирования, оркестрации, контроля и управления сетевыми ресурсами посредством программного обеспечения, то есть приложений SDN [12].

Необходимый анализ пакетов, необходимые изменения информации в пакетах и правила пересылки возлагаются на контроллер. Сами устройства следуют инструкциям контроллера, нагрузка на вычислительные ресурсы значительно снижается. Достигается централизация логики управления сетью, что позволяет конфигурировать сеть как единое целое и существенно упрощает эксплуатацию сети.

Есть четыре области, в которых технология SDN может иметь значение для организации.

1. Программируемость сети. SDN позволяет контролировать поведение сети с помощью программного обеспечения, которое находится за пределами сетевых устройств, на едином контроллере. В результате системные администраторы могут адаптировать поведение своих сетей для поддержки новых услуг.

2. Логическая централизация контроля. SDN построен на логически централизованных сетевых топологиях, которые обеспечивают управление сетевыми ресурсами. Устройства функционируют автономно с ограниченной осведомленностью о состоянии сети. Благодаря централизованному

управлению, которое обеспечивает сеть на основе SDN, управление полосой пропускания, восстановление, безопасность и политики могут быть высокоинтеллектуальными и оптимизированными, и организация получает целостное представление о сети [9].

3. Абстрагирование сети. Сервисы и приложения, работающие по технологии SDN, абстрагируются от базовых технологий и оборудования, которые обеспечивают физическое соединение с помощью сетевого управления. Приложения будут взаимодействовать с сетью через API (Application Programming Interface), а не через интерфейсы управления, тесно связанные с оборудованием.

4. Открытость. Архитектура SDN открывает новую эру открытости, которая обеспечивает совместимость с несколькими поставщиками. Открытые API-интерфейсы поддерживают широкий спектр приложений, включая облачную оркестровку и важные для бизнеса сетевые приложения. Кроме того, интеллектуальное программное обеспечение может управлять оборудованием различных производителей с помощью открытых программных интерфейсов, таких как OpenFlow. Наконец, из SDN интеллектуальные сетевые службы и приложения могут работать в общей программной среде.

Архитектура сетей SDN подразделяется на три уровня:

- уровень приложений;
- уровень контроля;
- уровень передачи данных.

Ресурсы уровня передачи данных выполняют сетевые функции, такие как передача и обработка данных, но их поведение управляется уровнем контроля. Взаимодействие контроллера с уровнем передачи данных возможно с помощью интерфейсов и специализированных протоколов, например, OpenFlow, обеспечивающих взаимодействие с сетевыми устройствами. На другой стороне контроллер предоставляет стандартизированные программные интерфейсы API, наличие которых позволяет создавать приложения для управления сетью. Такие приложения могут, например, управлять пропускной способностью,

динамически назначать приоритеты различным видам трафика, контролировать доступ к сетевым ресурсам.

Архитектура сети SDN представлена на рисунке 6.

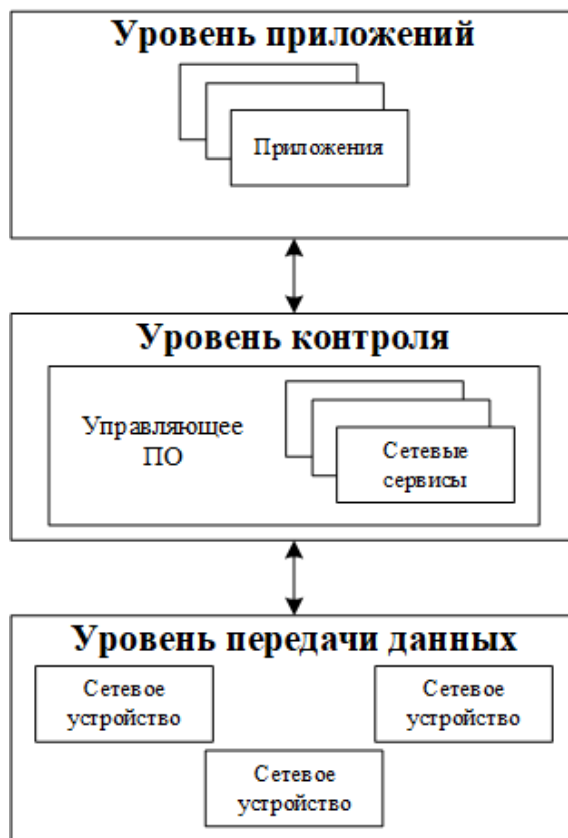


Рисунок 6 – Схема архитектуры сети SDN

К недостатку концепции относится высокая стоимость реализации. Оборудование с поддержкой данной технологии, полностью управляемое из центрального контроллера, может позволить не каждая компания. К тому же, в настоящее время существует лишь несколько производителей подобного оборудования.

Поэтому необходимо альтернативное решение для организации передачи разнородного трафика в сети с минимальными расходами, актуальными технологиями и оптимальным обеспечением качества сети.

2.4 Предлагаемое решение

Концепция SDN является актуальным решением в настоящее время, но не может быть реализована в уже существующей корпоративной сети предприятия с оборудованием, не поддерживающим технологии SDN.

Из определения SDN следует, что всё управление сетью снимается с коммутационного оборудования, поэтому оборудование в корпоративной сети заменять нет необходимости. Уровень приложений можно организовать с помощью технологии QoS, которая уже поддерживается даже на самых простых коммутаторах и маршрутизаторах, поэтому её можно использовать в качестве определения приоритета трафика. На порты коммутаторов уже будет поступать трафик с назначенными приоритетами, оборудование будет лишь заниматься очередями пакетов и продвижением их по сети.

