ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЁННОЕ ВОЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ АКАДЕМИЯ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ОХРАНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

На правах рукописи

МИРОНОВ ОЛЕГ ЮРЬЕВИЧ

РАЗРАБОТКА И ИССЛЕДОВАНИЕ АЛГОРИТМОВ ДИНАМИЧЕСКОГО РЕЗЕРВИРОВАНИЯ КАНАЛЬНОГО РЕСУРСА ЗАЩИЩЕННЫХ КОРПОРАТИВНЫХ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ

Специальность 05.12.13 – Системы, сети и устройства телекоммуникаций

Диссертация на соискание ученой степени

кандидата технических наук

Научный руководитель:

кандидат технических наук, доцент

Лебеденко Евгений Викторович

Орёл – 2019 г.

Аннотация

Современные защищенные корпоративные мультисервисные сети связи (ЗКМСС) выполняют задачи обеспечения гарантированного качества обслуживания информационных сервисов реального времени, при этом защищенное взаимодействие пользователей между собой и с информационными ресурсами обеспечивается путем построения их на основе технологии VPN с использованием шифрования данных в VPN-шлюзах сети доступа. В то же время применение VPN-шлюзов влечет за собой агрегирование шифрованных потоков данных в VPN-туннелях, что не позволяет реализовать процедуры гибкого управления трафиком отдельных потоков, входящих в состав VPN-туннеля. В результате гарантированное обеспечение требуемого качества обслуживания предоставляемых сервисов достигается за счет резервирования канального ресурса, производимого на стадии планирования сети с применением моделей теории телетрафика, ориентируемых под пиковую возможную нагрузку, что приводит к неэффективному использованию арендуемого канального ресурса транспортного уровня.

Для решения данной проблемы в диссертационной работе разработан комплекс алгоритмов, позволяющих: учесть процесс агрегирования потоков данных сервисов реального времени в VPN-шлюзе сети доступа с точки зрения влияния на параметры трафика передаваемых потоков данных и вычислить требуемый канальный ресурс для гарантированного обеспечения качества обслуживания потоков данных, входящих в состав агрегированного потока VPN-туннеля; определить оптимальный набор допущенных к обслуживанию потоков в условиях возникновения перегрузки с учетом их приоритетов и длительности сеанса; повысить степень использования канального ресурса в условиях штатного функционирования сети доступа (отсутствие перегрузки) за счет перераспределения незадействованного канального ресурса между предоставляемыми инфокоммуникационными сервисами.

Оглавление

Аннотация…..……..2
Введение…..……...….....5
Раздел 1. Методы управления доступом к ресурсам защищенных корпоративных мультисервисных сетей связи……..……14
1.1. Введение…….……..…….…..14
1.2. Принципы построения защищенных корпоративных мультисервисных сетей связи…….……..……...15
1.2.1. Обеспечение безопасности передаваемой информации.……19
1.2.2. Обеспечение требуемого уровня качества обслуживания потоков данных …….……..…….....21
1.3. Анализ существующих математических моделей агрегированного потока данных……..……..……..34
1.4. Исследование влияния процедур функционирования VPN-шлюзов на параметры передаваемого трафика……..…...36
1.5. Постановка научной задачи диссертационного исследования….....45
1.6. Выводы по первому разделу……..……..……...……..48
Раздел 2. Разработка алгоритма динамического резервирования канального ресурса агрегированного потока данных сервисов реального времени……..……..……..……...…….49
2.1. Введение……..……..……..……49
2.2. Исследование применимости существующих математических моделей агрегированного потока данных в защищенной корпоративной мультисервисной сети связи…..……..…..49
2.3. Разработка алгоритма динамического резервирования канального ресурса агрегированного потока данных..……...……..62
2.4. Исследование свойств алгоритма динамического резервирования канального ресурса агрегированного потока данных…….……..….68
2.5. Выводы по второму разделу…..…….……..70

Раздел 3. Разработка алгоритма допуска потоков в транспортную сеть защищенной корпоративной мультисервисной сети связи и исследование его свойств……..……..…….72
3.1. Введение……..……..……..……72
3.2. Выработка и обоснование критериев эффективного использования канального ресурса..……..…….73
3.3. Разработка алгоритма допуска потоков в транспортную сеть защищенной корпоративной мультисервисной сети связи…….83
3.4. Разработка имитационной модели сегмента защищенной корпоративной мультисервисной сети связи……..……..90
3.5. Выводы по третьему разделу…..……103
Раздел 4. Разработка комплекса алгоритмов согласования трафика с VPN-туннелем ……..……..……..……...104
4.1. Введение……..……..……..……..104
4.2. Алгоритм классификации трафика……..……..…….109
4.3. Алгоритм сглаживания трафика ……..……..……111
4.4. Алгоритм управления планировщиком пограничного маршрутизатора……..……..……..…….113
4.5. Оценка времени выполнения процедуры сортировки потоков данных в VPN-шлюзах…..……..……116
4.6. Оценка времени переконфигурирования пограничного маршрутизатора…….……..…….……...120
4.7. Выводы по четвертому разделу…..……124
Заключение…….……125
Список сокращений и условных обозначений…….127
Список литературы…….132
Приложение. Акт использования результатов диссертации……..148

Введение

Актуальность темы исследования. Создание новых и совершенствование существующих защищенных корпоративных мультисервисных сетей связи (ЗКМСС) имеет большое значение для развития телекоммуникационной инфраструктуры систем управления промышленных компаний, организаций, ведомств и органов государственной власти.

Как правило, для таких сетей связи транспортная сеть создается на основе аренды канального ресурса (КР) у операторов Единой сети электросвязи РФ. Применение арендованных каналов связи порождает проблему эффективного использования их пропускной способности в условиях предоставлении пользователям мультисервисных услуг, в частности, таких сервисов реального времени, как IP-телефония, видеотелефония, видеоконференция с требуемым уровнем качества обслуживания (КО). При этом для предоставления данных услуг в качестве базового способа распределения КР используется предоставление каждому сервису полосы пропускания исходя из возможной нагрузки от пользователей всех категорией [5,33].

Другой особенностью ЗКМСС является необходимость обеспечения конфиденциальности и целостности передаваемой информации. Фактически, такие сети представляются множеством защищённых логических соединений (VPN-туннелей), создаваемых VPN-шлюзами (криптомаршрутизаторами), установленными на границе сети доступа и транспортной сети [83,89,123]. Выбор туннельного режима обусловлен возможностью создания закрытого информационного пространства с обеспечением сокрытия сведений об IP-адресах узлов отправителя и получателя, типе транспортного протокола, являющихся наиболее значимыми в отношении понимания структуры взаимодействия узлов. Однако использование подобных механизмов не

позволяет реализовать классификацию и приоритетное обслуживание субпотоков в ядре сети.

Указанные особенности ЗКМСС оказывают существенное влияние на качество предоставляемых услуг. В частности, в условиях динамического добавления абонентских терминалов, не предусмотренных схемой организации сети, возможно возникновение режима перегрузки – блокирования допуска потоков данных в транспортную сеть, в результате чего КР может быть загружен низкоприоритетным трафиком. При этом даже в условиях штатного функционирования таких сетей связи возможны ситуации неэффективного использования КР, зарезервированного для предоставления высокоприоритетных инфокоммуникационных услуг, из-за невозможности перераспределения КР между предоставляемыми сервисами.

Исходя из вышеизложенного, одной из важнейших задач, которые необходимо решить для обеспечения гарантированного уровня качества обслуживания предоставляемых сервисов в ЗКМСС, является оценивание требуемого канального ресурса для обслуживания потоков данных сервисов реального времени с учетом всех указанных особенностей функционирования данных сетей. Решение данной задачи видится в совершенствовании существующих и разработке специализированных алгоритмов динамического резервирования канального ресурса, учитывающих влияние VPN-шлюзов на параметры передаваемого трафика, что нашло свое отражение в данной работе и говорит об актуальности проведенного диссертационного исследования.

Степень разработанности темы. Существующий методологический аппарат моделирования процессов функционирования мультисервисных сетей связи, предложенный в работах Ф.П. Келли, В. Иверсена, С.Н. Степанова, представляет модификацию моделей Эрланга и Энгсета, ориентированных на использование эффективной скорости передачи данных [97]. Существенным ограничением такого подхода является применение фиксированных значений выделяемого КР и использование средних

значений длительности обслуживания заявки, не зависящих от загрузки звена мультисервисной сети связи, что снижает точность получаемых оценок.

Методы динамического распределения КР, предложенные в работах С.Н. Степанова, предусматривают при увеличении интенсивности высокоприоритетных заявок как возможность снижения скорости передачи данных до некоторого минимального значения, так и возможность блокирования предоставляемой инфокоммуникационной услуги. При этом их особенностью является достаточно высокая вычислительная сложность алгоритма перераспределения КР, что позволяет эффективно использовать эти методы на этапе проектирования, а не на этапе оперативного управления сетью связи.

Методы оперативного управления КР, предложенные в работах Л. Георгадиса, Р.Л. Круза, Д. Кларка, А.К. Пареха [118,119,122] и базирующиеся на аппарате теории сетевого исчисления в явном виде не могут быть использованы в VPN-шлюзах сети доступа ЗКМСС, поскольку служебная информация, необходимая для их функционирования, зашифрована, что, в свою очередь, не позволяет идентифицировать отдельные потоки данных и обеспечить их приоритетное обслуживание. Следовательно, эти методы обеспечивают управление КР преимущественно на уровне агрегированных потоков данных и сформированных для них VPN-туннелей. В результате сложившейся ситуации для обеспечении заданного уровня КО передаваемых потоков данных реального времени (ПДРВ) «из конца в конец» применяется распределение имеющегося КР для каждого предоставляемого сервиса на базе архитектуры дифференцированных услуг DiffServ как в сетях доступа, так и в транспортной сети [113]. Анализ механизмов КО данной архитектуры и логики их функционирования, подробно представленный в работах [97,105,106], показал, что они являются статичными и несогласованными между собой.

Подводя итог, можно сделать вывод о том, что в научно-технической области существует актуальная задача реализации максимальной загрузки

дорогостоящего арендуемого КР транспортного уровня ЗКМСС и разработки эффективных алгоритмов, обеспечивающих решение задачи оперативного управления, связанной с оцениванием, резервированием и перераспределением требуемого КР для агрегированных потоков данных, передаваемых в VPN-туннелях.

Объект исследования - система управления потоками данных в VPN-шлюзах сети доступа защищенной корпоративной мультисервисной сети связи.

Предмет исследования - процесс агрегирования потоков данных сервисов реального времени в VPN-шлюзах сети доступа защищенной корпоративной мультисервисной сети связи.

Целью диссертационного исследования является разработка моделей и алгоритмов динамического оценивания, резервирования и перераспределения канального ресурса защищенной корпоративной мультисервисной сети связи, учитывающих процесс агрегирования потоков данных сервисов реального времени в VPN-шлюзах сети доступа и позволяющих обеспечить гарантированный уровень требуемого качества обслуживания предоставляемых сервисов, как в условиях штатного функционирования сети доступа, так и в условиях возникновения перегрузки.

Для достижения заявленной цели в диссертации были решены следующие **задачи:**

1. Проведен анализ существующих принципов построения сетей доступа и транспортной сети ЗКМСС, существующих методов обеспечения КО ПДРВ, исследовано влияние процесса агрегирования потоков данных в VPN-шлюзе на значения таких параметров трафика, как мгновенная пиковая, средняя скорость информационного потока, длина пакетов, средняя задержка и вариация средней задержки для сервисов реального времени.

2. Разработан алгоритм динамического резервирования КР агрегированного потока данных сервисов реального времени, определяющий зависимость объема зарезервированного КР для VPN-туннеля от задержки,

вносимой процессом агрегирования потоков данных сервисов реального времени в процесс обработки пакетов в VPN-шлюзе сети доступа.

3. Разработан алгоритм допуска потоков в транспортную сеть и комплекс алгоритмов классификации и сглаживания трафика, управления планировщиком пограничного маршрутизатора, позволяющие повысить степень использования КР в условиях штатного и нештатного (условия возникновения перегрузки) функционирования сети.

4. Разработана имитационная модель сегмента ЗКМСС в среде моделирования Network Simulator 3 с целью проведения экспериментальных исследований эффективности предложенного комплекса алгоритмов, как для условий возникновения перегрузки, так и для условий ее штатного функционирования.

5. Предложены варианты технической реализации модельно-алгоритмического обеспечения в VPN-шлюзах.

Основные положения, выносимые на защиту:

1. Результаты анализа существующих моделей потоков данных сервисов реального времени показали необходимость учета влияния процесса их агрегирования в VPN-шлюзах сети доступа на значения параметров мгновенной пиковой, средней скорости передачи данных, длины пакетов, средней задержки и вариации средней задержки предоставляемых инфокоммуникационных услуг.

2. Разработанный алгоритм динамического резервирования канального ресурса агрегированного потока данных сервисов реального времени дает возможность учесть влияние задержки, связанной с процессом агрегирования потоков данных в VPN-шлюзах сети доступа защищенной корпоративной мультисервисной сети связи, на объем канального ресурса, распределяемого между множеством VPN-туннелей.

3. Разработанный алгоритм допуска потоков в транспортную сеть обеспечивает учет приоритетов поступающих на обслуживание потоков данных, длительность сеансов сервисов реального времени, способ агрегирования потоков в VPN-шлюзах и уменьшает вероятность потерь

вызовов от приоритетных пользователей. При функционировании сети в условии перегрузки выигрыш (по значению вероятности потерь вызовов) от применения алгоритма может достигать до 30%.

4. Разработанный комплекс алгоритмов согласования трафика с VPN-туннелем совместно с алгоритмом допуска потоков в транспортную сеть дает возможность повысить степень использования канального ресурса: в условиях штатного функционирования сети доступа за счет перераспределения незадействованного канального ресурса между предоставляемыми инфокоммуникационными сервисами, а в условиях возникновения перегрузки за счет решения задачи выбора оптимального набора допущенных к обслуживанию потоков с учетом их приоритетов и длительности сеанса. При отсутствии перегрузки повышение степени использования резервируемого на этапе планирования сети канального ресурса федерального сегмента может составлять до 40 %.

Методы исследования. Для решения задач диссертационного исследования применялись методы теории систем, теории вероятностей и математической статистики, теории сетевого исчисления, теории телетрафика, планирования эксперимента.

Научная новизна.

1. Разработан алгоритм динамического резервирования канального ресурса агрегированного потока данных сервисов реального времени, отличающийся от известных учетом влияния параметров трафика и максимальной допустимой задержки, связанной с процессом агрегирования потоков данных в VPN-шлюзах, на требуемый объем канального ресурса, распределяемого между множеством VPN-туннелей.

2. Разработан алгоритм допуска потоков в транспортную сеть, отличающийся от известных учетом приоритетов поступающих на обслуживание потоков данных, длительности сеансов сервисов реального времени, способа агрегирования потоков в VPN-шлюзах и уменьшением вероятности потерь вызовов от приоритетных пользователей.

3. Разработан комплекс алгоритмов согласования трафика с VPN-туннелем, позволяющих совместно с алгоритмом допуска потоков в транспортную сеть повысить степень использования канального ресурса: в условиях штатного функционирования сети доступа за счет перераспределения незадействованного канального ресурса между предоставляемыми инфокоммуникационными сервисами, а в условиях возникновения перегрузки за счет решения задачи выбора оптимального набора допущенных к обслуживанию потоков с учетом их приоритетов и длительности сеанса.

Теоретическая и практическая значимость работы. Теоретическая значимость работы состоит в совершенствовании методов динамического управления канальным ресурсом транспортной сети, арендуемой у операторов Единой сети электросвязи, на основе учета процесса агрегирования потоков данных реального времени в VPN-шлюзах сети доступа защищенной корпоративной мультисервисной сети связи.

Практическая значимость работы заключается в доведении разработанного комплекса алгоритмов до уровня программного обеспечения, что подтверждается патентом на изобретение № 2601604 от 14.10.2016 г. «Способ сглаживания приоритетного трафика данных и устройство для его осуществления», а также его использовании в составе системы управления потоками VPN-шлюза сети доступа мультисервисной сети связи ПАО АКБ «Авангард», что подтверждается соответствующим актом реализации.

Степень достоверности и апробация результатов.

Достоверность и обоснованность полученных результатов подтверждается: корректно спланированными экспериментами, применением известных методов исследования, адекватных природе изучаемых процессов и явлений, непротиворечивостью и воспроизводимостью результатов, полученных теоретическим путем и результатами имитационного моделирования.

Основные результаты докладывались и обсуждались на Международной научно-практической конференции «ИНФОКОМ-2013»

(Ростов-на-Дону, 2013), VIII Международной молодежной научно-практической конференции «ИНФОКОМ-2015» (Ростов-на-Дону, 2015), XX Всероссийской научно-технической конференции «Научная сессия ТУСУР – 2015», (Томск, 2015), XXI, XXII Международной открытой научной конференции «Современные проблемы информатизации» (Воронеж, 2015, 2017), XII Международной отраслевой научно-технической конференции «Технологии информационного общества», (Москва, 2018).

Всего по теме диссертации опубликовано 16 научных работ, из них 4 – в научных изданиях, включенных в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук: «Информационные системы и технологии» – 1 [70]; «Телекоммуникации» – 1 [74], «Научные ведомости БелГУ» – 1 [64], «T-Comm. – Телекоммуникации и транспорт» – 1 [62], в 7 сборниках тезисов докладов [63,67,68,69,75,76,77], в патенте на изобретение [73], в 4-х зарегистрированных программах для ЭВМ [65,66,71,72].

Во введении обоснована актуальность выбранной темы диссертационной работы, сформулирована ее цель и частные научные задачи, необходимые для достижения цели исследования. Сформулированы научные положения, выносимые на защиту, представлена их научная новизна, теоретическая и практическая значимость, приведены сведения о публикациях, апробациях и реализации полученных результатов.

В первом разделе диссертационной работы проведен анализ предметной области. Описана и доказана существующая техническая особенность механизмов обеспечения КО архитектуры интегрированного обслуживания IntServ [115] в сети доступа и дифференцированного обслуживания DiffServ в транспортной сети из-за применения VPN-шлюзов в туннельном режиме. Проведен анализ существующих и известных способов оценивания параметров агрегированного потока данных, в результате которого произведен выбор подхода на основе оценивания эффективной

скорости передачи данных, за счет чего обеспечивается требуемый уровень КО для предложенной нагрузки. Обосновано использование математического аппарата детерминированной теории сетевых исчислений [39,114] для этой цели. В формализованном виде представлена научная задача исследования. Определены ограничения и допущения, применяемые при ее решении.

Второй раздел посвящен аналитическому описанию функционирования VPN-шлюзов, применяемых в ЗКМСС. Статистическая обработка результатов эксперимента позволила определить влияние процедуры шифрования данных на параметры передаваемого трафика: мгновенную пиковую и среднюю скорости передачи данных, длины генерируемых пакетов. Получены выражения, позволяющие оценить требуемый КР для агрегированного потока данных при использовании существующих VPN-шлюзов отечественного производства в ЗКМСС.

В третьем разделе диссертации на основании полученных зависимостей разрабатывается алгоритм допуска потоков данных реального времени в транспортную сеть ЗКМСС и исследуются его свойства. Проведен анализ существующих подходов к решению оптимизационной задачи повышения степени использования КР при гарантированном обеспечении КО ПДРВ. С целью оценивания эффективности разработанного модельно-алгоритмического обеспечения была создана имитационная модель сегмента ЗКМСС в среде сетевого моделирования Network Simulator 3 с реализованной функцией динамического управления допуском приоритетных ПДРВ и резервирования канального ресурса.

В **четвертом разделе** предложены алгоритмы, обеспечивающие согласование поступающих потоков данных с VPN-туннелями (traffic conditioning), применение которых позволяет гибко использовать пропускную способность арендуемого канала связи за счет переконфигурирования планировщика пограничного маршрутизатора при изменении предложенной нагрузки. В заключении приводятся основные выводы по результатам диссертации и формулируются направления дальнейших исследований в предметной области.