В основу реализации концепции SDN в существующей корпоративной сети входит разработка методов управления разнородным трафиком. К уровню контроля будут относиться серверы администрирования, которые могут централизованно управлять приложениями вышестоящего уровня. Управление данными серверами передаётся ответственному лицу, например, системному администратору, который сможет управлять приложениями по мере необходимости. В дальнейшем эту задачу планируется переложить на программное обеспечение.

На уровне передачи данных сетевые устройства оставляют за собой передачу данных и управление очередями, но не назначают приоритеты различным классам обслуживания.

Таким образом будет выполняться требование к актуальности решения проблемы и оптимальным обеспечением качества сети с минимальными расходами.

2.5 Выводы

В главе было проведено исследование существующих систем оптимизации качества обслуживания и выявлены достоинства и недостатки рассмотренных систем. На основании этого был сделан вывод о необходимости разработки системы для улучшения качества обслуживания без финансовых затрат на оборудование и программного обеспечения, а также выбраны показатели и критерии качества сети передачи данных.

3 Разработка структурной схемы, функциональной схемы и правил блока приложений

3.1 Структурная схема разрабатываемой системы

В соответствии с поставленными задачами и выдвинутыми требованиями, разработана структурная схема системы, представленная на рисунке 7.

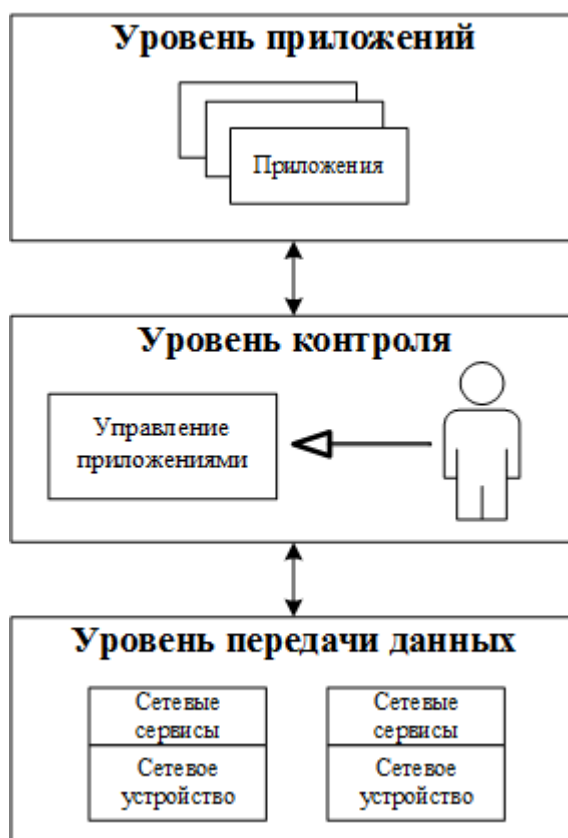


Рисунок 7 – Структурная схема системы

Схема представляет собой совокупность блоков:

- уровень приложений;
- уровень контроля;
- уровень передачи данных.

Блок контроля является «ядром» всей системы и представляет из себя сервер с управляющим программным обеспечением, который централизованно

управляет приложениями вышестоящего блока и передают правила передачи данных нижестоящему блоку. Управление сервером осуществляется системным администратором, который сможет управлять и контролировать приложения в зависимости от потребности сети.

Блок приложений представляет собой совокупность различных приложений:

- производственные приложения;
- приложения, обеспечивающих автоматизацию систем охраны и пожарной безопасности предприятия;
- приложения, обеспечивающих администрирование;
- другие приложения, обеспечивающие работоспособность сети.

На уровне приложений назначаются приоритеты пакетам приложений так, как было назначено на уровне контроля. Приложения взаимодействуют друг с другом от серверов до рабочих станций и обратно через блок передачи данных.

Блок передачи данных представляет собой сеть коммутационного оборудования, которая осуществляет передачу данных с уже определёнными приоритетами с уровня приложений и управление очередями. Блок передачи данных не анализирует какой приоритет назначить тому или иному пакету.

3.2 Функциональная схема разрабатываемой системы

В соответствии с разработанной структурной схемой и определенным составом компонентов в разделах 1.1 и 1.2 соответственно, разработана функциональная схема системы (рисунок 8).

К уровню контроля относится сервер администрирования пользовательских рабочих станций и серверов производственных приложений с именем AD (Active Directory). Сервер AD отвечает за групповые политики пользователей домена корпоративной сети. Также с данного сервера настраиваются с помощью конфигурационных файлов IP-телефоны.

Управление данным сервером отводится системному администратору. Изменяя по необходимости параметры в программном обеспечении и конфигурационных файлах сервера AD, происходит управление трафиком в сети передачи данных. Уровень контроля передаёт уровню приложений и уровню передачи данных как взаимодействовать их компонентам друг с другом.