Раздел 1

Методы управления доступом к ресурсам защищенных корпоративных мультисервисных сетей связи

1.1. Введение

На существующем этапе информационного развития общества решение экономических задач крупных организаций невозможно без внедрения в технологический процесс мультисервисных сетей связи [95,97]. К достоинствам таких сетей относится обеспечение оперативного управления технологическими процессами, удаленный доступ клиентов корпоративной сети к серверному оборудованию, базам данных, распределение функциональных задач между объектами организации относительно их подчиненности. Предоставление большинства услуг (сервисов) в таких сетях обеспечивается в защищенном виде, для чего применяются средства криптографической защиты информации (СКЗИ) (в дальнейшем VPN-шлюзы).

Применение VPN-шлюзов ограничивает возможность динамического резервирования КР транспортного уровня в связи с шифрованием полезной информации, передаваемой в протокольных блоках специализированных для этой цели сигнальных протоколов. Наиболее распространенным таким протоколом является сигнальный протокол резервирования ресурсов RSVP (Resource Reservation Protocol) [116].

Преодоление сложившейся технической особенности заключается в совершенствовании протокола RSVP в направлении поддержания шифрования (протокол IPSec) на сетевом уровне модели ЭМВОС. Однако вышеизложенная проблема не была решена полностью, поскольку минимально возможным потоком данных, идентифицируемым по служебному полю открытого заголовка IPSec на пограничных узлах коммутации стали потоки транспортного уровня. Управлять КР по

количественному составу таких потоков при предоставлении мультимедийных услуг, одновременно поддерживающим в течение сеанса большое количество различных транспортных потоков, с технической точки зрения пока не представляется возможным. В данной работе в связи с применением в ЗКМСС VPN-шлюзов в туннельном режиме и установлением шифрованных логических соединений – VPN-туннелей разрешение данной технической особенности видится в определении требуемого для обслуживания каждого VPN-туннеля КР на этапе их установления и его резервирования, что позволит обеспечить требуемый уровень КО предаваемых потоков данных и избежать их взаимного влияния.

1.2. Принципы построения защищенных корпоративных мультисервисных сетей связи

На примере существующих отечественных и зарубежных аналогов построение и развертывание ЗКМСС, как правило, базируется на концептуальных положениях сетей следующего поколения NGN, где в качестве технологической основы передачи пользовательского трафика выступает технология пакетной передачи данных – IP/MPLS [31,112,127].

Выбор архитектуры NGN обусловлен прежде всего возможностью предоставления услуг реального времени на базе IP-технологии, где логическая связность терминального оборудования осуществляется по принципам «точка-точка», «точка–многоточка», «многоточка–многоточка», а также значительным снижением затрат на развертывание и обслуживание линейных трактов. При таком подходе архитектура ЗКМСС может быть представлена четырьмя основными функциональными уровнями: уровнем доступа, транспортным уровнем, уровнем управления и уровнем услуг с определенными задачами и функциями, возложенными на них [70,130].

В рамках настоящего исследования ограничимся следующими наиболее часто предоставляемыми услугами ЗКМСС, которые, по сути, являются функциональным наполнением уровня услуг, а их приоритет

соответствует очередности предоставления в условиях недостаточности КР, т.е. при возникновении перегрузки сети.

Таблица 1.1 – Перечень предоставляемых услуг в защищенных корпоративных мультисервисных сетях связи

Краткое назначение	Наименование предоставляемой услуги	Приоритет услуги	Терминал
Видеотелефония (в т.ч. видео-конфернцсвязь)	Система защищенной видеосвязи корпоративной мультисервисной сети связи	Высокий	Терминал ЗВС
IP-телефония	Телефония на базе протокола IP	Высокий	IP-телефон
Видеонаблюдение	Организация видеонаблюдения за объектами ЗКМСС	Высокий	Видеокамера
Телевидение высокой четкости	Телевизионная трансляция высокой четкости на базе IP-протокола	Средний	Телевизор (ПК)
Электронный документооборот	Система защищенного корпоративного электронного документооборота	Средний	ПК
WWW	Предоставление выхода в интернет	Низкий	ПК

Уровень доступа ЗКМСС представляет собой системно-сетевую инфраструктуру, состоящую из абонентских линий, узлов доступа, систем передачи и агрегации трафика. Данный уровень, как правило, базируется на оборудовании, принадлежащем корпорации, в результате чего задачи по настройке оборудования, поддержания работоспособного состояния уровня системы возлагаются на собственные структурные ИТ-подразделения [82,120].

Роль **транспортного уровня** ЗКМСС выполняет транспортная сеть связи, предназначенная для передачи агрегированных потоков данных между территориально-распределенными филиалами (объектами организации) с требуемым уровнем КО, регламентированным рекомендациями МСЭ-Т Y.1540, Y. 1541 [78, 131,132,133].

Для обеспечения защиты передаваемой информации в ЗКМСС применяются VPN-шлюзы. Проведенный в [88] анализ показал, что данные средства могут функционировать в одном из двух режимах: туннельном или

транспортном. Отмечено, что создание защищенного информационного пространства корпорации за счет использования VPN-шлюза в туннельном режиме позволяет не только осуществить управление КР, приоритезацию трафика и его маршрутизацию, реализовать функцию контроля передаваемых потоков и их фильтрацию, но и существенно снизить экономические затраты корпорации на создание защищенной инфокоммуникационной системы. В этой связи в последующем одним из ограничений при проведении исследований выступает применение VPN-шлюзов в туннельном режиме. В обобщенном виде схема построения ЗКМСС представлена на рисунке 1.1.

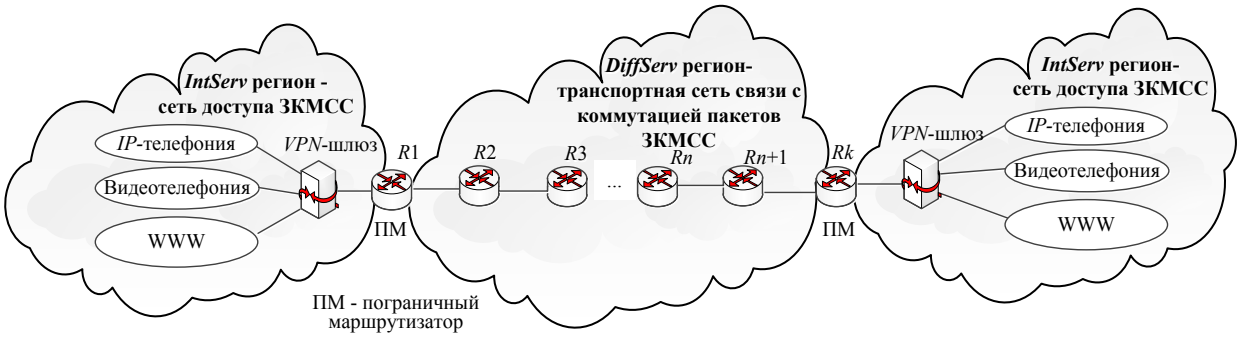


Рисунок 1.1 – Обобщенная схема построения защищенной корпоративной мультисервисной сети связи

Несмотря на перечисленные достоинства туннельного режима, наиболее значимыми недостатками, присущими ему, является агрегирование шифрованных потоков данных в VPN-туннелях, шифрование полезных данных сигнальных протоколов, например RSVP, архитектуры IntServ [90,136]. На пограничных маршрутизаторах (ПМ) транспортной сети идентификация вида предоставляемой услуги, количества установленных сеансов связи, внутренних IP-адресов отправителя и получателя становится невозможной, за исключением идентификации VPN-туннелей по внешним (открытым) IP-адресам VPN-шлюзов.

Вышеизложенные особенности построения и эксплуатации ЗКМСС **не позволяют реализовать процедуры гибкого управления трафиком и**

загрузкой арендуемых каналов связи, зная количественный состав активных потоков данных и транслируемые значения параметров передаваемого трафика.

Структурная схема ЗКМСС ПАО АКБ «Авангард», изображенная на рисунке 1.2., в дальнейшем **выступает технологической основой для реализации, апробации полученных результатов.**

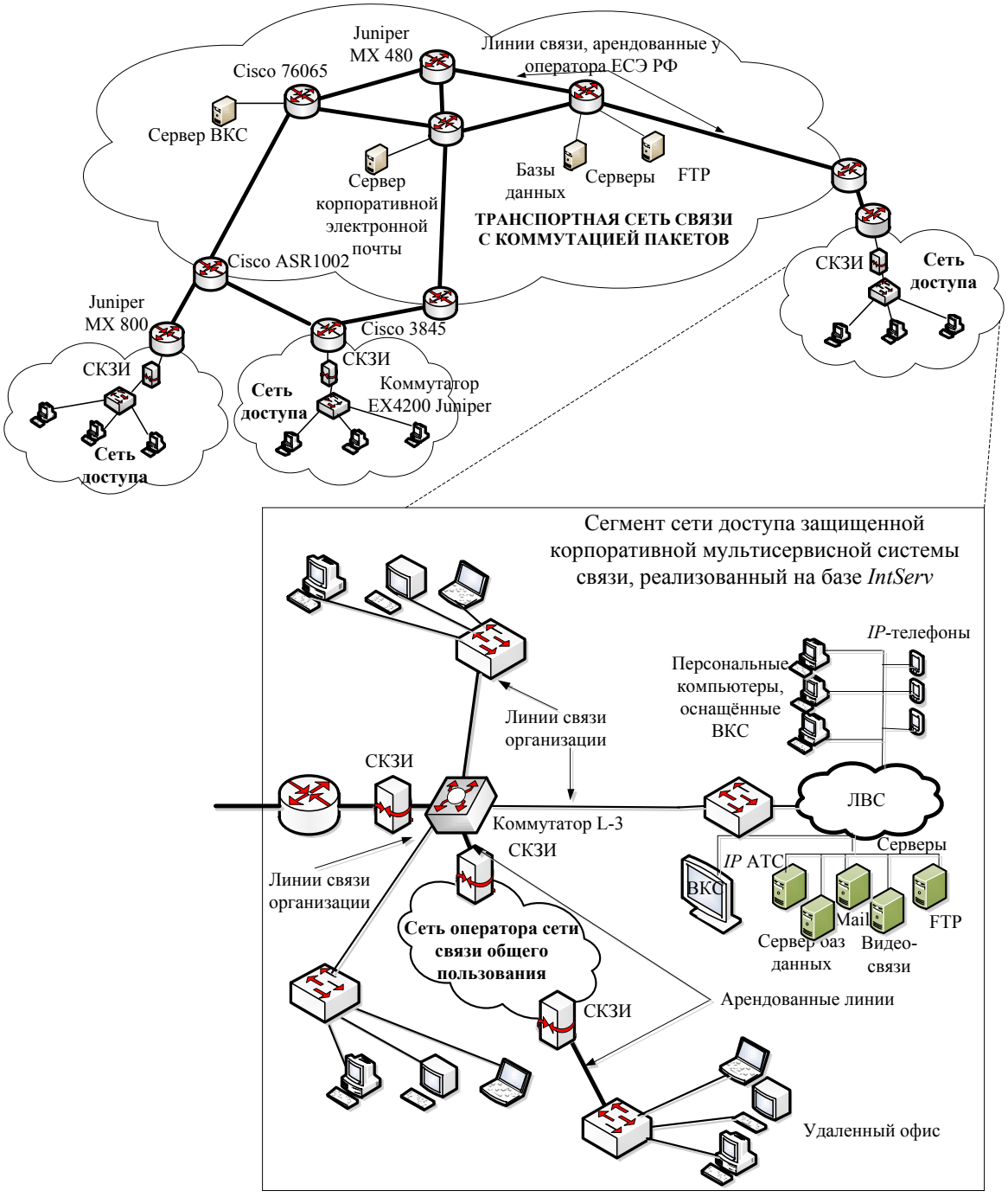


Рисунок 1.2 – Структурная схема защищенной корпоративной мультисервисной сети связи

1.2.1. Обеспечение безопасности передаваемой информации

Наиболее распространенным протоколом сетевого уровня, позволяющим реализовать функции конфиденциальности и целостности циркулирующей информации, защиты серверного оборудования от внешних атак и воздействий, контроля передаваемой из защищаемой сети доступа информации, приоритезации потоков и управления доступом в сеть, является протокол IPSec [128]. В состав данного протокола в настоящее время входит около 20 стандартов и 18 рекомендаций RFC, касающихся реализации способов шифрования, аутентификации и обеспечения защиты передаваемых по открытой сети IP-пакетов.

Основные протоколы и стандарты IPSec:

Internet KeyExchange (IKE) – протокол (стандарт), обеспечивающий аутентификацию сторон, согласование параметров ассоциаций защиты (SA), а так же выбор ключей шифрования;

Authentication Header (AH) – протокол (стандарт), обеспечивающий аутентификацию пакетов и выявление их воспроизведения;

Encapsulating Security Payload (ESP) – протокол (стандарт), обеспечивающий конфиденциальность, аутентификацию источника и целостность данных, а также сервис защиты от воспроизведения пакетов;

Hashed Message Authentication Code (HMAC) – протокол (стандарт) аутентификации сообщений с использованием хэш функций;

Data Encryption Standard (DES), 3DES, AES – стандарты шифрования данных.

В IPSec используются две базы данных – SPD (Security Policy Database), куда записываются правила обеспечения безопасности: IP-адреса узлов отправителя и получателя, идентификаторы пользователей, уровень чувствительности данных, протокол транспортного уровня, протокол IPSec, порты отправителя и получателя, класс IPv6, метка потока IPv6, тип сервиса IPv4 и SADB (Security Association Database), где хранятся данные об активных ассоциациях безопасности: алгоритмы аутентификации и

шифрования и их секретные ключи, параметры обмена несекретными ключами, данные о политиках маршрутизации и фильтрации трафика.

С целью создания закрытого информационного пространства циркулирующая информация подлежит преобразованию согласно функциям протокола ESP, а в отдельных случаях и совместному преобразованию AH/ESP.

Основным отличием ESP от AH является тот факт, что ESP инкапсулирует зашифрованные данные, то есть включает в себя и заголовок, и концевик. Основной функцией ESP является защита трафика от несанкционированного просмотра, в то время как защита от изменения посредством аутентификации является опциональной. Однако ESP аутентифицирует только полезную нагрузку и ESP заголовок, в то время как AH аутентифицирует и большинство полей в стандартном IP-заголовке.

Протокол ESP может функционировать в двух режимах: транспортном и туннельном. Транспортный режим используется преимущественно для защиты соединений «из конца в конец», в результате чего производится инкапсуляция поля данных дейтограммы. Исходный IP-заголовок формируется на сетевом уровне узла отправителя, в результате чего все поля заголовка, за исключением поля «следующий протокол – nexthdr», остаются неизмененными. Инкапсулированное поле данных протоколов верхних уровней шифруется, и в случае необходимости к нему добавляется так называемый «концевик», состоящий из информационного заполнения (padding) с указанием его длины, а также протокола следующего уровня.

Функционирование ESP в туннельном режиме предназначено для создания и поддержания сервиса виртуальных частных сетей, когда производится полное перекрытие аутентификационного заголовка и инкапсулированного поля данных. **В данном режиме исходные IP-пакеты узла отправителя шифруются полностью и инкапсулируются в новые IP-пакеты, а в конце пакета также добавляется «концевик».** Это позволяет не только скрыть IP-адреса узлов отправителя и получателя, но и реализовать функции межсетевого экрана, поскольку обработка пакетов

производится на входе (выходе) защищаемых сетей в сетевых шлюзах. В результате такого преобразования информации перехватчику, находящемуся «по середине», становятся не доступны сведения о том, что два сетевых объекта соединены в VPN, которые являются наиболее значимыми в отношении понимания структуры взаимодействия узлов. При таком подходе даже тип транспортного протокола (TCP, UDP или ICMP) оказывается скрыт от постороннего.

Несмотря на перечисленные достоинства туннельного режима, наиболее значимыми недостатками, присущими ему, является **агрегирование шифрованных потоков данных в криптотуннелях, шифрование полезных данных сигнального протокола RSVP архитектуры IntServ.** На пограничных маршрутизаторах транспортной сети ЗКМСС идентификация вида предоставляемой услуги, количества установленных сеансов связи, внутренних IP-адресов терминалов отправителя и получателя становится невозможной, за исключением идентификации VPN-туннелей по внешним (открытым) IP-адресам VPN-шлюзов.

1.2.2. Обеспечение требуемого уровня качества обслуживания потоков данных

В настоящее время специально созданными международными институтами телекоммуникационных инженеров (рабочими группами) сформировано три основных архитектуры построения сети: архитектура интегрированных услуг (IntServ), архитектура дифференцированных услуг (DiffServ), архитектура многопротокольной коммутации по меткам (MPLS) с возможностью управления (инжиниринга – Traffic Engineering) трафиком, а также реализации маршрутизации с обеспечением заданных параметров КО.

Уровень КО в ЗКМСС рассматривается с позиции рекомендации Е. 800 «Термины и определения по инженерии трафика», в которой вводиться понятие уровень обслуживания (GoS, Grade of Service). Под GoS

понимается совокупность технических параметров, характеризующих соответствие некоторой группы ресурсов поступающей нагрузке при определенных условиях [53,109]. В отличие от КО на уровне соединения, характеризующего степень удовлетворения пользователя, параметры GoS являются подмножеством параметров КО, описывающих только производительность сетевой инфраструктуры. Сетевые характеристики и требования к показателям в IP-сетях определены в рекомендациях ITU-Y.1540 и Y.1541.

Вариация задержки (джиттер) оказывает негативное влияние на работоспособность приложений реального времени. Одним из способов, широко используемым для компенсации джиттера является буферизация получаемых пакетов перед воспроизведением информации, так называемое отложенное воспроизведение. В том случае, когда каждому пакету потока обеспечивается гарантированная задержка передачи пакетов, джиттер не превышает допустимого значения. В таком случае, если на каждом сетевом элементе ЗКМСС обеспечить задержку обрабатываемых пакетов не превышающую некоторое верхнее значение, можно обеспечить гарантированный уровень КО предоставляемых сервисов.

Суммируя вышеизложенное, в дальнейшем **определение уровня КО каждого потока данных будем производить по своевременности доставки пакета**, оцениваемой **достижимой максимальной сквозной задержкой пакета *i*-го потока данных «из конца в конец» s-го класса из множества S классов трафика** $t(\text{дост})$, **не превышающей требуемого значения** $t(\text{треб})$, определяемого рекомендацией Y.1541:

$$\forall s \in \{S\}, \forall i \in \{1,...,n\} \;\; t(\text{дост}) \le t(\text{треб}). \qquad (1.1)$$

В таблице 1.2 регламентированы нормы на максимально допустимую задержку передачи пакета «из конца в конец», которая обозначена как $t(\text{треб})$ и оценивается для каждого *i*-го потока данных. Значение Н обозначает – не определено.

Таблица 1.2 – Нормы для услуг с распределением по классам качества обслуживания

Сетевые характеристики	Классы качества обслуживания					
	0	1	2	3	4	5
Задержка доставки пакета	100 мс	400 мс	100 мс	400 мс	1с	Н
Вариация задержки пакета	50 мс	50 мс	Н	Н	Н	Н
Коэффициент потери пакетов	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	Н
Коэффициент ошибок пакетов	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	Н

Модель распределения суммарной задержки «из конца в конец» по сетевым элементам ЗКМСС представлена на рисунке 1.3.