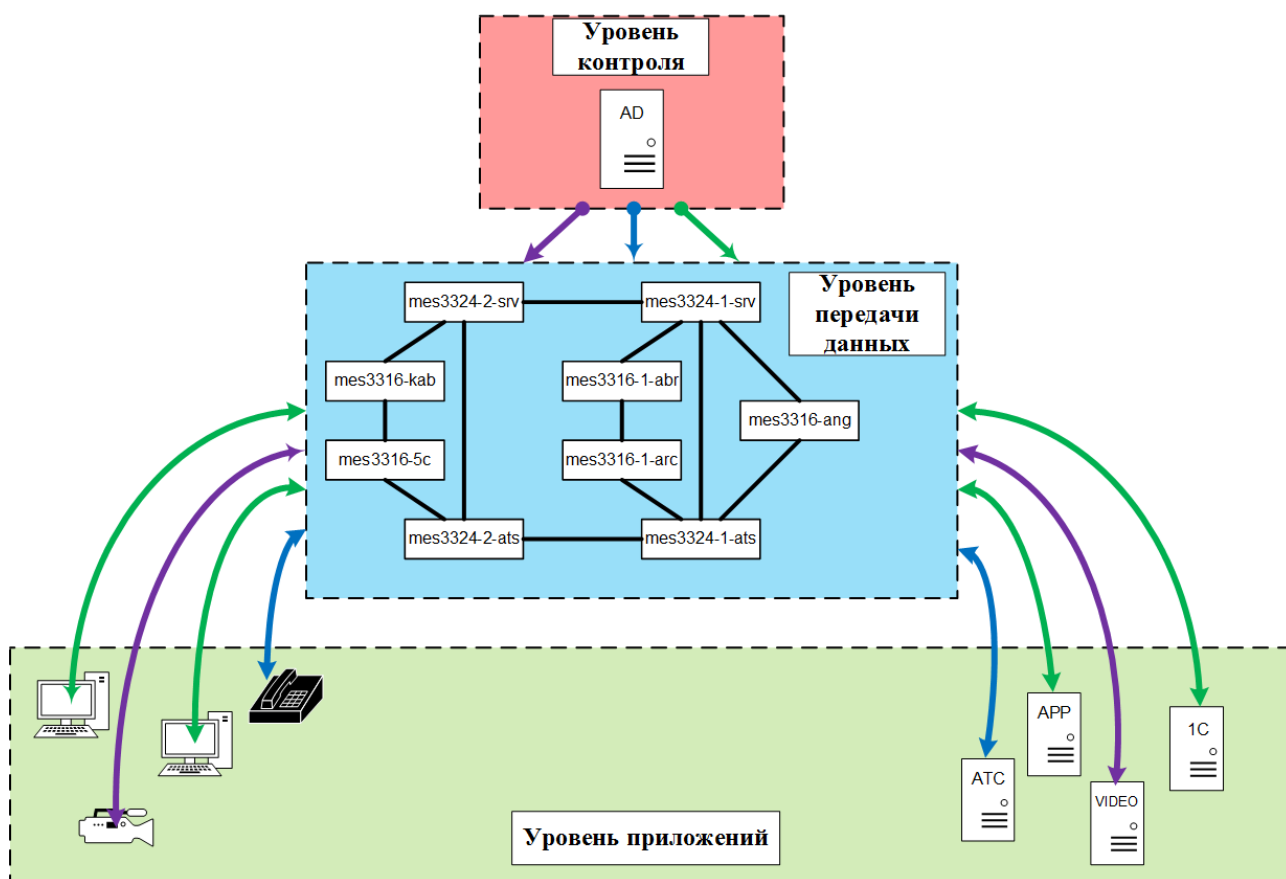


Рисунок 8 – Функциональная схема системы

Уровень передачи данных представляет собой сеть коммутаторов, распределённых по территории предприятия, по которой происходит передача данных преимущественно между серверами и устройствами: телефоны, рабочие станции, видекамеры. Коммутаторы передают пакеты с уже назначенными правилами передачи и регулируют только очереди пакетов. Коммутаторы поддерживают до восьми очередей.

К уровню приложения относятся рабочие пользовательские станции и периферийные устройства, IP-телефоны и видекамеры. Правила передачи

трафика через уровень передачи данных, данный уровень получает централизованно от уровня контроля. Взаимодействие с серверами происходит через уровень передачи данных по своим назначенным потокам с приоритетами.

Физически архитектура сети не меняется, замена оборудования не производится.

Разработанные структурная и функциональная схемы позволяют разработать правила для приложений и настроить блок контроля для существующей корпоративной сети.

3.3 Разработка правил для приложений

В главе 1 определено, что производственные приложения установлены на рабочие станции с операционной системой Microsoft Windows, и серверы приложений под управлением Microsoft Windows Server. Поэтому управление этих приложений можно организовать с помощью групповых политик домена сети. Групповые политики позволяют централизованно определять набор правил, в соответствии с которыми производится настройка рабочей среды.

Перед созданием политики качества обслуживания важно понимать два ключевых элемента управления QoS, которые используются для управления сетевым трафиком.

- Значение DSCP;
- Ограничение частоты передачи.

Для конфигурации использовано значение DSCP подробно описанном во второй главе. DSCP позволяет указывать значения от 0 до 63 в поле пакета IPv4. Сетевые коммутаторы используют значение DSCP для классификации сетевых пакетов и постановки их в очередь соответствующим образом.

В рамках стратегии обеспечения качества обслуживания сети необходимо предусмотреть количество очередей и поведение для пакетов с разными приоритетами.

В соответствии с характеристиками и требованиями к категориям приложений в разделе 1.2 классы обслуживания были распределены следующим образом:

1. Класс 1 – интерактивный трафик (IP-телефония);
2. Класс 2 – трафик клиент-серверных приложений (производственные приложения);
3. Класс 3 – потоковый трафик (видеонаблюдение с рабочих станций).

В разделе 2.2 были определены классы моделей поведения и соответствующие им значения DSCP и подходящие классы приложений.

В таблице 3 выделенным классам определены следующие модели поведения и значения DSCP (приоритет).

Таблица 3 – Определение классам обслуживания модели поведения

Класс обслуживания	Модель поведения	Значение DSCP
Класс 1	EF, AF31	46, 26
Класс 2	AF23, AF13	22, 14
Класс 3	AF11	10

По необходимости приоритеты для приложений можно изменять в зависимости от потребности сетевых ресурсов в различные периоды времени.

Политику можно применить ко всем приложениям, к конкретному приложению, определяемому именем исполняемого файла, либо к серверным приложениям HTTP, обрабатывающим запросы для определенного URL-адреса.

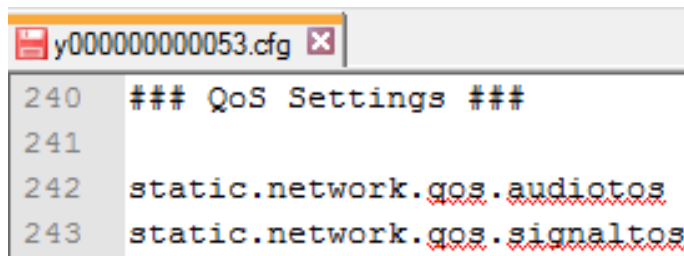
Также можно указать исходный и конечный IP-адреса, протоколы TCP и UDP и порты источника и назначения.

Политики можно изменять в любое время и обновить их применение.

В главе 1 также было определено, что IP-телефоны поддерживают технологию автоматического обновления, которую можно использовать для реализации разработанной системы.

Изменяя два параметра в одном общем конфигурационном файле можно добиться применения правил во всех телефонах.

Необходимые параметры для назначения DSCP отображены на рисунке 9.

A screenshot of a text editor window titled 'y0000000000053.cfg'. The window displays four lines of configuration text: line 240 contains '### QoS Settings ###', line 241 is blank, line 242 contains 'static.network.qos.audiotos :', and line 243 contains 'static.network.qos.signaltos'. The text is in a monospaced font with a light gray background.

```
240  ### QoS Settings ###
241
242  static.network.qos.audiotos :
243  static.network.qos.signaltos
```

Рисунок 9 – Параметры QoS конфигурационного файла

3.4 Выводы

В данной главе в соответствии с поставленной задачей была разработана структурная схема разрабатываемой системы для улучшения качества обслуживания корпоративной сети и схема функциональной структуры процесса её функционирования. Разработанные структурная схема и функциональная схема обеспечили возможность разработки правил уровня приложений и дальнейшую разработку блока контроля для существующей корпоративной сети.

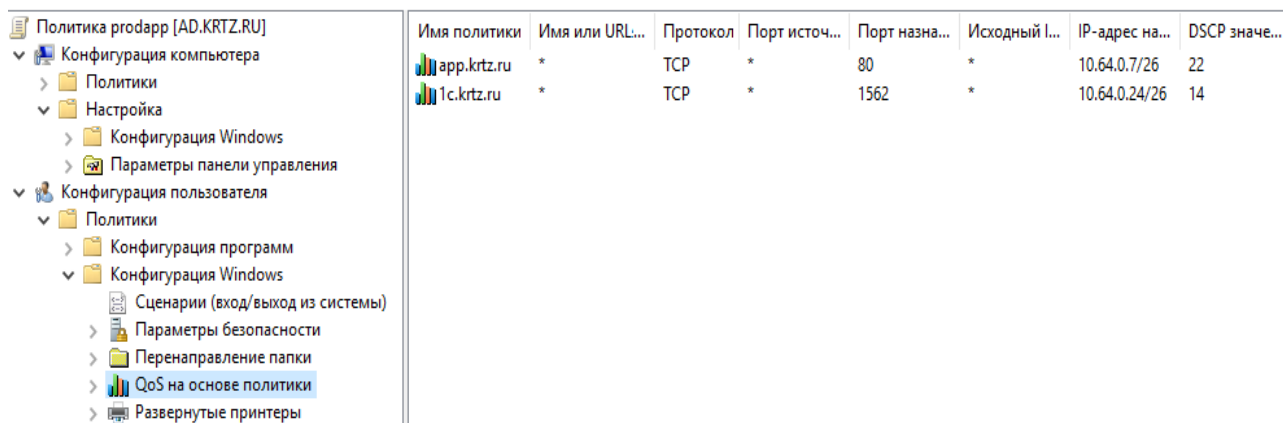
4 Применение разработанной системы на существующей сети передачи данных предприятия

4.1 Применение разработанных правил на сервере блока контроля

В первую очередь для реализации системы необходимо создать правила для уровня приложений, то есть опеределить приоритеты для пакетов данных с помощью технологии QoS.

С помощью групповых политик описанных в разделе 3.3 для всех пользователей домена были созданы правила, определяющие значение DSCP для производственных приложений (рисунок 10):

- для сервера производственных приложений APP определён класс обслуживания AF23 со значением DSCP равным 22;
- для приложений сервера 1C определён класс обслуживания AF13 со значением DSCP равным 14.



Имя политики	Имя или URL...	Протокол	Порт источ...	Порт назна...	Исходный I...	IP-адрес на...	DSCP значе...
app.krtz.ru	*	TCP	*	80	*	10.64.0.7/26	22
1c.krtz.ru	*	TCP	*	1562	*	10.64.0.24/26	14

Рисунок 10 – Настройка групповых политик

Результат применения групповых политик на примере одного из пользователей сети изображён на рисунке 11.