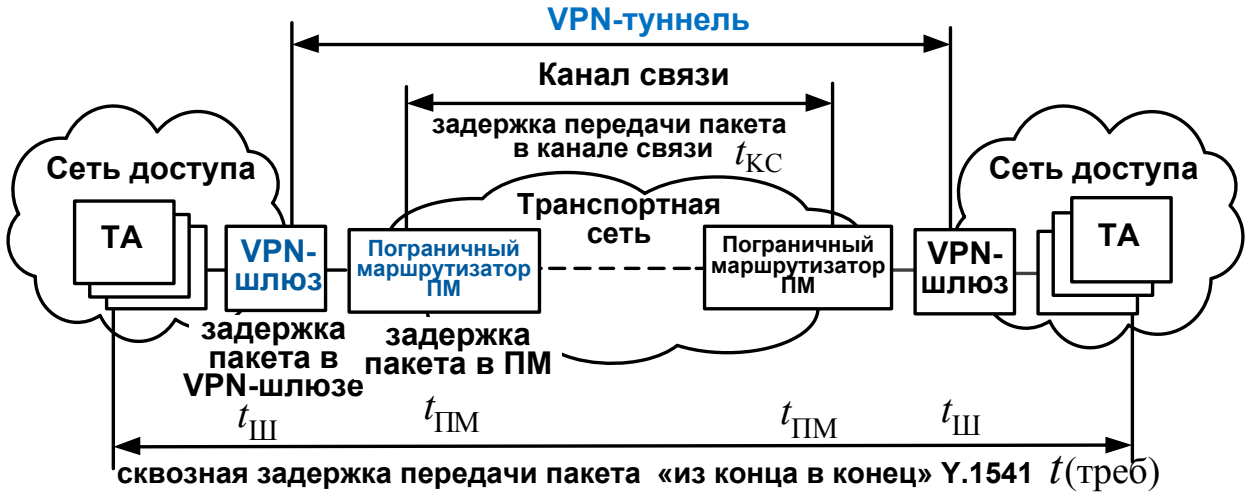


Рисунок 1.3 – Обобщенная схема тракта прохождения пакетов данных от источника к получателю защищенной корпоративной мультисервисной сети связи

Гарантированное КО сервисов реального времени в ЗКМСС достигается путем **обеспечения требуемой задержки обработки пакетов *i*-го потока в пограничном маршрутизаторе (ПМ) транспортной сети**. Исходя из того, что выполнение задачи обеспечения КО предоставляемых сервисов в ЗКМСС возложено на VPN-шлюз сети доступа, и учитывая то, что задержкой передачи пакета от VPN-шлюза сети доступа до ПМ можно пренебречь, определение максимально допустимой задержки обработки

пакетов *i*-го потока в ПМ транспортной сети осуществляется путем вычисления задержки обработки пакетов *i*-го потока в системе управления потоками VPN-шлюза сети доступа.

При расчете максимально допустимой задержки обработки пакета *i*-го потока в ПМ ЗКМСС $t_{\text{ПМ}}$ необходимо учесть, что задержка передачи пакета в *k*-ом арендованном канале связи ограничена верхним значением $t_{\text{КС}}$ и поддерживается оператором электросвязи в соответствии с заключенным на этапе планирования сети соглашением о качестве обслуживания SLA (Service Level Agreement), а задержка обработки пакета вследствие реализации процедуры шифрования информации в VPN-шлюзе, оцененная статистически, не превышает $t_{\text{Ш}}$ и обеспечивается заданной производительностью криптоядра – выражение (1.2):

$$2t_{\text{Ш}} + 2t_{\text{ПМ}} + t_{\text{КС}} \le t(\text{треб}). \qquad (1.2)$$

На основании выражения (1.2) оценка максимально допустимой задержки обработки пакета в ПМ может быть вычислена следующим образом:

$$t_{\text{ПМ}} \le \frac{t(\text{треб}) - t_{\text{КС}} - 2t_{\text{Ш}}}{2}. \qquad (1.3)$$

В случае обеспечения заданной задержки обработки пакетов *i*-го потока гарантируется и требуемый уровень КО.

Важное значение с точки зрения обеспечения требуемого уровня обслуживания потоков данных реального времени в ЗКМСС имеет выбор и взаимодействие алгоритмов обеспечения КО в сети доступа и транспортной сети коммутации пакетов. Это связано с тем, что ЗКМСС представляют собой, как правило, виртуальные частные сети (VPN – Virtual Private Network) с двухуровневой архитектурой телекоммуникационной плоскости [22,89]: транспортная сеть и сети доступа, на границе которых устанавливаются VPN-шлюзы [79,125]. При этом в сети доступа до

VPN-шлюза реализуется архитектура интегрированных услуг IntServ, а в транспортной сети – архитектура дифференцированного обслуживания DiffServ. Реализация IntServ в сети доступа позволяет осуществить процедуру управления допуском соединений, агрегирование потоков и формирование запросов на резервирование сетевых ресурсов от VPN-шлюза сети доступа на ПМ DiffServ региона.

Согласно [102], модель VPN-шлюза сети доступа в общем случае включает: маршрутизатор внутренней сети, обеспечивающий управление допуском потоков данных в VPN-шлюз от терминальных аппаратов пользователей; криптомодуль, реализующий шифрование поступающих от маршрутизатора внутренней сети данных и агрегирование шифрованных потоков в VPN-туннелях; маршрутизатор внешней сети, обеспечивающий управление допуском VPN-туннелей в транспортную сеть ЗКМСС (рисунок 1.4).

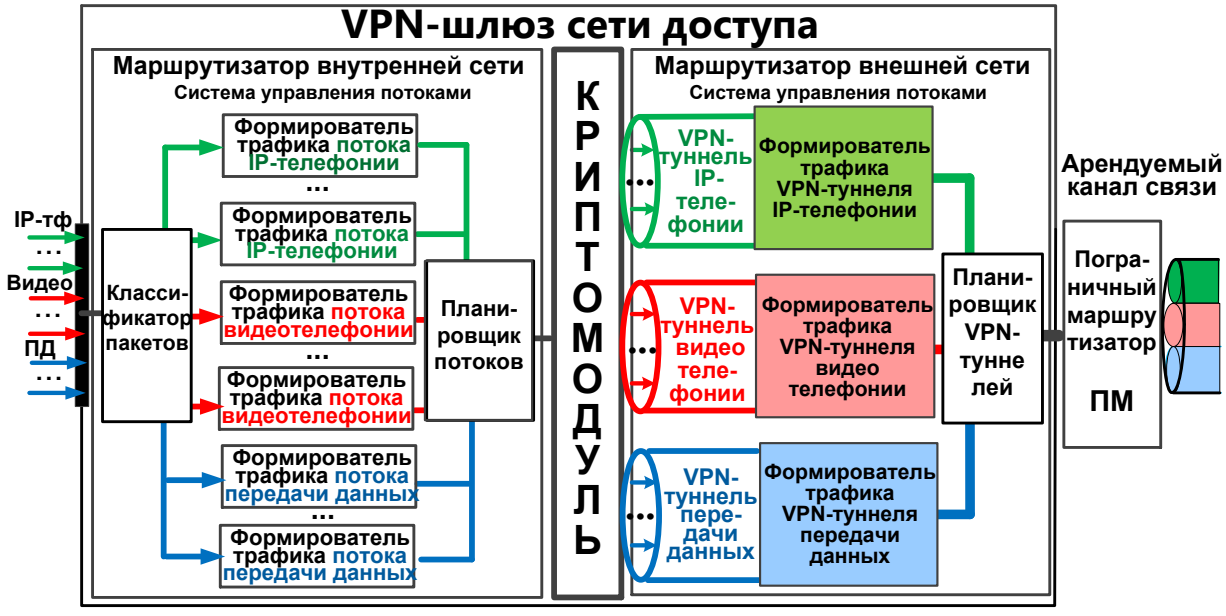


Рисунок 1.4. – Обобщенная схема VPN-шлюза сети доступа

До криптомодуля, выступающего в роли узла агрегирования шифрованных потоков данных сервисов реального времени, обработка трафика осуществляется механизмами архитектуры IntServ, реализованными

в системе управления потоками маршрутизатора внутренней сети и обеспечивающими требуемое КО поступающих потоков данных.

В общем случае система управления потоками маршрутизатора внутренней сети VPN-шлюза включает функциональные узлы доступа, классификации, буферизации, обслуживания (рисунок 1.5).

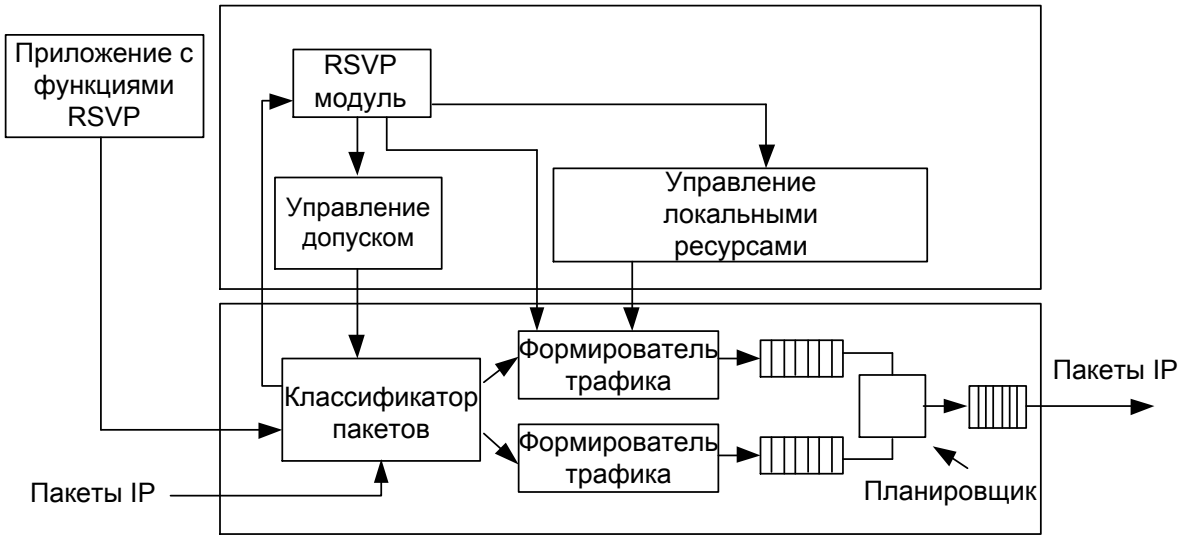


Рисунок 1.5 – Система управления потоками маршрутизатора внутренней сети VPN-шлюза сети доступа

Задача классификатора определить принадлежность каждого поступающего пакета определенному обслуживаемому или вновь поступившему потоку.

Формирователь трафика реализует один из двух типовых механизмов обработки – Leaky Bucket (далее – дырявое ведро) или Token Bucket (далее – ведро жетонов) [111] и предполагает контроль заявленных параметров потока, поступающих на вход криптомодуля.

Планировщик осуществляет выбор пакетов для передачи из буфера в криптомодуль. При этом данные обслуживаемых совместно потоков используют не только КР канала, но и буферное пространство, время центрального процессора и т.д. внутреннего маршрутизатора.

Для сравнительной оценки существующих планировщиков рассмотрим существующие типы обслуживания, представленные в [119,124]. Под типом обслуживания понимается набор условий, определяющий выполнение параметров КО передаваемых потоков информации (таблица 1.3).

Таблица 1.3 – Типы обслуживания потоков данных

Тип обслуживания	Выполнение параметров качества обслуживания	Уровень обслуживания	Степень использования сетевых ресурсов
Гарантированный	Гарантируется	Высокий	Низкая
Статистический	Нарушается в условиях перегрузки	Низкий	Высокая
Предсказуемый	Обеспечивается по возможности	Низкий	Высокая
Доступного качества	Не гарантируется	Низкий	Высокая

В качестве сопоставительных характеристик данных типов обслуживания в большинстве случаев используются следующие два параметра:

- уровень обслуживания потоков данных – процентное отношение количества пакетов, параметры качества обслуживания которых меньше допустимых значений, к общему количеству полученных пакетов;

- степень использования КР, которая определяется отношением занятого объема ресурсов к общему объему ресурсов узла коммутации (сети связи).

Представленные параметры позволяют судить об уровне КО, предоставляемого потокам данных, и соответственно об эффективности использования сетевых ресурсов.

С точки зрения соблюдения гарантий КО наиболее приемлемым в ЗКМСС является гарантированный тип обслуживания, реализуемый в архитектуре Intserv совокупностью перечисленных выше механизмов. В общем случае все планировщики, реализованные на основе способов

управления передачей пакетов можно классифицировать по способу определения очередности передачи пакетов (таблица 1.4).

Таблица 1.4 – Классы планировщиков

Класс планировщиков	Достоинства	Недостатки
С приоритетом передачи пакетов	Гарантированный уровень обслуживания высокоприоритетных потоков; высокая степень использования КР сети	Не обеспечивается гарантированный уровень обслуживания для потоков с различными параметрами КО; отсутствует количественный контроль ресурсов, занимаемых потоками
С контролем задержки передачи пакетов	Высокая степень использования КР сети	Не обеспечивается гарантированный уровень обслуживания для потоков с различными значениями параметров КО
С контролем скорости передачи потоков информации	Обеспечивается гарантированный уровень обслуживания для потоков с различными значениями параметров КО	Низкая степень использования для пачечного трафика
С динамическим распределением ресурсов	Обеспечивается предсказуемый уровень обслуживания для потоков с различными значениями параметров КО	Сложность реализации; низкая степень использования для пачечного трафика

В настоящее время вместо обслуживания очередей типа FIFO в мультисервисных сетях связи чаще применяется более прогрессивный механизм взвешенной справедливой очередности (WFQ) [47] с контролем скорости передачи потоков, когда ограниченный КР на выходе узла распределяется между несколькими агрегированными потоками (очередями).

Алгоритм WFQ основан на оценке виртуального времени завершения обслуживания каждого пакета в очередях. Тем самым реализуется принцип справедливого распределения ресурсов [78] и обеспечивается гарантированный тип обслуживания относительно времени задержки пакетов и предсказуемый относительно вероятности потерь за счет недостатка буферного пространства.

Для обеспечения гарантированных параметров передачи данных в архитектуре интегрированных услуг используется механизм предварительного резервирования ресурсов в маршрутизаторах для отдельных потоков (Resource Reservation). В качестве ресурсов рассматривается в первую очередь КР и буферное пространство портов маршрутизаторов на всем пути передачи данных. В IP-ориентированных сетях наиболее типичным механизмом резервирования является механизм, базирующийся на протоколе RSVP (Resource Reservation Protocol) [42].

Резервирование ресурсов «из конца в конец» начинается с запроса на резервирования ресурсов – RSVP PATH для однонаправленных симплексных потоков на всех сетевых элементах, находящихся на пути к получателю. Обработка служебных пакетов RSVP PATH и их передача последующим узлам осуществляется настроенным в сети алгоритмом маршрутизации. КО для отдельного потока данных реализуется с помощью механизмов управления трафиком (traffic control), которые включают функции классификации пакетов, входного контроля скорости передачи и планирования обслуживания пакетов.

Запрос RSVP PATH обрабатывается двумя локальными модулями: «управления допуском» (admission control) и «управления политикой» (policy control). Блок управления допуском определяет наличие у хоста ресурсов, достаточных для поддержки запрошенного уровня КО. Блок управления политикой определяет наличие у пользователя прав, достаточных для организации резервирования. Если обе проверки дают положительный результат, устанавливаются параметры классификатора пакетов. Если любая из проверок дает отрицательный результат, RSVP-модуль возвращает прикладному процессу сообщение об ошибке RSVP PATH ERR. RSVP ориентирован на сессию как поток данных с двумя обязательными параметрами: IP-адресом получателя (DestAddress), который может быть как индивидуальным, так и групповым, идентификатором протокола IP (ProtocolID) и одним необязательным параметром - обобщенным портом

получателя (DstPort), некоторой демультиплексируемой «точкой» транспортного или прикладного уровня получателя.

Запрос на резервирование RSVP PATH состоит из спецификации потока (flowspec) и спецификации фильтров (filterspec). Вместе их называют дескриптором потока. Спецификация потока указывает желаемые параметры КО. Спецификация фильтров совместно со спецификацией сессии определяет набор пакетов данных потока, к которым относятся параметры КО, заданные спецификацией потока. Спецификация потока служит для установки на узле параметров планировщика пакетов (численное значение весового коэффициента), а спецификация фильтров служит для установки параметров классификатора пакетов. Пакеты данных, адресованные конкретной сессии, но не соответствующие любому из заданных спецификацией фильтров параметру для данной сессии, будут обслуживаться по мере возможности (best-effort) или отбрасываться на входном порту маршрутизатора.

Спецификация потока в запросе на резервирование в общем случае включает класс обслуживания, а также два набора числовых параметров: RSPEC, определяющий желаемый уровень КО, и TSPEC, описывающий поток данных. Форматы и содержимое TSPEC и RSPEC определяются моделями интегрированного обслуживания [RFC 2210] и в общем случае не обрабатываются RSVP.

Точный формат спецификации фильтров зависит от используемого протокола (IPv4 или IPv6). В рамках настоящего исследования в качестве ограничения исследования будет ориентировано на протокол IPv4, поскольку адресное пространство ЗКМСС может дублироваться в защищаемых сетях доступа, и необходимость в IPv6 отсутствует.

Сообщения RSVP RESV поэтапно (hop-by-hop) переносят запросы на резервирование от получателей к отправителям по обратному пути доставки потока данных в этой сессии и готовности получателя к приему данных. IP-адресом получателя сообщения RSVP RESV служит индивидуальный

адрес предыдущего узла, полученный из состояния пути. В качестве IP-адреса отправителя служит адрес узла, передавшего сообщение.

После выполнения маршрутизатором внутренней сети VPN-шлюза задачи допуска потоков в VPN-шлюз, классифицированные потоки данных для каждой предоставляемой инфокоммуникационной услуги и соответствующего VPN-туннеля подвергаются шифрованию в криптомодуле. Это приводит к агрегированию потоков данных данной инфокоммуникационной услуги в общий поток соответствующего VPN-туннеля, что влечет за собой проблему организации управления допуском на уровне отдельных потоков в составе VPN-туннеля. **Минимально наблюдаемым потоком данных, доступным для управления, выступает трафик VPN-туннеля,** и идентификация вида предоставляемой услуги, количества установленных сеансов связи, внутренних IP-адресов терминалов отправителя и получателя в составе агрегированного потока данных VPN-туннеля становится невозможной, за исключением идентификации VPN-туннелей по внешним (открытым) IP-адресам VPN-шлюзов. В результате управление допуском в транспортную сеть осуществляется на уровне VPN-туннелей. Данную задачу осуществляет система управления потоками маршрутизатора внешней сети VPN-шлюза, включающая в себя те же функциональные узлы совместно с модулем маршрутизации, что и система управления потоками маршрутизатора внутренней сети.

Исходя из вышеизложенного, актуальным направлением является реализация максимальной загрузки арендуемого КР транспортного уровня ЗКМСС посредством разработки эффективных алгоритмов, обеспечивающих решение задачи оперативного управления, связанной с оцениванием, резервированием и перераспределением требуемого КР для агрегированных потоков данных, передаваемых в VPN-туннелях.

Разрешению данной задачи способствует реализация динамического резервирования КР транспортной сети ЗКМСС с архитектурой DiffServ посредством формирования RSVP запросов от VPN-шлюза к ПМ для

обслуживания с гарантированным уровнем КО каждого потока данных, входящего в состав агрегированного потока данных VPN-туннеля.

При этом необходимо учитывать особенность архитектуры DiffServ, заключающуюся в том, что механизмы управления трафиком DiffServ-маршрутизаторов, конфигурируемые в ЗКМСС, являются статичными, несогласованными друг с другом [104,113]. Адаптация данных механизмов к изменению поступающей нагрузки и загруженности канала связи возможна лишь за счет переконфигурирования. Для каждого заранее определенного класса трафика выделяется физический буфер и резервируется КР, чем добиваются изоляции потоков данных и снижения их взаимного влияния на достижимый уровень КО. Учитывая скорость изменения загруженности каналов связи, особенно в периоды наибольшей нагрузки, процедура переконфигурирования оборудования пограничного маршрутизатора вручную является технически не реализуемой.

Формирование RSVP запросов от VPN-шлюза к ПМ DiffServ региона обеспечивает резервирование ресурсов и включает следующие процедуры:

- определяется политика «пошаговой маршрутизации» PHB для запрошенной услуги;

- проводится сравнение ресурсов, запрашиваемых в RESV сообщении и уровня КО, предлагаемого сегментом DiffServ;

- в случае если ресурсов достаточно и параметры трафика соответствуют SLS (Service Level Specifications), то соединение поддерживается, а сообщение RESV направляется далее в сторону источника, иначе выполняются соответствующие процедуры, рассмотренные при описании протокола RSVP.