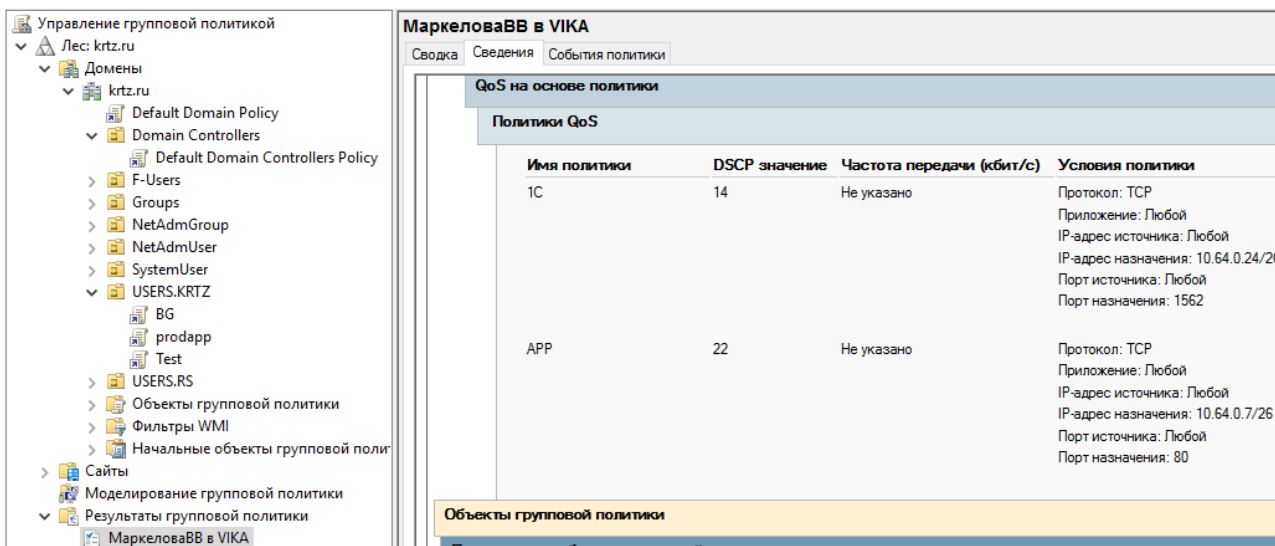


Рисунок 11 – Результат применения QoS на основе групповой политики

Для проверки применения разработанного правила трафик рабочей станции был перехвачен с помощью ранее упомянутого анализатора трафика Wireshark.

На рисунке 12 отображён захваченный пакет от пользовательской станции с IP-адресом 10.32.0.9 до сервера приложений 10.64.0.7, в котором можно увидеть, что значение DSCP приняло значение 22 (AF23). В обратном направлении от сервера к рабочей станции значение DSCP принимает такое же значение, так как групповые политики применены и к серверу.

No.	Time	Source	Destination	Protocol	Length	Info
1486...	58.624452	10.32.0.9	10.64.0.7	TCP	54	59459 → 80 [ACK] Seq=6495 Ack=333316 Win=529920 Len=0
1486...	58.624578	10.64.0.7	10.32.0.9	TCP	1514	80 → 59459 [ACK] Seq=333316 Ack=6495 Win=65536 Len=1460


```

> Frame 148684: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: AsustekC_c8:b2:84 (18:31:bf:c8:b2:84), Dst: IETF-VRRP-VRID_32 (00:00:5e:00:01:32)
> Internet Protocol Version 4, Src: 10.32.0.9, Dst: 10.64.0.7
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x58 (DSCP: AF23, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x686a (26730)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.32.0.9
    Destination: 10.64.0.7
  > Transmission Control Protocol, Src Port: 59459, Dst Port: 80, Seq: 6495, Ack: 333316, Len: 0
  
```

Рисунок 12 – Захваченный пакет, следующий от рабочей станции до сервера приложений

Для сервера приложений 1С заваченные пакеты примут значение DSCP равным 14 (AF13) (рисунок 13).

No.	Time	Source	Destination	Protocol	Length	Info
72636	29.275112	10.32.0.9	10.64.0.24	TCP	5134	53141 → 1562 [PSH, ACK] Seq=8193 Ack=1 Win=252 Len=5080
72637	29.275578	10.64.0.24	10.32.0.9	TCP	60	1562 → 53141 [ACK] Seq=1 Ack=2921 Win=256 Len=0

> Frame 72636: 5134 bytes on wire (41072 bits), 5134 bytes captured (41072 bits) on interface 0
> Ethernet II, Src: AsustekC_c8:b2:84 (18:31:bf:c8:b2:84), Dst: IETF-VRRP-VRID_32 (00:00:5e:00:01:32)
▼ Internet Protocol Version 4, Src: 10.32.0.9, Dst: 10.64.0.24
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x38 DSCP: AF13 ECN: Not-ECT
Total Length: 5120
Identification: 0x153d (5437)
> Flags: 0x4000, Don't fragment
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 10.32.0.9
Destination: 10.64.0.24
> Transmission Control Protocol, Src Port: 53141, Dst Port: 1562, Seq: 8193, Ack: 1, Len: 5080
> Data (5080 bytes)

Рисунок 13 – Захваченный пакет, следующий от рабочей станции до сервера приложений 1С

С помощью общего конфигурационного файла заданы настройки QoS. А именно значение DSCP для голосовых пакетов установлено равным 46 (класс обслуживания EF), а для SIP-пакетов, отвечающих за установление сессии голосового звонка – 26 (класс обслуживания AF31).

Изменения в конфигурационном файле изображены на рисунке 14.

```
y000000000053.cfg x
240  ### QoS Settings ###
241
242  static.network.qos.audiotos = 46 //DSCP для голосовых пакетов
243  static.network.qos.signaltos = 26 //DSCP для SIP пакетов
```

Рисунок 14 – Изменения в конфигурационном файле для IP-телефонов

Результат применения изменений в конфигурационном файле можно увидеть в веб-интерфейсе одного из пользовательских телефонов и изображён на рисунке 15.

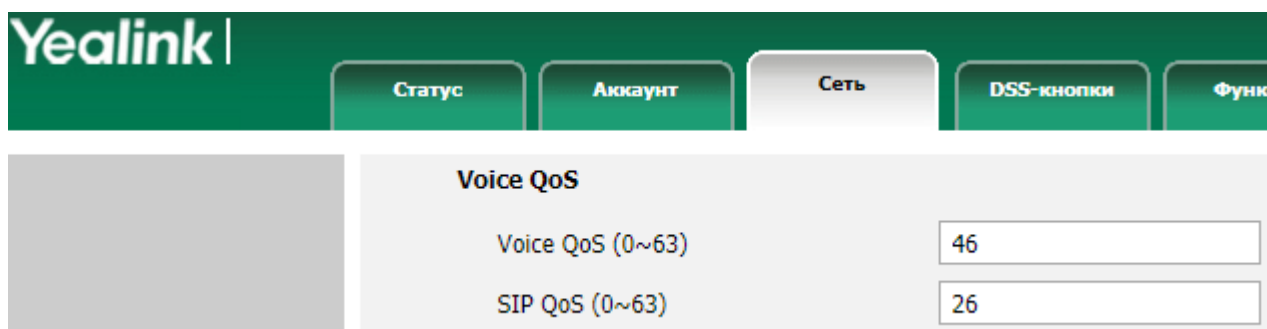


Рисунок 15 – Веб-интерфейс IP-телефона пользователя

Для проверки применения изменений трафик телефона был перехвачен с помощью трафика Wireshark.

На рисунке 16 отображён захваченный пакет от телефона с IP-адресом 10.48.0.20 до АТС 10.48.0.2, в котором можно увидеть, что значение DSCP приняло значение 46 (EF). В обратном направлении от телефонной станции к телефону значение DSCP принимает такое же значение.

No.	Time	Source	Destination	Protocol	Length	Info
2849...	111.325891	10.48.0.2	10.48.0.20	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6CDF307E, Seq=29955, Time=1066133805
2849...	111.336723	10.48.0.20	10.48.0.2	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6BFBF914, Seq=17152, Time=2744320


```

> Frame 284992: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0
> Ethernet II, Src: YealinkX_13:a0:85 (80:5e:c0:13:a0:85), Dst: IETF-VRRP-VRID_47 (00:00:5e:00:01:47)
v Internet Protocol Version 4, Src: 10.48.0.20, Dst: 10.48.0.2
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xb8 DSCP: EF PHB, ECN: Not-ECT
    Total Length: 200
    Identification: 0x0000 (0)
  > Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x24f8 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.48.0.20
    Destination: 10.48.0.2
  > User Datagram Protocol, Src Port: 12484, Dst Port: 28682
  > Real-Time Transport Protocol
  
```

Рисунок 16 – Захваченный пакет, следующий от IP-телефона до телефонной станции

По необходимости системный администратор может изменять настраиваемые значения DSCP. Все изменения вступают в силу сразу же с небольшой задержкой, связанной с программно-аппаратной частью устройств.

4.2 Исследование сети передачи данных

Для анализа качества сети необходимо поставить несколько экспериментов. В результате исследования метрик качества сети в разделе 2.1 в качестве характеристики для исследования выбрана средняя круговая задержка и максимальная задержка.

Цель исследования – измерить и проанализировать метрики качества сети до применения разработанной системы и после применения.

В первую очередь проведено исследования без применения системы на сети. Каждому из классов обслуживания был назначен приоритет равным нулю (Best Effort). Затем произведён захват трафика с пользовательских устройств в различное время и вычислена средняя задержка и максимальная задержка за время измерения.

Данные об испытываемой задержке пакетов без применения разработанной системы приведены в таблице 4.

Таблица 4 – Значения параметров для классов обслуживания до применения разработанной системы

Наименование показателя	Значения показателя		
	Класс 1	Класс 2	Класс 3
Приоритет	0	0	0
Максимальная задержка пакетов, мс	178,608	630,262	237,607
Средняя задержка пакетов, мс	19,981	19,998	11,05

Согласно таблице 4, у класса 1 (IP-телефония), чувствительного к задержке пакетов, средняя задержка выше, чем у класса 3 (поток видео на рабочей станции), и это отражается на качестве телефонной связи. Соответственно, существует возможность использовать выделенные ресурсы канала для класса 3 для снижения задержки класса 1 и класса 2 (производственные приложения).

Далее на сети был применен разработанный метод. Классам 1 и 2 были назначены приоритеты QoS в соответствии с категорией приложений в разделе 3.3. И произведён повторный захват трафика в различное время с рабочих станций и вычислена средняя задержка и максимальная задержка за время измерения.

Данные об испытываемой задержке пакетов с применением разработанной системы приведены в таблице 5.

Таблица 5 – Значения параметров для классов обслуживания после применения разработанной системы

Наименование показателя	Значения показателя		
	Класс 1	Класс 2	Класс 3
Приоритет	1	2	3
Максимальная задержка пакетов, мс	30,12	327,926	341,898
Средняя задержка пакетов, мс	18,1819	17,997	13,061

Согласно таблице 5 можно заметить, что для классов 1 и 2 уменьшились показатели средней и максимальной задержек за счёт класса 3.

Но нужно предполагать, что значение этого параметра может меняться в зависимости от топологии сети, передаваемого трафика, оборудования, количества пользователей в сети и так далее, но в целом с применением системы гораздо улучшено качество передачи трафика в сети, чем без него.

В качестве примера рассмотрим динамику задержки голосового трафика для оценки применения системы. Динамика задержки пакетов голосового трафика до назначения приоритета отображена на рисунке 17. Наблюдаются характерные высокие скачки задержки трафика, что негативно влияет на качество разговора абонентов.