Известно, что архитектура DiffServ позволяет эффективно использовать процессорную мощность маршрутизаторов высокоскоростных транспортных сетей, т.к. сетевые узлы обрабатывают поступающие пакеты с помощью простых механизмов КО, настройка которых производится на этапе планирования сети с ориентацией на пиковую возможную нагрузку по каждому классу трафика для обеспечения гарантированного КО. Несмотря на

простоту функционирования сетевого оборудования, в данной архитектуре ярко выражена проблема организации функции управления доступом на уровне соединений (Connection Admission Control – CAC), особенно в условиях применения VPN-шлюзов, когда минимально наблюдаемым потоком данных, доступным для управления, выступает трафик VPN-туннеля, классифицируемый только по IP-адресам VPN-шлюза отправителя и получателя. Такое состояние дел зачастую приводит или к ухудшению КО передаваемых потоков или к неэффективному использованию арендуемого КР, даже при условии, что имеется незадействованный в данный момент времени КР. Архитектура IntServ позволяет не только гарантировать КО каждому потоку данных, но и максимально эффективно использовать КР сети, т.к. при установлении новых соединений изначально производится его оценивание и состояние. Кроме того, строгая изоляция потоков друг от друга, позволяет защитить потоки от их взаимного влияния друг на друга вследствие некорректно запрошенных спецификаций, что наиболее значимо в транспортных сетях, где КР зачастую арендуется.

В архитектуре IntServ (сети доступа ЗКМСС) для обеспечения КО за счет резервирования КР используются планировщики WFQ, относящиеся к классу «с контролем скорости передачи потоков информации» и требующие значительных вычислительных затрат [117]. В транспортной сети с коммутацией пакетов для каждого агрегированного потока данных используются планировщик FIFO, а КР для функционирования FIFO выделяется алгоритмом по классам обслуживания CBQ (Class Based Queuing), описанным в RFC 2211.

Исходя из вышеизложенного можно сделать вывод, что существующие подходы превентивного динамического управления КР транспортной сети связи с коммутацией пакетов, учитывающие приоритетность передаваемых потоков данных и гарантирующие при этом требуемый уровень качества их обслуживания, невозможно реализовать в ЗКМСС без изменения модельно-

алгоритмической основы сигнальных протоколов архитектуры IntServ в сети доступа.

1.3. Анализ существующих математических моделей агрегированного потока данных

Проведенный анализ предметной области, а именно математических моделей агрегированных потоков данных показал, что они в основном применяются при оценивании требуемого КР для гарантированного обслуживания агрегированного потока данных механизмами управления допуском потоков данных в сеть CAC. Для этого изначально оцениваются параметры агрегированного трафика на выходе системы управления нагрузкой, а в последующем, учитывая нормированные значения параметров качества обслуживания, принимается решение о допуске или запрете к установлению нового потока данных.

Разработанные и реализованные на программно-аппаратном уровне в настоящее время модели управления допуском на уровне соединений классифицируются на:

1) Параметрические CAC Parameter-based CAC (PBAC) [47,48,56]. Вычисляется КР, необходимый для поддержки множества потоков на основе значений таких параметров как мгновенная пиковая скорость передачи, средняя скорость передачи, максимальная допустимая задержка, вероятность потери пакета, максимальный размер пачки (Maximum Burst Size) и т.п., заданных заранее или транслируемых от конечного терминального устройства.

2) Модели CAC, основанные на измерениях Measurement-based CAC MBAC [3,108]. Данные модели применяются на факте, что характеристики трафика не являются статичными, а все время меняются. Высокая степень использования канала достигается путем отсутствия строгих обязательств по параметризации потоков.

Модели РВАС подразделяется на детерминированные и вероятностные. Детерминированные модели РВАС применяются при оценивании КР по сумме пиковых скоростей допущенных потоков. Другие, более эффективные, используются для оценивания задержки обработки пакетов в ПМ при заданном зарезервированном КР и конфигурации средств управления нагрузкой, например «корзина с маркерами» [41]. При вычислении требуемого КР и использовании вероятностного подхода зачастую ориентируются на эффективную скорость передачи агрегированного потока данных. При этом используется методологический аппарат моделирования процессов функционирования мультисервисных сетей связи, предложенный в работах Ф.П. Келли, В. Иверсена, С.Н. Степанова, представляющий модификацию моделей Эрланга и Энгсета, ориентированных на использование эффективной, а не пиковой скорости передачи данных. Используя статистические оценки характеристик данного потока, размер буфера и значение КР, зарезервированных для обслуживания пакетов данного потока, производится оценка вероятности их потери. Мгновенные скорости отдельных потоков данных, составляющих агрегированный поток, в качестве допущения принимаются независимыми и одинаково распределенными, что на практике не достижимо, а техническая реализация подобных моделей не позволяет гарантировать достижимый уровень КО, что в свою очередь не допустимо при предоставлении мультимедийных услуг в ЗКМСС. Существенным ограничением такого подхода является применение фиксированных значений выделяемого КР и использование средних значений длительности обслуживания заявки, не зависящих от загрузки звена мультисервисной сети связи, что снижает точность получаемых оценок.

К отдельным методам РВАС можно отнести те, при которых одновременно учитываются известные параметры поступающих потоков, измеряются параметры средней скорости передачи данных и дисперсия средней скорости агрегированного потока. Модели специализированы под вид передаваемого трафика: трафик реального времени с неизменными

параметрами в течение сеанса связи, передача данных с переменной скоростью и т.д. Кроме того, результаты функционирования зависят от применяемой на маршрутизаторе системы обслуживания соединений.

Подгруппа методов с использованием прогнозирования поступающей нагрузки или их параметров более подробно рассматривается в работах [29,103,121]. Общим недостатком методов прогнозирования, имеющих дело с математическими моделями, является точность получаемых оценок, которая связана с периодом упреждения: чем он больше, тем меньше точность и тем полнее должны быть исходные данные о прогнозируемом объекте.

Вторая группа методов представлена в следующих работах [34,107,124,135]. Логика функционирования данных методов основана на контроле (мониторинге) косвенных параметров объектов, например загруженности канала связи, переполнения буферного устройства сетевого оборудования, увеличение количества поступающих на маршрутизатор потоков данных и т.д. При превышении допустимого состояния вышеуказанных объектов производится динамическое резервирование КР.

Из представленного анализа можно сделать вывод о том, что среди существующих на данный момент подходов к оцениванию требуемого КР транспортной сети связи с коммутацией пакетов при условии обеспечения требуемого уровня КО трафика ЗКМСС, позволяющих повысить степень использования КР магистральных каналов связи, наиболее подходящими являются детерминированные модели оценивания на основе параметров трафика, транслируемых источником.

1.4. Исследование влияния процедур функционирования VPN-шлюзов на параметры передаваемого трафика

Проведенные исследования показали, что в процессе активного развития способов управления допуском в инфокоммуникациях, передачи блоков данных, алгоритмов контроля и сглаживания профиля трафика методологический аппарат оценивания требуемого КР развит в

недостаточной мере и не учитывает особенности функционирования ЗКМСС. Одной из основных особенностей является влияние VPN-шлюзов на параметры агрегированного потока данных ЗКМСС, т.к. использование средств криптографической информации (СКЗИ) не позволяет в полной мере взаимодействовать алгоритмам обеспечения КО архитектуры IntServ через сегмент DiffServ в транспортной сети коммутации пакетов за счет добавления нового заголовка пакета с открытыми IP-адресами и внесения дополнительной задержки в обработку пакетов. В работе было проведено исследование влияния процедур функционирования VPN-шлюза на параметры передаваемого трафика ЗКМСС, включающее два этапа.

На первом этапе выполнялось оценивание численных значений параметров трафика, генерируемого терминальным оборудованием характерным для ЗКМСС, на узле доступа в транспортную сеть ЗКМСС. Для этого был проведен полунатурный эксперимент, схема которого представлена на рисунке 1.6.

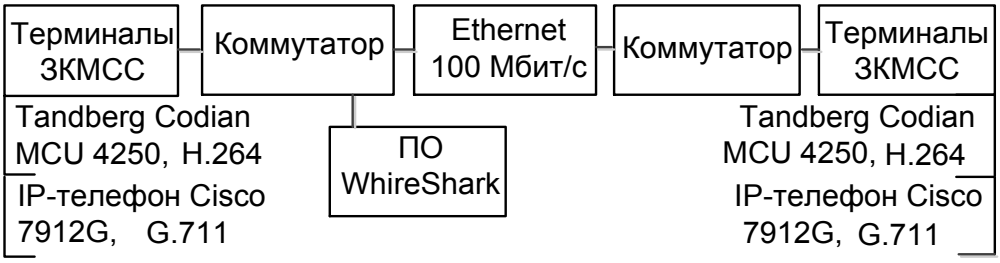
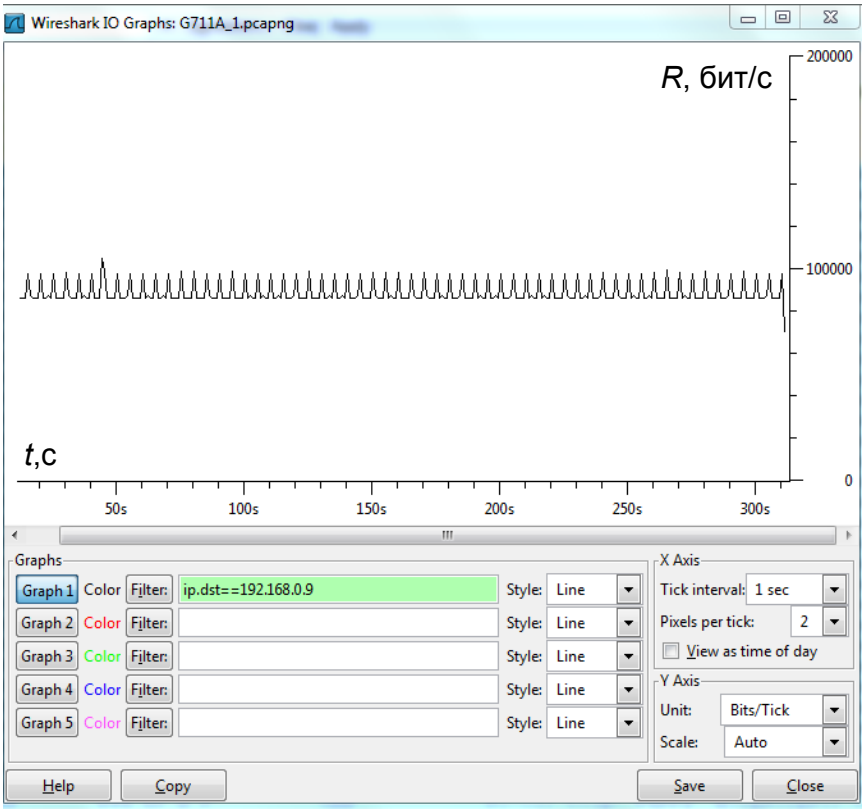
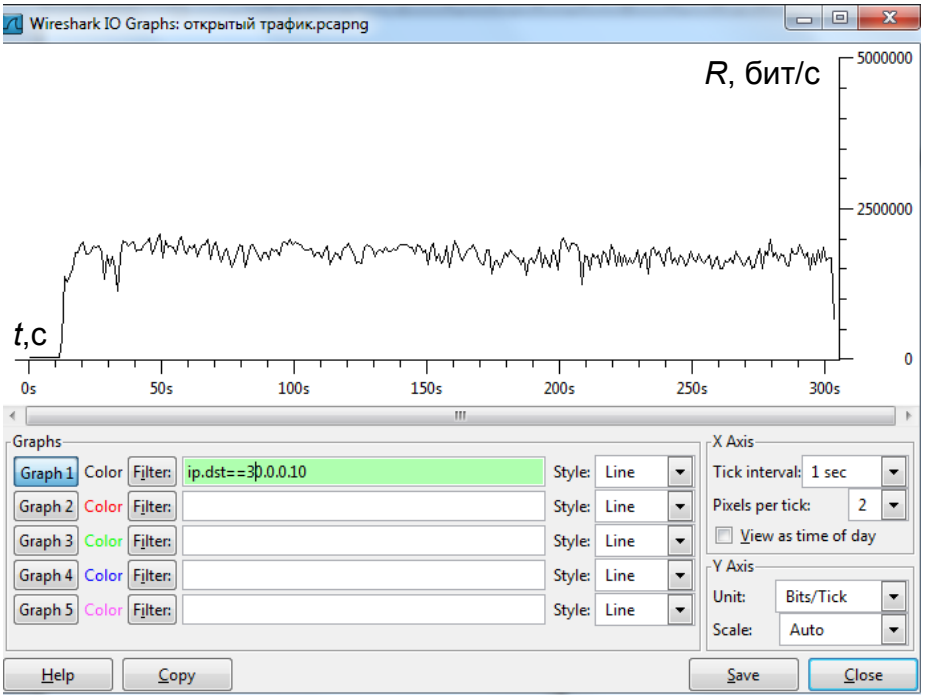


Рисунок 1.6 – Экспериментальный стенд для исследования параметров трафика, генерируемого терминальным оборудованием

Для наглядности представления статистического материала объемы, передаваемые источником данных с интервалом регистрации, выбранном равным 1 секунде и представляющие собой мгновенную скорость передачи данных, генерируемых IP-телефоном Cisco 7912G со встроенным речевым кодеком G.711 и видеотерминалом Tandberg Codian MCU 4205 со встроенным протоколом передачи видео H.264, представлены на графиках (рисунок 1.7).



а

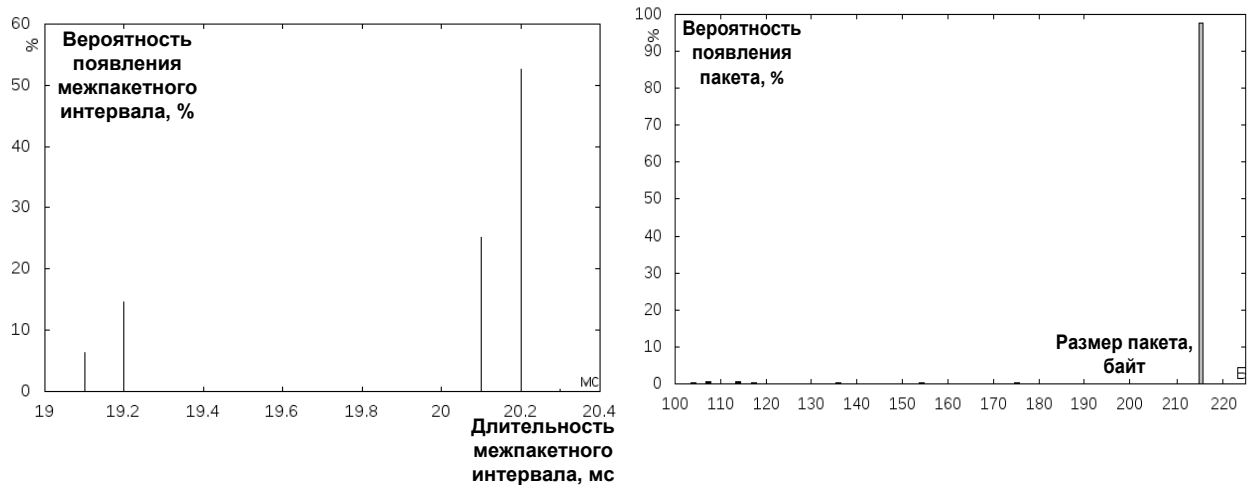


б

Рисунок 1.7 – Мгновенная скорость а) на выходе IP-телефона, б) на выходе видеотерминала

Гистограммы длин генерируемых пакетов и межпакетный интервал представлены на рисунке 1.8.

G.711



H.264

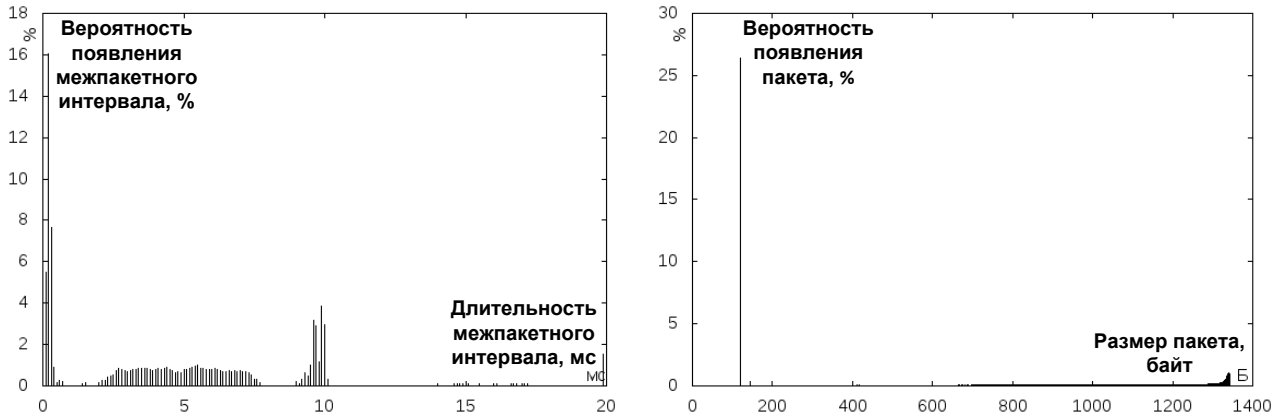


Рисунок 1.8 – Гистограммы длин пакетов и межпакетного интервала на выходе IP-телефона и видеотерминала

Оценивание численных значений долгосрочных параметров трафика: мгновенной пиковой и средней скорости передачи данных производилось на временном отрезке усреднения равным 100 секундам. Данное значение выбрано из соображений о том, что согласно проведенным международной организацией по исследованиям RACE при строительстве сетей связи, средняя длительность сеанса телефонии и видеотелефонии принимается равной 100 секундам. Максимальные значения данных параметров, оцененных с помощью программы WireShark, сведены в таблицу 1.5.

Таблица 1.5 – Численные значения параметров трафика

	Значения параметров трафика					
	Видеотелефония			IP-телефония		
	p Мбит/с	r Мбит/с	L Байт	p Мбит/с	r Мбит/с	L Байт
От терминала	2,1	0,87	1346	0,112	0,096	214

На втором этапе исследовалось влияние СКЗИ на параметры ПДРВ. Для этого был проведен эксперимент, обобщенная схема экспериментального стенда которого представлена на рисунке 1.9.