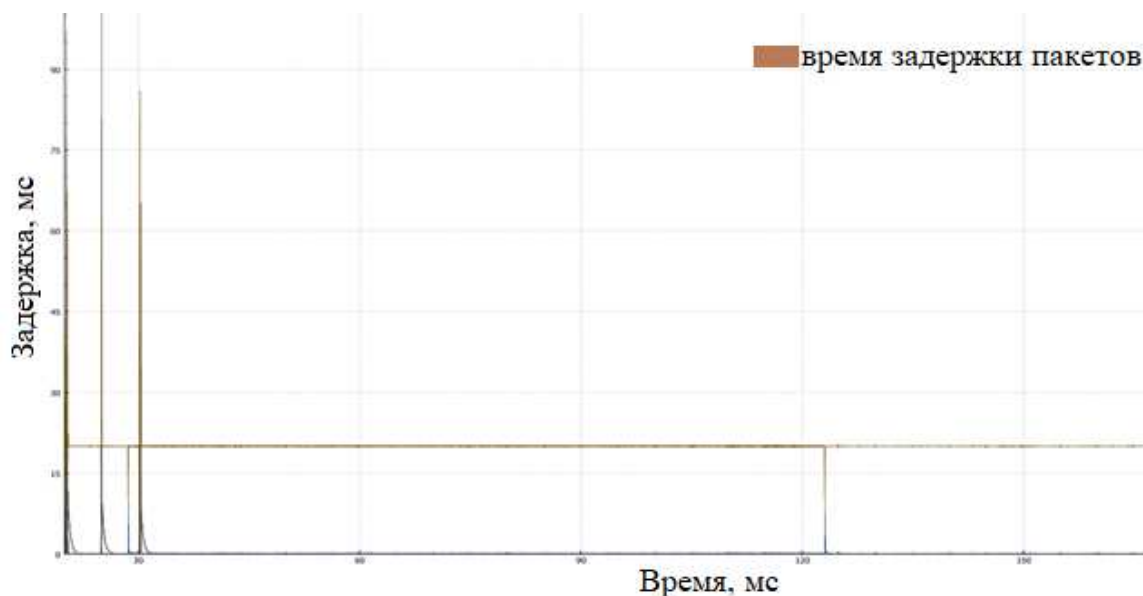


Рисунок 17 – График задержки пакетов голосового трафика до применения метода (ось X – время совершения голосового вызова (с), ось Y – круговая задержка (мс))

Для сравнения изменений на рисунке 18 представлен график задержки голосового трафика после применения метода. Можно заметить на сколько уменьшилось количество пиков больших задержек, а также их значения.

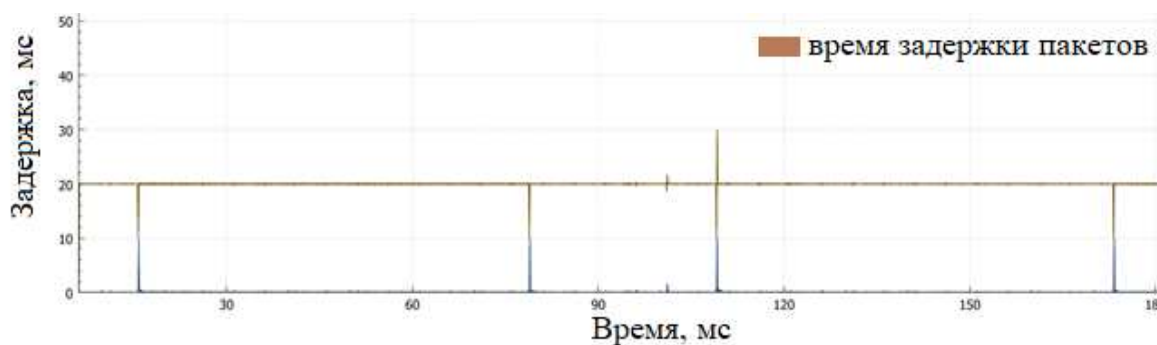


Рисунок 18 – График задержки пакетов голосового трафика после применения метода (ось X – время совершения голосового вызова (с), ось Y – круговая задержка (мс))

В результате экспериментов произведена оценка доли предоставляемых ресурсов в пользу классов 1 и 2. Можно сделать вывод, что для третьего класса услуг доля отдаваемых ресурсов достигает 15% в пользу классов 1 и 2, при превышении этого предела для классов 1 и 2 также нарушатся QoS-ограничения.

Это, в свою очередь, позволит подключить дополнительное число пользователей к тому же сегменту сети. При этом с ростом качества обслуживания запросов пользователей повышается производительность работающих приложений.

4.3 Выводы

В данной главе в соответствии с поставленной задачей были разработаны настройки сервера блока контроля системы в существующей корпоративной сети и проверен результат их применения.

Проведено исследование метрик качества сети до применения разработанной систем и после. Установлено, что применение разработанной системы улучшает показатели метрик качества сети.

ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы была разработана программно-аппаратная система для повышения качества обслуживания корпоративной сети предприятия без увеличения пропускной способности каналов связи.

В первом разделе пояснительной записки было проведён анализ и описание существующей корпоративной сети предприятия. На основании этого были поставлены цель и задачи ВКР, а также сформированы требования для разработки системы и сделан вывод о необходимости разработки системы с наименьшей финансовой стоимостью.

Во втором разделе проведён аналитический обзор методов решения поставленной задачи. Выделены достоинства и недостатки существующих методов решения поставленной цели, предложено решение в соответствие с целью и требованиями ВКР. Также исследованы метрики для оценки качества сети.