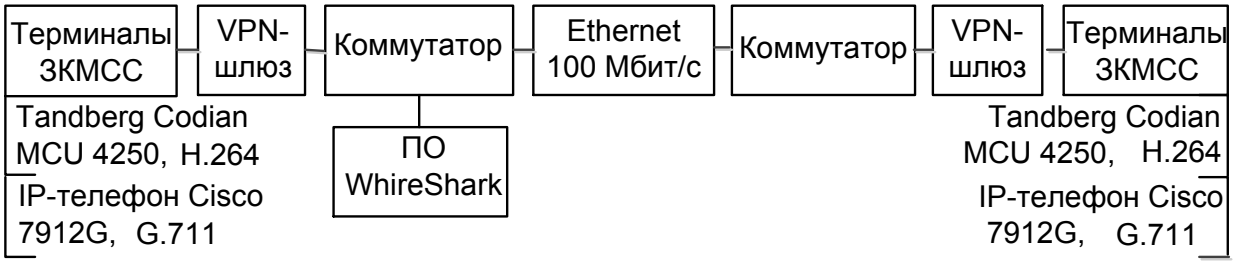
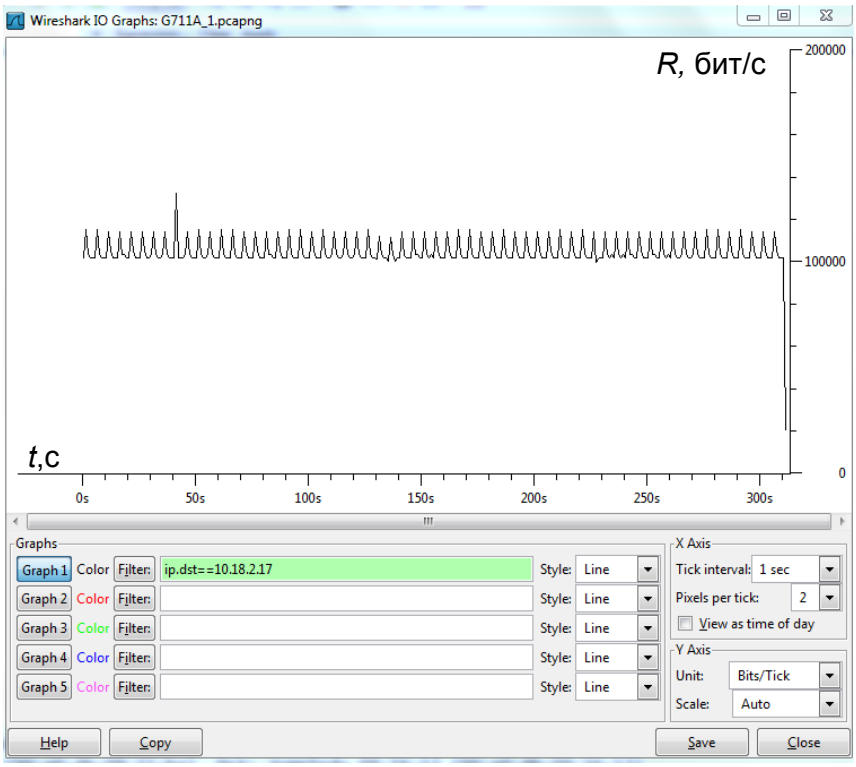


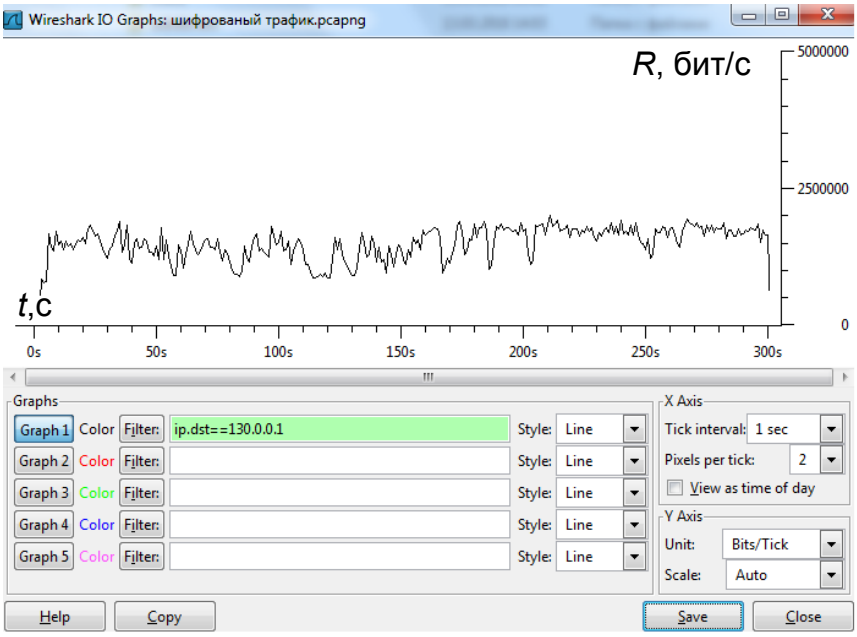
Рисунок 1.9 – Экспериментальный стенд для исследования влияния СКЗИ на параметры трафика, генерируемого терминальным оборудованием

В результате проведения эксперимента ПО WireShark осуществляется равноточные наблюдения: фиксируется время появления пакета на выходе VPN-шлюза (время обработки пакета в коммутаторе не учитывается, т.к. коммутатор функционирует в режиме «зеркалирования» портов, без внесения дополнительной задержки на обработку пакетов).

Для наглядности представления статистического материала объемы, передаваемые источником данных с интервалом регистрации, выбранным равным 1 секунде и представляющие собой мгновенную скорость передачи на выходе VPN-шлюза, функционирующего в туннельном режиме, представлены на графиках (рисунок 1.10).



а

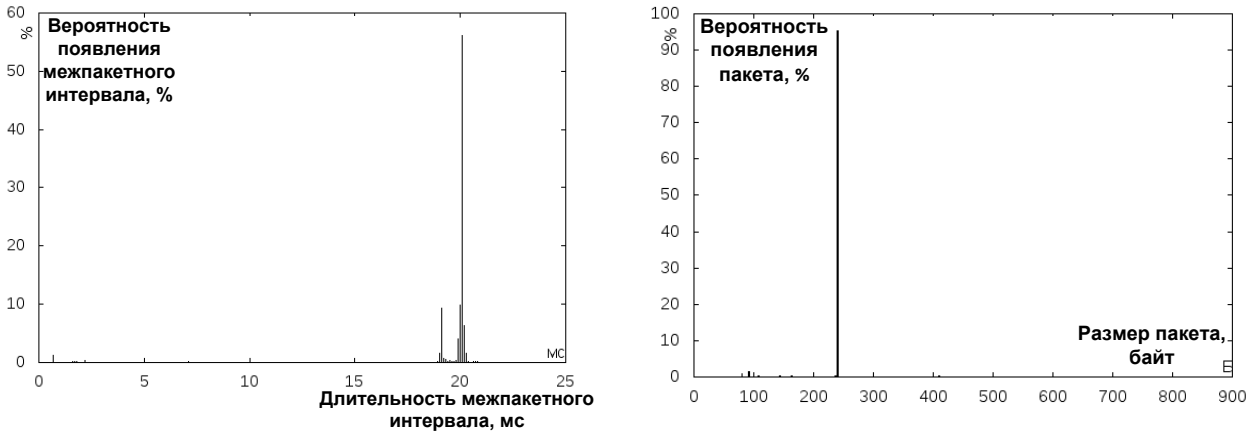


б

Рисунок 1.10 – Мгновенная скорость на выходе VPN-шлюза
а) потока данных IP-телефонии, б) видеотелефонии

Гистограммы длин пакетов и межпакетного интервала на выходе СКЗИ представлены на рисунке 1.11.

G.711



H.264

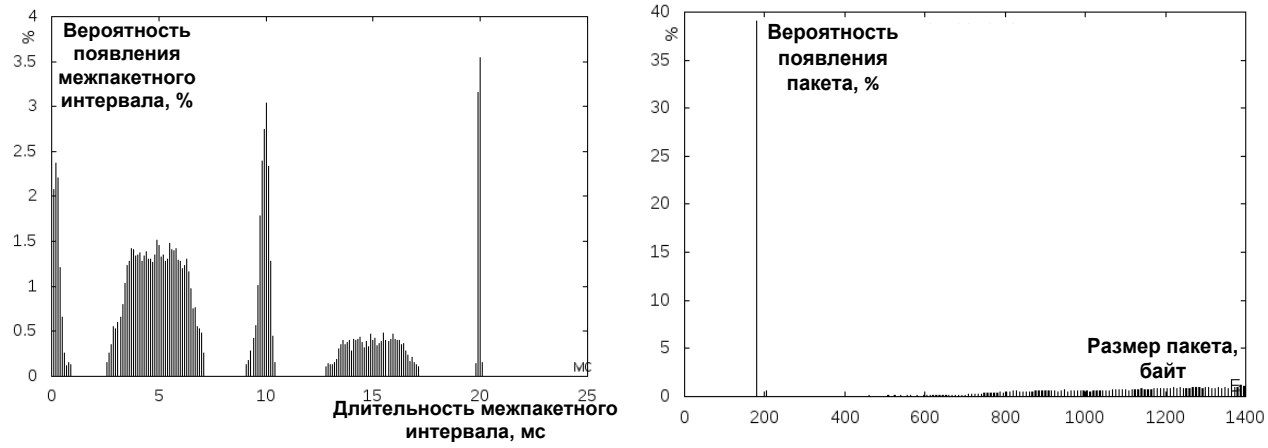
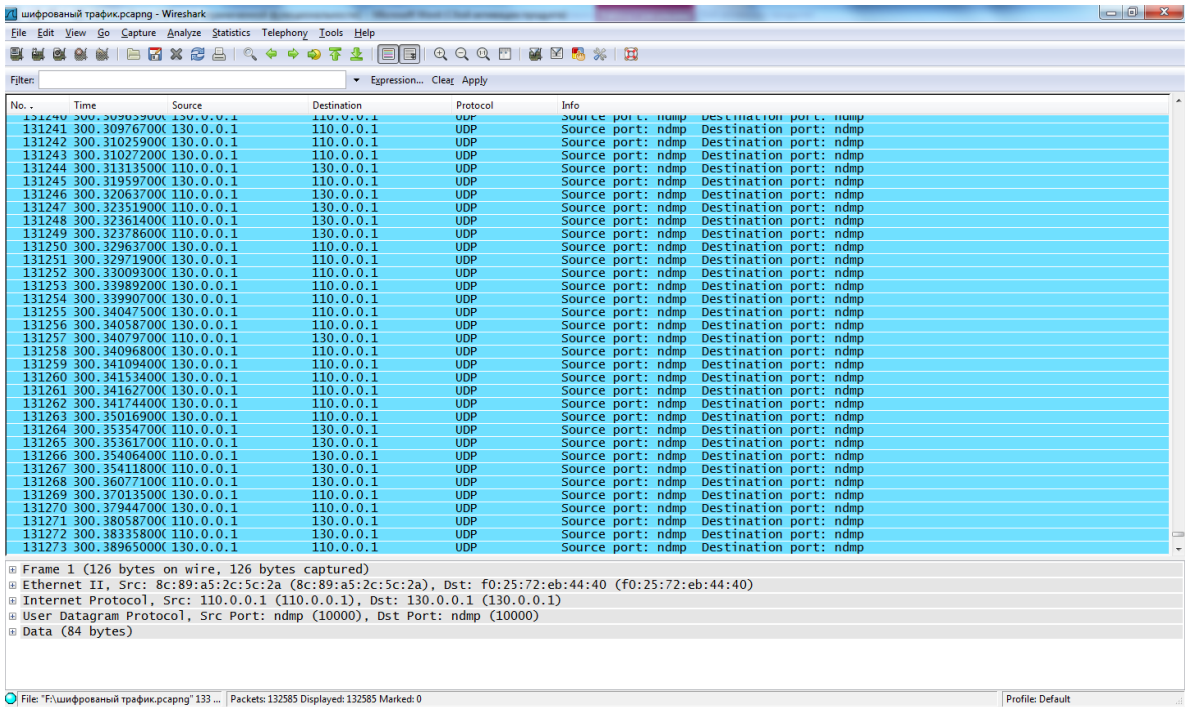


Рисунок 1.11 – Гистограммы длин пакетов и межпакетного интервала на выходе VPN-шлюза потока данных IP-телефонии и видеотелефонии

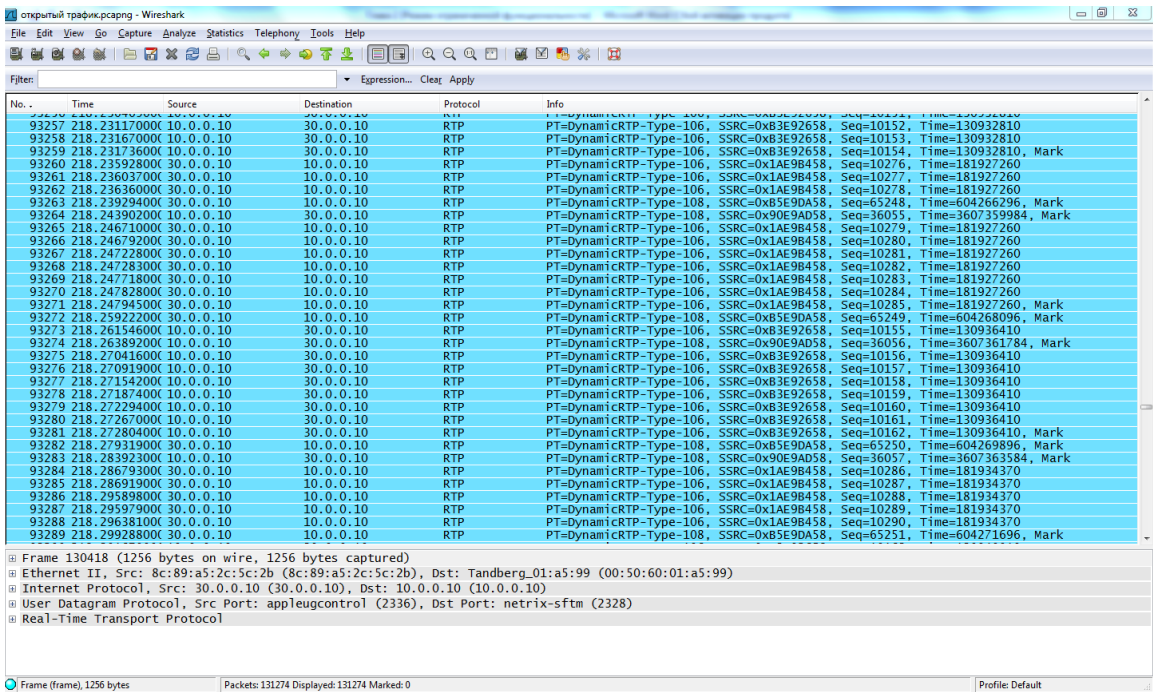
Проведенный эксперимент позволил выявить влияние VPN-шлюза на параметры средней и мгновенной пиковой скоростей передачи трафика, изменение длин пакетов, генерируемых оконечным терминальным оборудованием. Визуальный анализ представленных графиков позволяет сделать следующие выводы: при передаче аудиопотоков средняя и мгновенная пиковая скорости передачи данных повышаются, межпакетный интервал практически остается неизменным и находится в пределах от 19 до 20,5 миллисекунд. Это позволяет сделать вывод о том, что шифрование данных IP-телефонии не вносит дополнительных задержек; средняя и пиковая скорости передачи данных видеопотока данных значительно

снижаются после прохождения VPN-шлюза, что связано с бо́льшими по сравнению с речевым трафиком размерами пакетов и значительно меньшей длительностью межпакетного интервала, в основном заключенным в пределах от 2 до 7 и от 9 до 11 миллисекунд. На выходе VPN-шлюза трафик более равномерный за счет неоднократной буферизации пакетов на входном порту, в буфере криптоядра, а также в выходном буфере, т.е. выходной трафик с VPN-шлюза сглаживается по сравнению с трафиком на входе, при этом длины пакетов увеличивается за счет заголовка и концевика протокола шифрования ESP не значительно. Таким образом, VPN-шлюз вносит значительную задержку в передачу пакетов видеотрафика за счет их шифрования и практически не вносит задержку в аудиотрафик данных.

Статистический материал, подлежащий обработке на уровне пакетов данных, представлен рисунке 1.12.



а



б

Рисунок 1.12 – Статистический материал а) IP-телефонии, б) видеотелефонии

Таким образом, выявлено влияние процедур функционирования VPN-шлюза на параметры передаваемого трафика: пиковую (p) и среднюю (r) скорость передачи информационных потоков, длину генерируемых пакетов (L) сервисов видеотелефонии и IP-телефонии. Результаты статистической обработки данных представлены в таблице 1.6, а условия и результаты выполнения статистического эксперимента – в работах [62,64].

Таблица 1.6 – Значения параметров трафика на входе и выходе VPN-шлюза

	Значения параметров трафика					
	Видеотелефония			IP-телефония		
	p Мбит/с	r Мбит/с	L Байт	p Мбит/с	r Мбит/с	L Байт
От терминала	2,1	0,87	1346	0,112	0,096	214
На выходе VPN-шлюза	1,74	1,22	1392	0,126	0,107	254

Результаты статистического эксперимента позволили ввести поправочные коэффициенты α, β, γ для соответствующих параметров

передаваемого трафика, учитывающие искажения, вносимые криптомодулем. Данные коэффициенты определены: α - как отношение пиковой скорости потока данных, оценённой на ПМ транспортной сети без учета влияния VPN-шлюза (в таблице 1.6 - значения параметров трафика от терминала) к пиковой скорости с учетом влияния VPN-шлюза (в таблице 1.6 - значения параметров трафика на выходе VPN-шлюза); β - как отношение средней скорости потока данных, оценённой без учета влияния VPN-шлюза (в таблице 1.6 - значения параметров трафика от терминала) к средней скорости с учетом влияния VPN-шлюза (в таблице 1.6 - значения параметров трафика на выходе VPN-шлюза); γ - как отношение максимальной длины пакета, оценённой без учета влияния VPN-шлюза (в таблице 1.6 - значения параметров трафика от терминала) к максимальной длине пакета с учетом влияния VPN-шлюза (в таблице 1.6 - значения параметров трафика на выходе VPN-шлюза).

1.5. Постановка научной задачи диссертационного исследования

В рамках достижения цели диссертационного исследования, учитывая вышеизложенные особенности построения и функционирования ЗКМСС, требуется осуществить формальную постановку научной задачи исследования, заключающуюся в необходимости:

1) разработки алгоритма динамического резервирования канального ресурса агрегированного потока данных сервисов реального времени, передаваемого в VPN-туннеле защищенной корпоративной мультисервисной сети связи, позволяющий обеспечить гарантированный уровень качества, зависящий от:

- n – множества потоков данных, агрегируемых в VPN-туннеле;
- p – пиковой скорости потока данных, байт/с;
- r – средней скорости потока данных, байт/с;
- L – максимального размера передаваемого пакета, байт;

● t(треб) – максимально допустимой задержки передачи пакета потока данных, определяемой рекомендацией Y.1541, с;

● $R_{\text{КС}}$ – пропускной способности канала связи защищенной корпоративной мультисервисной сети связи, байт/с;

2) разработки алгоритма допуска потоков в транспортную сеть ЗКМСС, позволяющего в условиях перегрузки обслужить наибольшее количество потоков данных с наивысшим приоритетом с гарантированным уровнем КО;

3) разработки комплекса алгоритмов согласования трафика с VPN-туннелем, обеспечивающего совместно с алгоритмом допуска потоков в транспортную сеть повышение степени использования КР: в условиях штатного функционирования сети доступа за счет перераспределения незадействованного КР между предоставляемыми инфокоммуникационными сервисами, а в условиях возникновения перегрузки за счет решения задачи выбора оптимального набора допущенных к обслуживанию потоков с учетом их приоритетов и длительности сеанса.

В качестве показателя оценивания степени использования КР ЗКМСС при отсутствии перегрузки выбрана относительная величина увеличения объема выделяемого ресурса для обслуживания низкоприоритетной нагрузки:

$$\delta^{\text{исп}}(t) = \frac{\sum_{s=1}^{n} \Delta R_s}{\sum_{s=1}^{n} R_s} \cdot 100\%, \qquad (1.6)$$

где $\Delta R_s = R_s - \sum_{l=1}^{L} R_l$ – незадействованный КР, зарезервированный для s-го предоставляемого сервиса, R_s – максимальный резервируемый КР на этапе планирования сети, R_l – резервируемый КР для l-го VPN-туннеля из множества L VPN-туннелей, создаваемых для s-го предоставляемого сервиса.

В качестве показателя оценивания степени использования КР ЗКМСС при возникновении перегрузки (нештатное функционирование сети) выбрана вероятность потерь вызовов приоритетных пользователей. Принято допущение, что нагрузка, создаваемая абонентами высших категорий, при возникновении перегрузки обслуживается с гарантированным качеством. При этом разработанный алгоритм допуска потоков в транспортную сеть позволяет за счет выбора оптимального набора допущенных к обслуживанию потоков с учетом их приоритетов и длительности сеанса, а также резервирования КР на основе разработанного алгоритма динамического резервирования канального ресурса агрегированного потока данных уменьшить вероятность потерь вызовов от приоритетных пользователей. При наличии категорий пользователей в ЗКМСС, которым предоставляется данный класс услуг (0 – руководители корпорации и их заместители, 1 – начальники отделов, 2 – рядовые сотрудники), нагрузка, создаваемая абонентами высшей категории (№0) обслуживается с гарантированным качеством, вероятность потерь вызовов от пользователей категории №1 уменьшается.

При решении научной задачи определены ограничения и допущения:

1) максимальная задержка обработки пакетов в арендуемых каналах связи и их пропускная способность не изменяется;

2) между взаимодействующими VPN-шлюзами для каждого предоставляемого сервиса устанавливается один VPN-туннель;

3) максимальная задержка обработки пакета в VPN-шлюзах не изменяется при увеличении его загруженности;

4) для формирования трафика во всех ПМ сети применяются алгоритмы «корзина маркеров»;

5) во всех сетевых устройствах функционирует планировщик обслуживания пакетов, базирующийся на алгоритме взвешенной справедливой очередности WFQ.