В третьем разделе в соответствии с заданием на ВКР была разработана структурная схема предлагаемого решения и схема функциональной структуры системы. Разработанные структурная схема и функциональная схема обеспечили возможность дальнейшей разработки правил для блока приложений, назначаемых блоком контроля.

В четвертом разделе разработаны настройки программного обеспечения сервера блока контроля и проведена проверка применения системы на сети передачи данных. Определена метрика для дальнейшего исследования качества сети. Проведено исследование качества сети до применения разработанной системы и после применения. Сделаны выводы об успешности применения метода на корпоративной сети передачи данных предприятия.

Разработанная система соответствует всем выдвинутым требованиям, а также обладает рядом достоинств, таких как отсутствие финансовых затрат, гибкость и масштабируемость. Система легко конфигурируется в случае, если

потребуется изменить приоритеты работающим приложениям и имеет возможность для увеличения количества приложений.

Результаты работы представлены в формате доклада на Международной молодёжной научной конференций «Перспектив Свободный — 2020».

СПИСОК СОКРАЩЕНИЙ

AD – Active Directory

API – Application Programming Interface

ICMP – Internet Control Message Protocol

IETF – Internet Engineering Task Force

IP – Internet Protocol

OSPF – Open Shortest Path First

PHB – Per-Hop Behavior

PoE – Power over Ethernet

QoS – Quality of Service

RTT – Round Trip Time

SDN – Software-Defined Networking

SIP – Session Initiation Protocol

SPF – Small Form-factor Pluggable

TFTP – Trivial File Transfer Protocol

VLAN – Virtual Local Area Network

VoIP – Voice over Internet Protocol

АТС – автоматическая телефонная станция

ВКР – выпускная квалификационная работа

ВТ – Вычислительная техника

ИКИТ – Институт космических и информационных технологий

ОС – операционная система

СКД – система контроля доступом

СФУ – Сибирский федеральный университет

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Маркелова, В. В. Оптимизация качества обслуживания существующей корпоративной сети / В. В. Маркелова // Проспект Свободный. – 2020. – №3.
2. Официальный сайт АО «НПП «Радиосвязь» [Электронный ресурс] : информация о предприятии. – Режим доступа : <http://кртз.рф>
3. Ethernet-коммутаторы агрегации серии MES33xx, версия ПО 4.0.13. Техническое описание. – Новосибирск : ООО «Предприятие «ЭЛТЕКС», 2020. – 4 с.
4. Коммутаторы магистрального уровня, коммутаторы уровня агрегации, коммутаторы уровня доступа MES53xx, MES33xx, MES35xx, MES23xx. Руководство по эксплуатации, версия ПО 4.0.13. – Новосибирск : ООО «Предприятие «ЭЛТЕКС», 2020. – 337 с.
5. Гибридная платформа SMG-2016 с функциями IP-АТС. Техническое описание. – Новосибирск : ООО «Предприятие «ЭЛТЕКС», 2020. – 5 с.
6. YeaLink T Series IP Phone. Administration Guide. – Xiamen, China : «YeaLink Network Technology», 2018. – 662 с.
7. ITGLOBAL.COM [Электронный ресурс] : корпоративный блог о Managed IT, облачных технологиях и Hi-Tech новостях, которые имеют непосредственное влияние на бизнес. – Электрон. журн. – Москва, 2019. – Режим доступа: <https://itglobal.com>
8. LinkMeUp [Электронный ресурс] : научно-популярный блог. – Электрон. журн. – Москва, 2018. – Режим доступа: <https://linkmeup.ru>.
9. Пат. RU2643469C2 Российская Федерация, МПК H04L 12/723(2013.01). Способ передачи фреймов Ethernet через программно-конфигурируемые сети (SDN) / А.С. Румянков, М.В. Каминский, С.И. Романов ; патентообладатель Би4Эн Груп Лимитед. – № 2015139531 ; заявл. 31.05.2016; опубл. 01.02.2018, Бюл. N 4. – 6 с.

10. Маньков В. А., Краснова И. А. Алгоритм динамической классификации потоков в мультисервисной SDN-сети //Т-Comm-Телекоммуникации и Транспорт. – 2017. – Т. 11. – №. 12.


11. Гольштейн Б. С., Пинчук А. В., Суховицкий А. Л. IP-телефония (третье издание). М.: Радио и связь, 2006. -336 с.: ил. ISBN 5-256-01585-0

12. Davidson J., Peters J., Bhatia M. Voice over IP fundamentals. – Cisco press, 2006.

13. Администрирование АТС. Техническое описание [Электронный ресурс] : Руководство по эксплуатации. – Москва : ЗСХ, 2019. – Режим доступа: <https://www.3cx.ru/docs/manual/pbxmanagement.html>

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий
институт
Вычислительная техника
кафедра

 УТВЕРЖДАЮ
Заведующий кафедрой
О. В. Непомнящий
подпись инициалы, фамилия
«__» _____ 2020 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Настройка и оптимизация качества обслуживания
корпоративной сети предприятия
тема

09.04.01 Информатика и вычислительная техника
код и наименование направления

09.04.01.05 Сети ЭВМ и телекоммуникации
код и наименование магистерской программы


Научный
руководитель


подпись, дата

доцент, канд.техн.наук
должность, ученая степень

Н.Ю.Сиротина
инициалы, фамилия

Выпускник


подпись, дата

В.В.Маркелова
инициалы, фамилия


Рецензент


подпись, дата

нач. ИВЦ АО
«НПП «Радиосвязь»
должность, ученая степень

М.В.Дибров
инициалы, фамилия

Нормоконтролер


подпись, дата

Н.Ю.Сиротина
инициалы, фамилия

Красноярск 2020