1.6. Выводы по первому разделу

1. Проведенные исследования ЗКМСС показали, что в процессе активного развития способов управления допуском в инфокоммуникациях, передачи блоков данных, алгоритмов контроля и сглаживания профиля трафика методологический аппарат оценивания требуемого КР развит в недостаточной мере и не учитывает особенности функционирования ЗКМСС.

2. Существующие инструментальные средства управления трафиком ориентированы на сети связи общего пользования, тогда как отличительными особенностями ЗКМСС с точки зрения обеспечения КО являются:

– разделение пользователей по категориям обслуживания, что требует гарантий в уровне КО и организации приоритетного допуска в условиях перегрузки;

– отсутствие собственной транспортной инфраструктуры, вследствие чего арендуются каналы на основе технологии IP/MPLS;

– использование при построении ЗКМСС оборудования иностранного производства с реализацией планировщиков, позволяющего предоставлять услугу с гарантированным КО только в сети доступа (сегменте IntServ);

– использование VPN-шлюзов не позволяет взаимодействовать алгоритмам обеспечения КО IntServ услуг через сегмент DiffServ в транспортной сети за счет добавления нового заголовка пакета с открытыми IP-адресами и внесения дополнительной задержки в обработку пакетов.

3. Для эффективного использования арендуемого КР транспортной сети целесообразно оценивать влияние VPN-шлюзов на параметры агрегированного потока данных ЗКМСС, для чего необходимо усовершенствовать существующие модели агрегированных потоков данных.

4. Применяемые в сетях связи общего пользования способы приоритетного обслуживания потоков данных не отражают специфику функционирования ЗКМСС, что требует проработки порядка приоритетного обслуживания, отвечающего принципам предоставления инфокоммуникационных услуг в ЗКМСС.

Раздел 2

Разработка алгоритма динамического резервирования канального ресурса агрегированного потока данных сервисов реального времени

2.1. Введение

Проведенный в первой главе анализ условий функционирования и эксплуатации ЗКМСС показал, что арендуемый КР транспортной сети ЗКМСС используется неэффективно. Это вызвано, прежде всего, отсутствием проработанного математического обеспечения оценивания требуемого КР для обслуживания ПДРВ с гарантированным КО. В результате чего применение существующих математических моделей агрегированного потока данных не дает точных оценок требуемого КР в условиях применения VPN-шлюзов, чем ограничивается реализация архитектуры интегро-дифференцированного обслуживания передаваемого трафика.

В этой связи требуется усовершенствовать существующие модели в направлении учета влияния VPN-шлюзов на параметры мгновенной пиковой скорости передачи данных, средней скорости передачи данных, длин генерируемых пакетов.

2.2. Исследование применимости существующих математических моделей агрегированного потока данных в защищенной корпоративной мультисервисной сети связи

Математической основой таких моделей выступает теория сетевых исчислений (NC – Network Calculus) [129,138,139], позволяющая по известным численным параметрам формирователя трафика (в системе

управления потоками VPN-шлюза сети доступа ЗКМСС) рассчитать граничные оценки параметров КО.

Согласно данной теории входящий в формирователь трафика системы управления потоками VPN-шлюза поток ограничивается детерминированной функцией входящего потока, а выходной поток напрямую зависит от применяемой дисциплины обслуживания и ограничивается функцией обслуживания [55,57,59]. Детерминированный характер используемых допущений математических моделей является вполне адекватным, если учесть, что в реальных сетях трафик всегда ограничен пропускной способностью канала связи, а также вследствие прохождения механизмов формирования поступающей нагрузки, реализованных в архитектурах IntServ и DiffServ. Описание потоков данных с использованием данного математического аппарата позволяет свести сложные нелинейные системы к линейным.

Для описания потоков данных, поступающих от источников в формирователь трафика системы управления потоками VPN-шлюза, используется кумулятивная функция $A(t)$, определяющая число байт данных, поступивших в систему за интервал времени $[0,t]$. При этом, принимается, что $A(0)=0$. Функция $A(t)$ – всегда неубывающая. В последующем такая функция в работе именуется как детерминированная функция поступления.

Поток A является ограниченным функцией f тогда и только тогда, когда для всех $t_1 \le t_2$ выполняется:

$$A(t_2)-A(t_1)\le f(t_2-t_1). \qquad (2.1)$$

С вычислительной точки зрения значительно удобнее для описания телекоммуникационных систем использовать непрерывные функции. Однако в реальных системах используются минимальные неделимые блоки данных – пакеты, следовательно, и модели, описывающие непрерывную работу систем передачи данных, являются идеальными и не учитывают погрешность «дискретизации». В мультисервисных IP-сетях, использующих технологию Ethernet на канальном уровне ЭМВОС, поступающая нагрузка может быть

аппроксимирована непрерывной функцией в связи с тем, что дисперсия размеров пакетов и межпакетного интервала достаточно велика [46,126].

При максимальном размере пакета данных *i*-го потока L_i (байт), известной пиковой скорости генерации пакетов p_i (байт/с), средней скорости генерации пакетов r_i (байт/с) и выделенном размере буфера b_i (байт) в ЗКМСС в системе управления потоками VPN-шлюза сети доступа с реализованной функцией формирования трафика поток данных на выходе описывается выражением [55,59]:

$$A_i(t) = \begin{cases} L_i + p_i t & t < \dfrac{b_i - L_i}{p_i - r_i}; \\ b_i + r_i t & t \geq \dfrac{b_i - L_i}{p_i - r_i}, \end{cases} \tag{2.2}$$

где $A_i(t)$ – количество нагрузки i-го потока, поступившей в систему за период времени (0, t] для наихудшего случая, когда размер пакетов равен максимально возможному значению L_i. При этом пиковое значение скорости поступления пакетов *i*-го потока всегда должно быть строго больше средней скорости на интервале средней длительности сеанса для рассматриваемого потока, т.е. $p_i > r_i$, и это условие является обязательным для всех выражений рассматриваемых ниже, что не противоречит физическому смыслу реальных процессов в сети.

Поток на выходе системы управления потоками VPN-шлюза при резервировании доли КР *k*-го канала связи с пропускной способностью $R_{\text{КС}}$ для *i*-го потока данных R_i (байт/с) при условии, что $\sum_{i=1}^{n} R_i \leq R_{\text{КС}}$, описывается функцией обслуживания $W_i(t)$, определяющей минимальный объем данных, переданных в канал связи за время *t*:

$$W_i(t) = R_i(t - t_{\text{зап}\,i}), \tag{2.3}$$

где $t_{\text{зап}\,i}$ представлена выражением 2.4:

$$t_{\text{зап}\,i} = \frac{L_i}{R_i} + \frac{L_i}{R_{\text{КС}}}. \qquad (2.4)$$

Функция обслуживания планировщика WFQ представляет собой функцию «скорость-запаздывание» с характеристиками скорости R_i и запаздывания $t_{\text{зап}\,i}$ в секундах.

Исходя из того, что задержка передачи пакета от VPN-шлюза сети доступа до ПМ транспортной сети не учитывается, описание потоков в системе управления потоками VPN-шлюза можно применить к формирователю трафика ПМ транспортной сети. Тогда объемные характеристики потоков данных на выходе формирователя трафика ПМ транспортной сети ЗКМСС могут быть представлены следующим образом (рисунок 2.1).

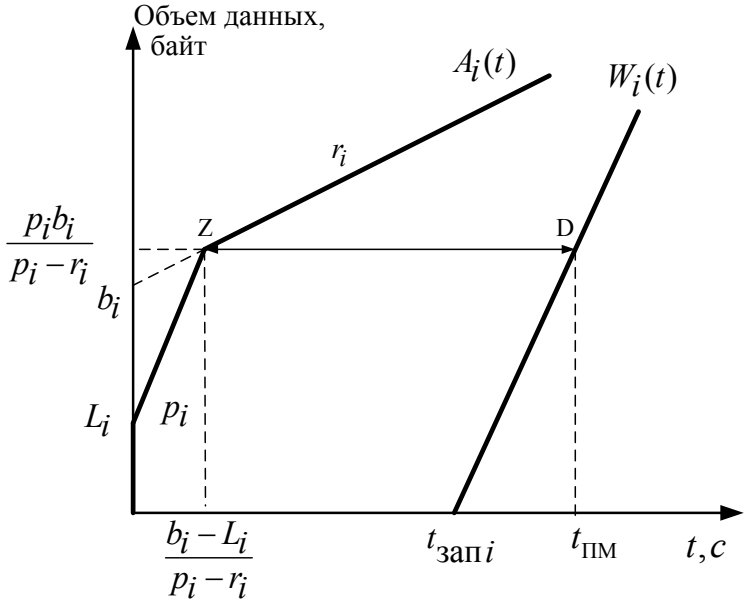


Рисунок 2.1 – Графическое представление объемных характеристик потоков данных на выходе сетевого устройства защищенной корпоративной мультисервисной сети связи

На данном рисунке показаны функции поступления и обслуживания нагрузки, иллюстрирующие порядок расчета параметров, характеризующих обеспечение гарантированного КО на наихудший случай. На вход планировщика «взвешенной справедливой очередности» WFQ подается

нагрузка, пропущенная через формирователь трафика "корзина маркеров", что в свою очередь позволяет формально описать нагрузочные характеристики потоков с переменной скоростью [43,134]. Данный алгоритм позволяет применять какие-либо действия (сброс или перемаркировку) только лишь к пакетам, которые не соответствуют заявленному профилю, а конформные пакеты проходят через «корзину с маркерами» без дополнительной задержки, связанной с ограниченной интенсивностью исходящей нагрузки [111].

В системах управления допуском потоков данных в сеть немаловажным достоинством математического аппарата описания параметров трафика на выходе сетевых устройств является минимальное время вычисления требуемого КР [15,20,44]. Особенно, когда интенсивность поступления заявок на обслуживание в ЗКМСС и требования ко времени допуска потока данных не позволяют использовать сложные в вычислительном плане аналитические выражения без значительного увеличения производительности процессоров.

В рамках решения задачи обеспечения требуемого уровня КО каждого поступающего в ПМ транспортной сети потока данных посредством оценивания верхней задержки обработки пакетов в ПМ, исходя из предположения, что механизм обслуживания реализован на базе одного из планировщиков класса WFQ, задержка для i-го потока не должна превышать значения, представленного выражением (1.3): $t_{\text{ПМ}} \le \frac{t(\text{треб}) - t_{\text{КС}} - 2t_{\text{Ш}}}{2}$.

Исходя из подхода, представленного в [47], на основе известных функций поступления и обслуживания становится возможным рассчитать значения управляемых параметров обслуживающей системы, определяемых на рисунке 2.1 положением прямой ZD, как верхней границы суммарной задержки пакета в ПМ и условии, что $p_i > r_i$:

$$t_{\text{ПМ}} = \begin{cases} \dfrac{(b_i - L_i)(p_i - R_i)}{R_i(p_i - r_i)} + \dfrac{2L_i}{R_i} + \dfrac{L_i}{R_{\text{КС}}}; & p_i > R_i > r_i, \\ \dfrac{2L_i}{R_i} + \dfrac{L_i}{R_{\text{КС}}}, \ R_i > p_i > r_i. \end{cases} \quad (2.5)$$

Здесь $t_{\text{ПМ}}$ имеет физический смысл верхнего граничного значения времени задержки, гарантирующего требуемый уровень КО поступающих в ПМ потоков данных, и может быть обеспеченно при резервировании пропускной способности R_i (в байтах/сек) в ПМ для обслуживания.

Значение $t_{\text{ПМ}}$ в свою очередь зависит от значения выделяемой обслуживаемому потоку полосы пропускания R_i.

Основой функционирования узла доступа к транспортной сети ЗКМСС при управлении допуском потоков данных является оценивание требуемого КР для агрегированного потока данных VPN-туннеля. При этом КР, выделяемый потоку, является важнейшим из ресурсов сети. Несмотря на то, что буферное пространство порта коммутационного оборудования также является разделяемым ресурсом, для расчета которого требуются точные аналитические выражения, стоимость элементов памяти, реализующих функционирование буфера значительно меньше, чем стоимость аренды КР транспортной сети [61,91]. В этой связи примем допущение, что буфер ПМ имеет бесконечную длину.

При эксплуатации сети связи зачастую возникает обратная задача – на основании выражения (2.5), при заданной требуемой сквозной задержке пакета *i*-го потока данных «из конца в конец» $t(\text{треб})$, определяемой рекомендацией Y.1541, требуется оценить необходимый КР для обслуживания предложенной нагрузки, выделяемый на ПМ:

$$R_i = \frac{p_i \dfrac{b_i - L_i}{p_i - r_i} + 2L_i}{t_{\text{ПМ}} + \dfrac{b_i - L_i}{p_i - r_i} - \dfrac{L_i}{R_{\text{КС}}}}. \quad (2.6)$$

Анализ структуры ЗКМСС показал, что в VPN-шлюзе реализуется агрегирование потоков данных в общий поток VPN-туннеля при передаче и разделение на подпотоки на приеме [6,101,137].

Для аналитического описания агрегированного потока данных, поступающего с выходного порта сетевого элемента, воспользуемся представленной в RFC 2216 [112] концепцией характеризации трафика агрегированных потоков, согласно которой сумма n потоков данных, специфицированных как TSpec, описывается суммарной функцией поступления (СФП) $A_{\text{СФП}}(t)$:

$$A_{\text{СФП}}(t)=\begin{cases} L_i + p_{\text{СФП}} t & t < \dfrac{b_i - L_i}{p_{\text{СФП}} - r_{\text{СФП}}}; \\ b_i + r_{\text{СФП}} t & t \geq \dfrac{b_i - L_i}{p_{\text{СФП}} - r_{\text{СФП}}}, \end{cases} \tag{2.7}$$

где L_i – максимальная длина пакета i-го потока из n потоков, входящих в состав агрегированного потока данных VPN-туннеля, $p_{\text{СФП}}$ – пиковая скорость генерации пакетов агрегированного потока VPN-туннеля, $r_{\text{СФП}}$ – средняя скорость генерации пакетов агрегированного потока VPN-туннеля, b_i (байт) – выделенный размер буфера формирователя трафика агрегированных потоков VPN-туннелей, равный размеру буфера, выделяемого для обслуживания i-го потока из n потоков, входящих в состав агрегированного потока данных VPN-туннеля.

Для оценивания требуемого КР для агрегированных потоков данных в теории сетевых исчислений разработаны модели изолированного обслуживания потоков данных (выражение 2.8) и модель группового обслуживания потоков данных на основе СФП (выражение 2.9):

$$R_{\text{изол}}(n)=\sum_{i=1}^{n}\frac{p_i\dfrac{(b_i-L_i)}{(p_i-r_i)}+2L_i}{t_{\text{ПМ}}+\dfrac{(b_i-L_i)}{(p_i-r_i)}-\dfrac{L_i}{R_{\text{КС}}}}, \tag{2.8}$$

$$R_{\text{СФП}}(n) = \frac{\sum_{i=1}^{n} p_i \frac{\sum_{i=1}^{n} b_i - L_i}{\sum_{i=1}^{n}(p_i - r_i)} + 2L_i}{t_{\text{ПМ}} + \frac{\sum_{i=1}^{n} b_i - L_i}{\sum_{i=1}^{n}(p_i - r_i)} - \frac{L_i}{R_{\text{КС}}}}, \quad (2.9)$$

где n – количество потоков в составе агрегированного потока данных, i – порядковый номер потока, входящего в состав агрегированного потока данных, L_i – максимальный размер пакета данных i-го потока, выбранный из всех n потоков агрегированного потока данных, $t_{\text{ПМ}}$ – минимально требуемая задержка к обработке пакета в ПМ среди n потоков данных, $R_{\text{КС}}$ – пропускная способность канала связи, p_i – пиковая скорость генерации пакетов i-го потока, r_i – средняя скорость генерации пакетов i-го потока, b_i – выделенный размер буфера формирователя трафика для i-го потока.

Выражение (2.7) позволяет описать наихудший случай генерации трафика n источниками, на основе которого становится возможным вычислить требуемый КР для n потоков с учетом обеспечения $t_{\text{ПМ}}$ из всех поступивших требований к КО. При этом агрегированный поток данных обслуживается в маршрутизаторах транспортной сети ЗКМСС как изолированное соединение с дисциплиной обслуживания *FIFO* в отдельно зарезервированном буфере [41,117].

Исследование применимости модели изолированного обслуживания потоков данных и модели группового обслуживания потоков данных на основе СФП для расчета КР трафика ЗКМСС проведена на экспериментальном стенде с применением сетевого и криптографического IP/MPLS оборудования, применяемого в сегменте ЗКМСС ПАО АКБ

«Авангард» Центрального федерального округа. Структурная схема экспериментального стенда представлена на рисунке 2.2.

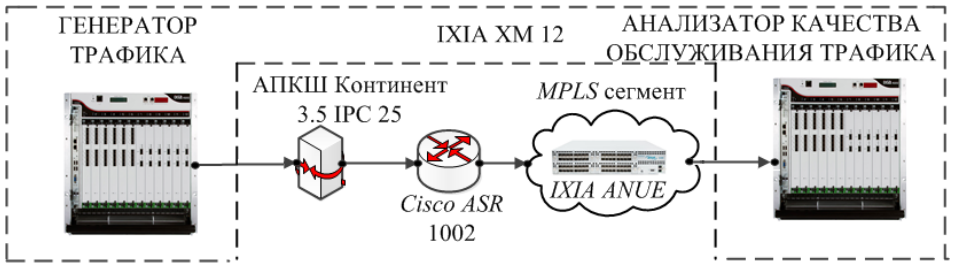


Рисунок 2.2 – Структурная схема экспериментального стенда сегмента защищенной корпоративной мультисервисной сети связи

Подготовительная стадия исследования:

– сборка схемы (рисунок 2.2), подключение устройств и настройка работоспособного состояния исследуемого фрагмента ЗКМСС;

– настройка генератора трафика;

– настройка механизмов управления трафиком и поддержания требуемого КО (выбор дисциплины обслуживания, средств управления нагрузкой, размера буфера и порядка обслуживания пакетов).

Основная стадия исследования.

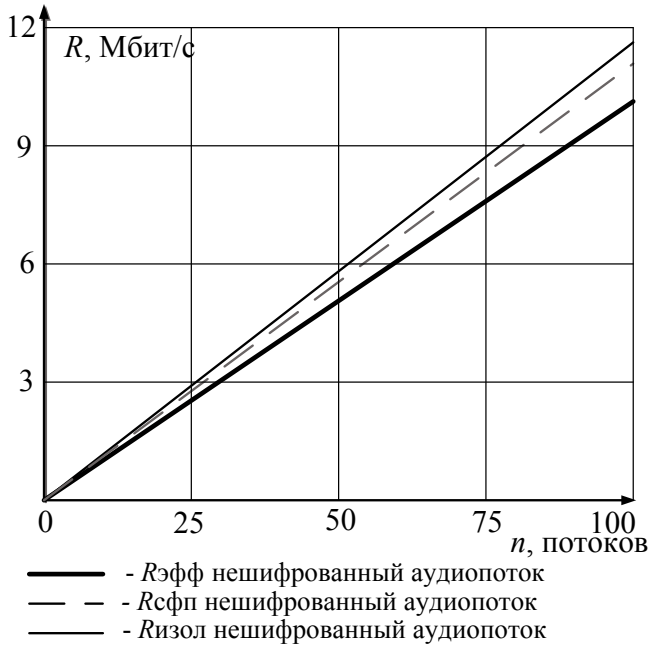
Численные значения параметров потоков данных, генерируемого терминальным оборудованием характерным для ЗКМСС ПАО АКБ «Авангард», полученные на первом этапе исследования влияния процедур функционирования VPN-шлюза на параметры передаваемого трафика ЗКМСС (описание эксперимента (рисунок 1.6), значения параметров трафика (таблица 1.5) представлены в разделе 1.6), были использованы при расчете требуемого КР с использованием существующей модели изолированного обслуживания потоков данных - выражение (2.8) и модели группового обслуживания потоков данных на основе СФП - выражение (2.9) [63,74].

По имеющимся статистическим данным пиковой и средней скорости передачи данных (таблица 1.5) генератором трафика IXIA XM 12

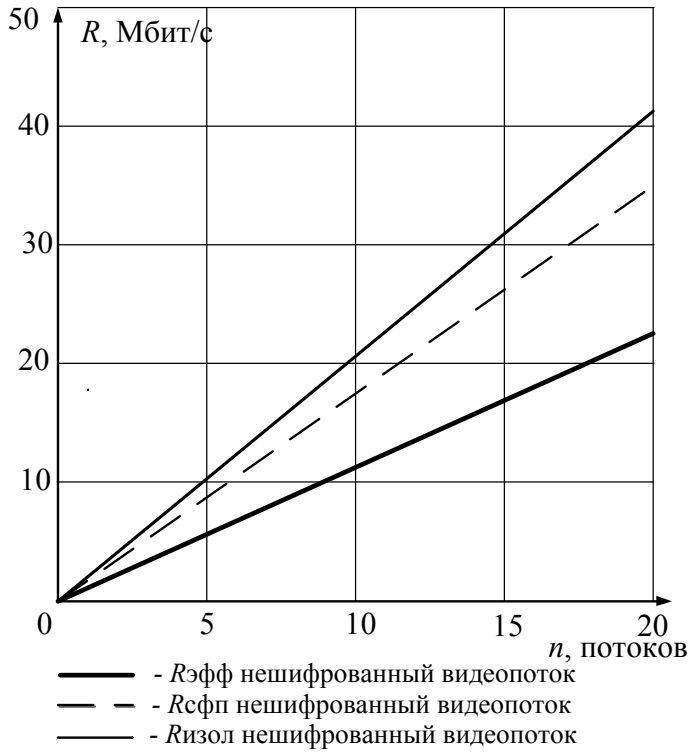
формируется тестовая нагрузка. Эмулятором IP-каналов ANUE Network Emulator вносится задержка обработки пакетов, характерная транспортному сегменту ЗКМСС. Сгенерированная нагрузка поступает на обслуживание в IP/MPLS пограничный маршрутизатор Cisco ASR 1002.

Исследовался суммарный поток данных при группировании 100 потоков IP-телефонии и 20 потоков видеотелефонии. Данные численные значения являются исходными данными федерального уровня ЗКМСС ПАО АКБ «Авангард». Исследуемым параметром выступала максимальная задержка обработки пакета в ПМ при резервировании КР, оцененного с помощью существующих математических моделей агрегированного потока данных - выражения (2.8), (2.9). Численное значение требуемой задержки обработки пакета в ПМ не должно превышать 10 мс исходя из физической и логической топологии данной ЗКМСС в соответствии с рекомендацией Y.1541 [58].

Рассчитанные значения требуемого КР в зависимости от поступающей нагрузки при описании поведения агрегированного потока с использованием существующей модели изолированного обслуживания потоков данных - выражение (2.8) и модели группового обслуживания потоков данных на основе СФП - выражение (2.9) представлены на рисунке 2.3.



а



б

Рисунок 2.3 – Оцененые значения требуемого канального ресурса для обслуживания группированного потока а) IP-телефонии и б) видеотелефонии

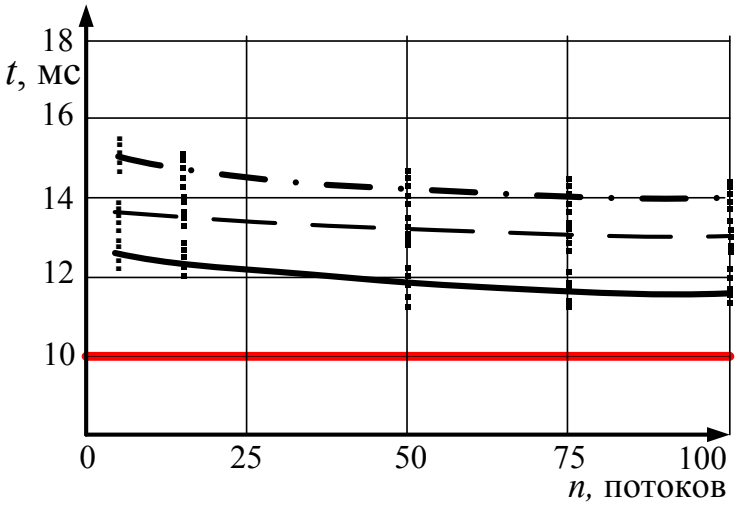
На рисунке 2.3 *R*эфф – значение резервируемого КР для *n* потоков сервисов реального времени, полученное на основе расчёта эффективной скорости передачи информационного потока [69,97] согласно выражения:

$$R_{\text{эфф}}(n) = n(1 - \frac{1}{50}\log P_{loss})r_i\ (1 + 3(-\frac{2p_i}{R_k}\log P_{loss})(1 - \frac{r_i}{p_i}))\ ,$$

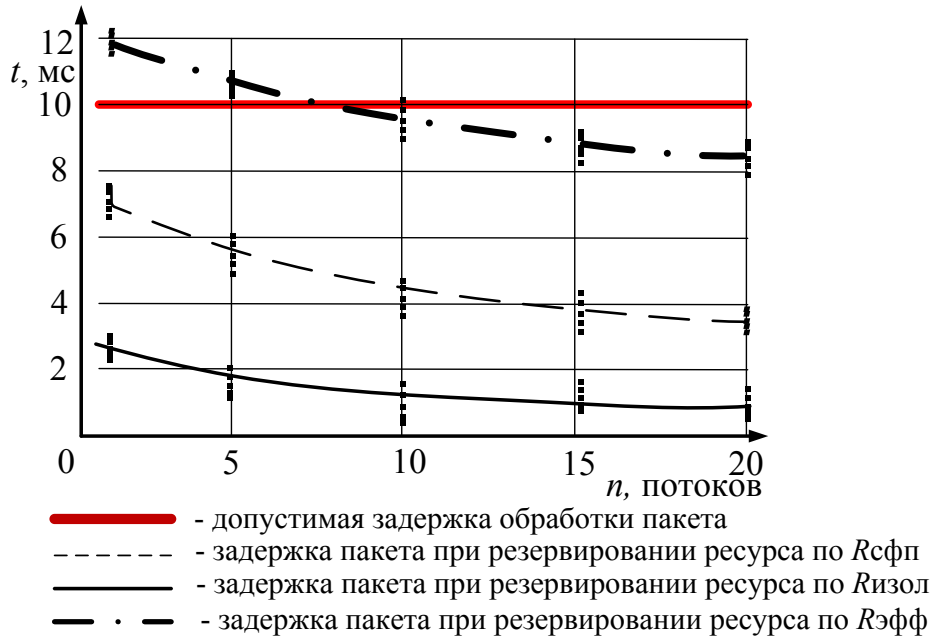
где P_{loss}=10^{-3} – коэффициент потери пакетов для 0-класса качества обслуживания.

Заключительная стадия исследования.

Оцененные максимальные значения достижимой задержки для трафика IP-телефонии и видеотелефонии, а также кривая, соединяющая их средние значения, представлены на рисунке 2.4 соответственно.



а



б

Рисунок 2.4 – Экспериментальное оценивание максимально-достижимой задержки в пограничном маршрутизаторе а) IP-телефония, б) видеотелефония

Анализ полученных зависимостей свидетельствует о том, что при расчете требуемого КР по существующим моделям агрегированных потоков для обслуживания трафика шифрованной IP-телефонии не обеспечивается требуемая задержка обработки пакетов данных в ПМ. При обслуживании потоков шифрованной видеотелефонии заданный уровень КО

обеспечивается за счет превышения зарезервированного ресурса пиковой достижимой скорости передачи.

Результаты эксперимента свидетельствует о несоответствии скорости поступления пакетов скорости их обслуживания: в первом случае выделенный КР меньше пиковой скорости передачи, во втором наоборот превышает ее. Незначительный разброс экспериментальных оценок достижимой задержки при различных опытных итерациях сводит к минимуму возможность проявления случайных выбросов [67].

Невозможность реализации существующих математических моделей в ЗКМСС приводит к необходимости статичного закрепления КР за каждым предоставляемым сервисом с ориентацией на пиковую возможную нагрузку. С учетом предложенного подхода коэффициент суточной загрузки арендуемых каналов транспортного уровня ЗКМСС ПАО АКБ «Авангард» Центрального федерального округа РФ представлен на диаграмме.

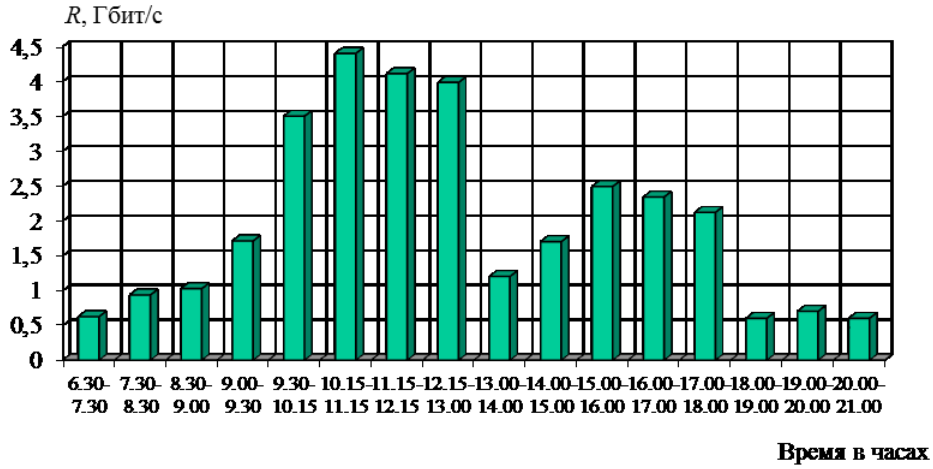


Рисунок 2.5 – Степень загруженности арендуемых каналов связи транспортной сети ЗКМСС ПАО АКБ «Авангард»

Из диаграммы видно, что аренда КР под пиковую нагрузку позволяет гарантировать требуемый уровень КО в течение суток, однако примерно 60% времени загрузка транспортного канала не превышает 40% уровня загрузки. Нетрудно рассчитать экономические убытки от недоиспользования арендуемого КР. На электронном портале для осуществления закупок государственными и юридическими компаниями представлена информация

по ориентировочной стоимости аренды пропускной способности 1 Мбит/с и отображена в таблице для услуг MPLS VPN в интересах ПАО АКБ «Авангард» Центрального федерального округа РФ.

Таблица 2.1 – Стоимость услуг по предоставлению VPN услуг для ПАО АКБ «Авангард»

ЗКМСС	Средняя стоимость 1 Мбит/с, рублей в месяц	Количество информационных направлений	Стоимость оказания услуг VPN, млн. рублей в год
Федеральный уровень ЗКМСС	2000	40-60	3-4

Так в среднем при аренде 40-60 VPN каналов для организации федерального уровня ЗКМСС по 100 Мбит/с каждый ежегодные затраты составляют порядка 3-4 млн. руб. в год. Ущерб от недоиспользования арендуемого канального ресурса обходится корпорации в 0,5-1,2 млн. руб. в год.

2.3. Разработка алгоритма динамического резервирования канального ресурса агрегированного потока данных

Под трафиком, генерируемым терминальным оборудованием ЗКМСС, в работе рассматривается поток пакетов дискретной длины, поступающих в сеть через стохастичные промежутки времени. Именно стохастичность, а не случайность межпакетного интервала, свидетельствует о возможности описания данных параметров трафика известными статистическими законами распределения значений случайной величины [84,92]. Поступающий поток пакетов создает нагрузку на обслуживающие приборы сетевых устройств, которая оценивается той работой, которую сеть выполняет при их передаче. Критичным с точки зрения обеспечения КО, предъявляемого инфокоммуникационными сервисами к сети, является время,

необходимое для передачи пакета (время коммутации), которое определяет пропускную способность сети связи и зависит от параметров конфигурирования используемого сетевого оборудования. Время передачи пакета зависит от его длины и скорости передачи линии связи. Пакеты, поступающие в узел коммутации в то время, когда передается очередной пакет, помещаются в буфер маршрутизатора, где ожидают своей очереди на передачу. Если количество ожидающих в очереди пакетов достигает некоторой заданной величины, то вновь поступающие пакеты удаляются. Данная схема обслуживания трафика в сетях с коммутацией пакетов присуща всем сетевым устройствам, в этой связи их конфигурирование представляет собой сложную задачу, зачастую априорно формализовано не решаемую и требующую эмпирического подхода [10,96].

Численные значения параметров трафика, генерируемого терминальным оборудованием, характерным для ЗКМСС, зафиксированные на пограничном маршрутизаторе транспортной сети ЗКМСС ПАО АКБ «Авангард» после прохождения VPN-щлюза, были получены на втором этапе исследования влияния процедур функционирования VPN-шлюза на параметры передаваемого трафика ЗКМСС и описаны в разделе 1.6 (обобщенная схема экспериментального стенда эксперимента представлена на рисунке 1.8, численные значения исследуемых параметров, необходимые для настройки формирователей трафика на сетевых устройствах, находящихся в направлении «из конца в конец» - таблица 1.6). Результаты статистического эксперимента для условий штатного функционирования системы управления потоками данных в VPN-шлюзе, а также для условия возникновения перегрузки позволили ввести поправочные коэффициенты α, β, γ для соответствующих параметров передаваемого трафика, учитывающие искажения, вносимые криптомодулем.

Учет влияния VPN-шлюза на параметры генерируемого трафика, выявленный на данном этапе, дает возможность усовершенствовать существующие модели агрегированных потоков данных в элементах мгновенной пиковой и средней скоростей передачи данных на выходе

VPN-шлюза и максимальных длин генерируемых пакетов [64].

При настройке формирователя трафика в VPN-шлюзе с целью формирования поступающего трафика *i*-го потока данных наихудший возможный случай расположения пакетов на его выходе приобретает детерминированный характер и может быть описан следующим выражением [62]:

$$A_i(t) = \begin{cases} \gamma L_i + \alpha p_i t \quad t < \dfrac{b_i - \gamma L_i}{\alpha p_i - \beta r_i}; \\ b_i + \beta r_i t \quad t \geq \dfrac{b_i - \gamma L_i}{\alpha p_i - \beta r_i}. \end{cases} \tag{2.10}$$

Тогда верхние граничные значения достижимой задержки пакета *i*-го потока в пограничном маршрутизаторе $t_{\text{ПМ}}$ при зарезервированном для него КР R_i :

$$t_{\text{ПМ}} = \begin{cases} \dfrac{(b_i - \gamma L_i)(\alpha p_i - R_i)}{R_i(\alpha p_i - \beta r_i)} + \dfrac{2\gamma L_i}{R_i} + \dfrac{\gamma L_i}{R_{\text{КС}}}; \\ \dfrac{2\gamma L_i}{R_i} + \dfrac{\gamma L_i}{R_{\text{КС}}}. \end{cases} \tag{2.11}$$

Эффект в ресурсопотреблении при агрегированном обслуживании потоков данных будет наблюдаться только при резервировании для каждого потока КР, ориентированного на эффективную скорость передачи данных, т.е. при выполнении условия: $\alpha p_i > R_i > \beta r_i$.

С учетом вышеизложенного объемные характеристики *i*-го потока данных на выходе формирователя трафика VPN-шлюза и ПМ транспортной сети ЗКМСС представлены на рисунке 2.6:

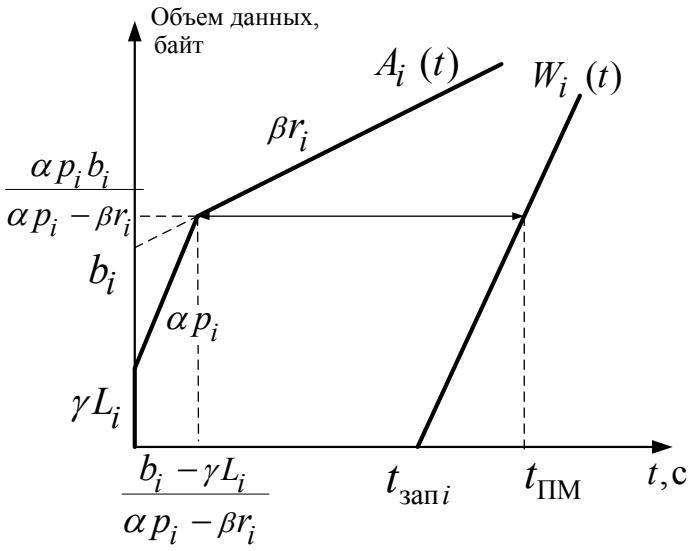


Рисунок 2.6 – Графическое представление объемных характеристик потоков данных на выходе VPN-шлюза и пограничного маршрутизатора

Для описания поведения агрегированного потока, т.е. потока данных VPN-туннеля, состоящего из n ПДРВ, усовершенствованная математическая модель шифрованного агрегированного потока данных представлена выражениями:

$$R_{\text{VPN}}^{\text{изол}}(n) = \sum_{i=1}^{n} \frac{\alpha p_i \dfrac{(b_i - \gamma L_i)}{(\alpha p_i - \beta r_i)} + 2\gamma L_i}{t_{\text{ПМ}} + \dfrac{(b_i - \gamma L_i)}{(\alpha p_i - \beta r_i)} - \dfrac{\gamma L_i}{R_{\text{КС}}}}, \tag{2.11}$$

$$R_{\text{VPN}}^{\text{СФП}}(n) = \frac{\sum\limits_{i=1}^{n} \alpha p_i \dfrac{\sum\limits_{i=1}^{n} b_i - \gamma L_i}{\sum\limits_{i=1}^{n} (\alpha p_i - \beta r_i)} + 2\gamma L_i}{t_{\text{ПМ}} + \dfrac{\sum\limits_{i=1}^{n} b_i - \gamma L_i}{\sum\limits_{i=1}^{n} (\alpha p_i - \beta r_i)} - \dfrac{\gamma L_i}{R_{\text{КС}}}}, \tag{2.12}$$

где n – количество ПДРВ в составе шифрованного агрегированного потока данных VPN-туннеля, i – порядковый номер потока, входящего в состав

агрегированного потока данных VPN-туннеля, L_i – максимальный размер пакета данных *i*-го потока, выбранный из всех *n* потоков агрегированного потока данных VPN-туннеля, $t_{\text{ПМ}}$ – минимально требуемая задержка к обработке пакета в ПМ среди *n* потоков данных, $R_{\text{КС}}$ – пропускная способность канала связи. При этом, пиковая скорость генерации пакетов *i*-го потока – p_i, средняя скорость генерации пакетов *i*-го потока – r_i, выделенный размер буфера формирователя трафика для *i*-го потока – b_i являются постоянными для всех *n* потоков агрегированного потока данных VPN-туннеля. Данные значения параметров трафика были оценены на узле доступа в транспортную сеть в результате проведения полунатурного эксперимента, описанного в разделе 1.4., при использовании терминального оборудования, характерного для ЗКМСС и представлены в таблице 1.5.

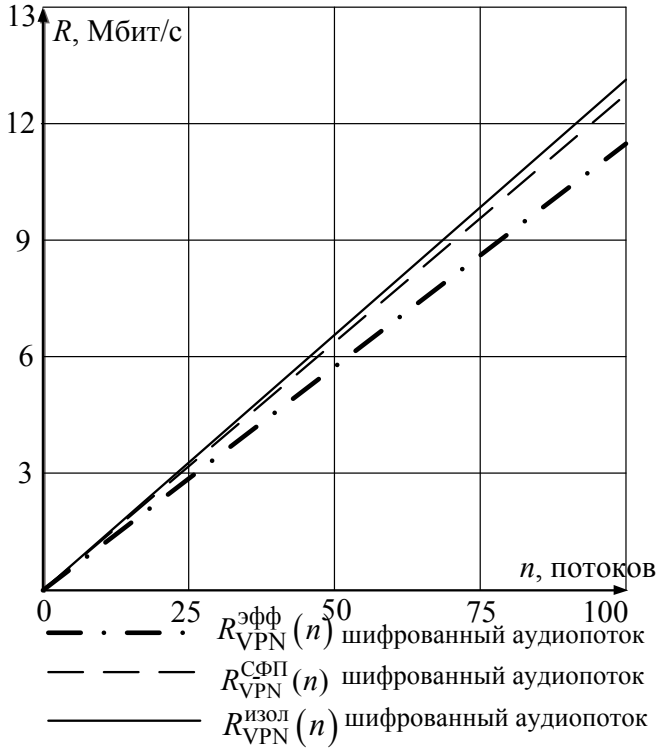
Усовершенствованная математическая модель шифрованного агрегированного потока данных на основе модели эффективной скорости передачи информационного потока представлена выражением (2.13):

$$R_{\text{VPN}}^{\text{эфф}}(n) = n(1-\frac{1}{50}\log P_{loss})\beta r_i\ (1+3(-\frac{2\alpha p_i}{R_{\text{КС}}}\log P_{loss})(1-\frac{\beta r_i}{\alpha p_i})), \qquad (2.13)$$

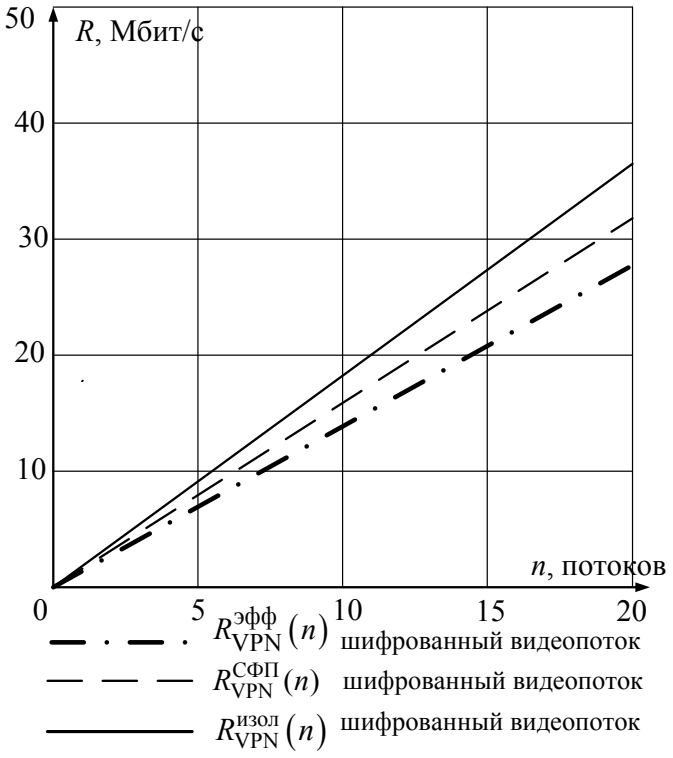
где P_{loss}=10^{-3} – коэффициент потери пакетов для 0-класса качества обслуживания.

Рассчитанные значения требуемого КР в зависимости от поступающей нагрузки при описании поведения агрегированного потока суммой изолированных, а также на основе СФП, при максимально допустимой задержке обработки пакета группового потока в пограничном маршрутизаторе, равной 10 мс, представлены на рисунке 2.7. Выполнено аналитическое сравнение усовершенствованной модели агрегированного потока данных сервисов реального времени с моделью агрегированного потока на основе эффективной скорости передачи $R_{эфф}$ для 0-класса качества обслуживания (рис. 2.7). Сравнение проводилось применительно к сети

доступа реальной ЗКМСС при ограничении $t_{\text{ПМ}}$ = 10 мс и допустимом коэффициенте потерь P_{loss} =10^{-3}.



а



б

Рисунок 2.7 –Результаты численного анализа модели агрегированного потока данных сервисов реального времени а) видеотелефонии, б) IP-телефонии

2.4. Исследование свойств алгоритма динамического резервирования канального ресурса агрегированного потока данных

Как отмечено в [27,32], усовершенствованная математическая модель шифрованного агрегированного потока данных в разработанном алгоритме динамического резервирования канального ресурса агрегированного потока данных должна быть чувствительна к изменению входных параметров, численные значения выходных параметров должны быть достоверны и не выходить за область допустимых значений при выборе допустимых значений входных параметров. Кроме того, немаловажно, чтобы выходная реакция данной модели оставалась устойчивой при незначительном изменении входных параметров. Как правило, исследование математических моделей производится методами статистического анализа экспериментальных данных [54]. Для исследования чувствительности необходимо произвести формальное описание функционирования сетевых элементов ЗКМСС при предоставлении услуг защищенной IP-телефонии и видеотелефонии.

Оценку чувствительности усовершенствованной математической модели необходимо произвести для различных условий функционирования ЗКМСС. Диапазон изменения входных данных должен соответствовать нагрузочным характеристикам федерального уровня ЗКМСС ПАО АКБ «Авангард» (таблица 2.2).

Таблица 2.2 – Нагрузочные характеристики защищенной корпоративной сети связи

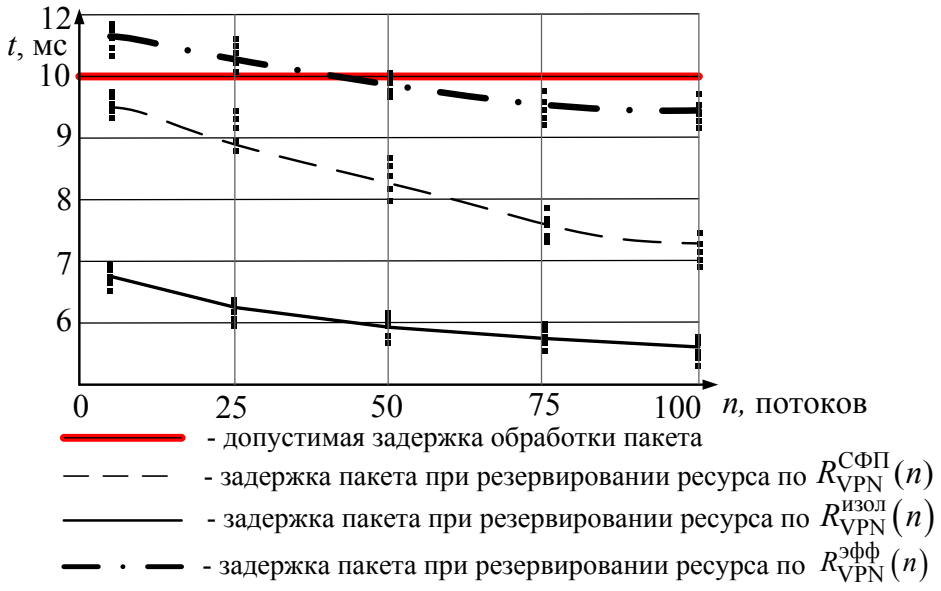
Услуга	N^{TA} ед.	Z^{TA} Эрл	p Мбит/с	r Мбит/с	L Байт	Арендуемый канальный ресурс, Мбит/с
IP-телефония	250	0,4	0,126	0,107	254	100
Видеотелефония	70	0,2	1,74	1,22	1392	

Моделирование функционирования сегмента ЗКМСС при предоставлении сервисов IP-телефонии и видеотелефонии с различными

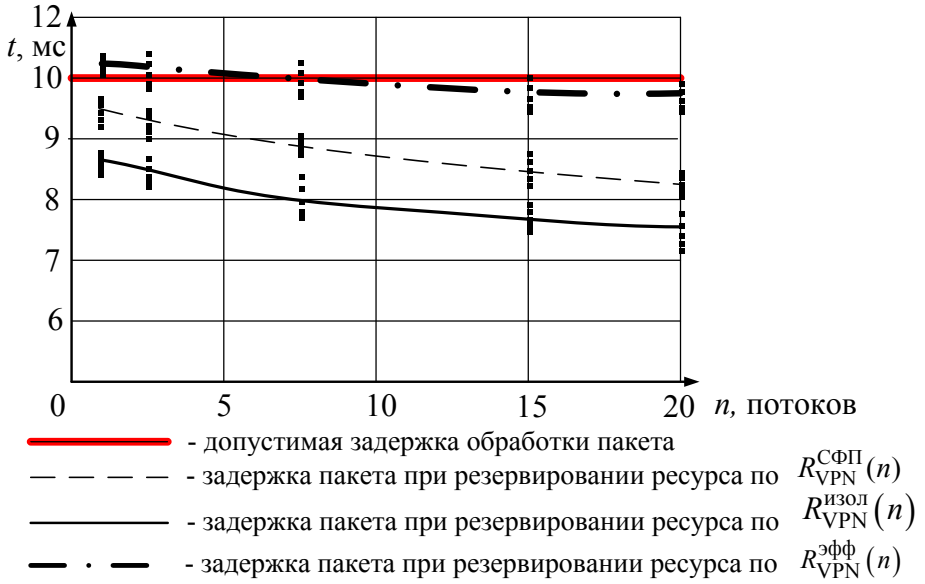
параметрами трафика как на уровне соединений (мгновенная пиковая и средняя скорость передачи данных), так и на уровне пакетов (длина пакетов, межпакетный интервал) позволит всесторонне исследовать зависимость между достижимым уровнем КО, предложенной нагрузкой и внутренней конфигурацией планировщика и системы управления потоками.

Экспериментальное исследование адекватности усовершенствованной математической модели проводилось на стенде транспортной IP/MPLS сети связи, структурная схема которого представлена на рисунке 2.2. Был спланирован и проведен однофакторный имитационный эксперимент, функцией отклика которого были выбраны значение $t_{\text{ПМ}}$ агрегированного потока данных реального времени, а фактором – резервируемого КР.

Исследовался суммарный поток данных при агрегировании 100 потоков IP-телефонии и 40 потоков видеотелефонии. Максимально достижимая задержка обработки пакета в ПМ оценивалась с помощью полунатурного эксперимента. Источником нагрузки с заданными характеристиками пиковой и средней скорости (таблица 1.5) выступал генератор трафика IXIA XM12. Задержка пакетов при распространении в сегменте транспортной MPLS сети воспроизводилась эмулятором IP-каналов IXIA ANUE. Результаты эксперимента представлены на рисунке 2.8.



а



б

Рисунок 2.8 – Экспериментальное оценивание максимально достижимой задержки в пограничном маршрутизаторе: а) IP-телефония, б) видеотелефония

Экспериментальное исследование разработанного алгоритма динамического резервирования канального ресурса агрегированного потока данных показало возможность оценки с помощью усовершенствованной математической модели шифрованного агрегированного потока требуемого КР для обслуживания поступающей нагрузки с гарантированным качеством. При обслуживании агрегированного потока IP-телефонии и видеотелефонии задержка обработки пакетов данных в ПМ не превышает заданное значение, в то время как при использовании модели на основе эффективной скорости передачи данное условие не выполняется на всем диапазоне входных данных.

2.5. Выводы по второму разделу

1. Эффективное функционирование системы управления допуском ЗКМСС в значительной степени зависит от точности оценивания требуемого канального ресурса сети для обслуживания потоков данных. Задача

оценивания канального ресурса сети наиболее остро стоит для агрегированного потока данных в ЗКМСС после VPN-шлюза, где отсутствует возможность наблюдения за каждым отдельным потоком данных и его измерения.

2. В ходе предварительных исследований и в результате моделирования показано, что при изолированном обслуживании потоков данных в сегменте сети доступа с IntServ решение задачи гарантированного качества обслуживания наилучшим образом реализуется на основе известной модели услуги гарантированной доставки. Данная модель основана на использовании планировщиков WFQ «с контролем скорости передачи», которые массово внедрены в существующие пограничные маршрутизаторы сегмента DiffServ.

3. Потоки данных после шифрования передаются как агрегированный поток данных. Ресурсы для обслуживания агрегированных потоков данных могут быть оценены на основе разработанного алгоритма динамического резервирования канального ресурса.

4. Экспериментальные исследования разработанного алгоритма динамического резервирования канального ресурса показали возможность получения достоверных результатов при оценивании требуемого канального ресурса для обслуживания поступающей нагрузки с требуемым качеством.

5. В отличие от применяемого в настоящее время подхода к резервированию сетевых ресурсов разработанный алгоритм динамического резервирования канального ресурса за счет учета влияния VPN-шлюзов на параметры трафика позволяет обеспечить требуемый уровень качества обслуживания потоков данных сервисов реального времени.

Раздел 3

Разработка алгоритма допуска потоков в транспортную сеть защищенной корпоративной мультисервисной сети связи и исследование его свойств

3.1. Введение

В данном разделе диссертации разрабатывается алгоритм допуска потоков данных в транспортную сеть ЗКМСС. Реализовать данный алгоритм возможно только на VPN-шлюзе, предназначенном для управления потоками данных, их фильтрацией, организацией приоритетного допуска потоков данных в VPN-туннели. Разрабатываемый на случай возникновения перегрузки алгоритм должен, прежде всего, оценивать состояние сети и по полученным результатам выполнять функции управления допуском потоков данных с учетом их приоритетов.

Выбор метода решения оптимизационной задачи максимизации загрузки имеющегося КР приоритетным трафиком зависит от размерности входных данных и их природы, а также от выбранных критериев перераспределения, которые в свою очередь зависят от конфигурирования сети и принятых правил ее функционирования.

На основании критериев эффективности использования арендуемого КР в нештатном режиме функционирования ЗКМСС, представленном в подразделе 3.2, разрабатывается алгоритм допуска потоков данных в транспортную сеть ЗКМСС, эффективность от внедрения которого исследуется методами имитационного моделирования.

3.2. Выработка и обоснование критериев эффективного использования канального ресурса

Разработка алгоритма допуска потоков данных в транспортную сеть ЗКМСС, функционирующего в условиях перегрузки с целью максимизации объема допущенных в VPN-туннель приоритетных ПДРВ, напрямую связана с заданными критериями эффективности [75,86].

Основными показателями эффективности использования КР ЗКМСС в условиях перегрузки являются:

– максимальная загрузка КР, зарезервированного для каждого предоставляемого класса сервиса:

$$R_{\text{VPN}}^{\text{СФП}}(n) \to R_S, \tag{3.1}$$

где $R_{\text{VPN}}^{\text{СФП}}(n)$ – пропускная способность для обслуживания агрегированного потока данных VPN-туннеля, состоящего из n потоков, вычисляемая на основе модели суммарной функции поступления (СФП), R_S – КР, зарезервированный для предоставляемого класса сервиса s;

– загрузка КР должна осуществляться наиболее приоритетным трафиком:

$$\sum_{i=1}^{n} Pr_i \cdot d_i \to \max, \tag{3.2}$$

где Pr_i – значение приоритета i-го ПДРВ, d_i – индикатор допуска i-го потока данных или отказа в обслуживании:

$$d_i = \begin{cases} 1, \text{ если поток данных допускается в сеть;} \\ 0, \text{ поток данных блокируется.} \end{cases}$$

Вышеизложенные разнородные критерии сводят задачу оптимизации к многокритериальной, так как выбор возможных вариантов (альтернатив) и векторный критерий, служащий правилом выбора наилучшего варианта, производится по нескольким показателям [13,16,28]. В этой связи представим данную задачу в математическом виде: требуется выбрать альтернативу x^*

из множества допустимых альтернатив X_β, удовлетворяющих заданным ограничениям, обеспечивающую экстремальное значение векторному целевому критерию $f(x)$ [99]:

$$f(x^*) = extr(f_1(x), f_2(x), ..., f_n(x)), \quad (3.3)$$

где X_β – множество допустимых альтернатив, $f_1(x), f_2(x), ..., f_n(x)$ – частные целевые функции.

Методология системного анализа и решения задач многокритериальной оптимизации предусматривает сведение многокритериальной задачи к однокритериальной и применение существующих математических методов решения последней [49,94]. В настоящее время широко распространены следующие такие методы:

- метод главного критерия;
- лексикографический метод упорядочивания;
- метод свертывания критериев;
- метод идеальной точки;
- метод «разности оценок альтернатив»;
- последовательных уступок.

Недостатком метода главного критерия является непосредственный учет лишь одного из многих критериев. Учет остальных производится опосредовано – в виде ограничений на их допустимые значения. При применении данного метода можно столкнуться с тем, что возможно наличие нескольких «главных» критериев, противоречащих друг другу. При этом алгоритм выбора ограничений на остальные не всегда прозрачен, что может привести к пустому множеству допустимых альтернатив. Общим недостатком, присущим второму и третьему подходам, является небольшая эффективность по одному показателю качества, которая всегда может быть скомпенсирована за счет другого. Кроме того, сложность построения обобщенного критерия заключается в том, что приходится соотносить друг с другом критерии, имеющие различную природу, в силу чего оценки по ним

даются по разным шкалам. С этой точки зрения использование положительных качеств метода главного критерия позволит за счёт отсечений области допустимых решений достичь уменьшения количества перебираемых вариантов [2,81].

В качестве главного критерия в условиях перегрузки примем второй критерий оптимальности, остальные критерии будут выступать в качестве ограничений. В таком случае целевая функция функционирования разрабатываемого алгоритма в формализованном виде может быть представлена следующим выражением:

$$\forall s \in \{S\} \;\; V(n) = \sum_{i=1}^{n} Pr_i \cdot d_i \to \max \,|\, \forall i,l : \sum_{l=1}^{L} R_{\text{VPN}\,l}^{\text{СФП}}(n) \le R_{\text{КС}} \cup t_i(\text{дост.}) \le t_i \;(\text{треб.}),$$

где $\{S\}$ – множество предоставляемых сервисов, i – порядковый номер обслуживаемого ПДРВ, Pr_i – значение приоритета i-го ПДРВ, d_i – индикатор допуска i-го ПДРВ или отказа в обслуживании, L – количество VPN-туннелей для всех предоставляемых классов сервиса, $R_{\text{VPN}\,l}^{\text{СФП}}(n)$ – пропускная способность для обслуживания агрегированного потока данных l-го VPN-туннеля, состоящего из n ПДРВ, вычисляемая на основе усовершенствованной модели СФП, $t_i(\text{дост})$ – достижимая максимальная сквозная задержка пакета i-го потока данных s-го класса трафика «из конца в конец», t_i (треб) – требуемая максимальная сквозная задержка пакета i-го потока данных s-го класса трафика «из конца в конец», определяемая рекомендацией Y.1541.

С учетом вышеизложенного разрабатываемый алгоритм изначально должен производить дифференцирование поступающих в VPN-шлюз потоков данных путем присвоения приоритетов при появлении заявки на обслуживание и только в случае достаточного количества КР на всем пути следования допускать их в сеть. Технически это может быть реализовано на сеансовом уровне ЭМВОС, а вся необходимая для этого информация содержится в служебных пакетах PATH и RESV протокола RSVP.

Как известно в ЗКМСС предоставляется набор услуг с различной ресурсоемкостью, при этом процедура назначения приоритетов услугам, предоставляемым в интересах одного пользователя, возлагается на ИТ-отдел на основании требований корпоративных руководящих документов [7,41]. Так, наиболее востребованные в настоящее время услуги предлагается классифицировать на услуги служебного трафика, наивысшего, высокого, среднего, низкого и минимального приоритета (таблица 3.1).

Таблица 3.1 – Наименование приоритетов циркулирующих в ЗКМСС ПАО АКБ «Авангард» потоков данных с указанием их характеристик

Наименование приоритета	Характеристики приоритета
Служебный	Трафик немедленной передачи с использованием по возможности очередей с минимизацией сетевой задержки. Резервирование гарантированного КР. Высокая доступность. Немедленное предоставление резерва.
Наивысший	Высокая доступность услуг. Услуги с высокой степенью критичности к задержкам. Использование очередей с минимизацией сетевой задержки. Предоставление гарантированного неснижаемого КР, который может быть превышен за счет КР, зарезервированного для услуг низкого и минимального приоритетов. Полное резервирование максимального КР при аварии или перегрузке сети без возможности ее превышения.
Высокий	Высокая доступность услуг. Критичность к задержкам средняя. Предоставление гарантированного неснижаемого КР, который может быть превышен за счет КР, зарезервированного для услуг низкого и минимального приоритетов. Полное резервирование при аварии или перегрузке сети.
Средний	Обеспечивается высокая доступность. Предоставляется гарантированный КР. В случае превышения скорости передачи данных выделенного ресурса, трафик данного класса перемаркируется в класс "низкий". Обеспечивается резервирование КР по его наличию.
Низкий	Гарантируется пониженная доступность услуг. Критичность к задержкам низкая. Предоставляется минимальный гарантированный КР. Превышение КР может быть только за счет недоиспользуемого ресурса более приоритетных классов. Обеспечивается резервирование только при наличии достаточного количества резервных ресурсов.
Минимальный	Гарантируется низкая доступность услуги. Не гарантируется КР и предоставляется за счет недоиспользуемого ресурса более приоритетных классов. Обеспечивается резервирование только при наличии достаточного количества резервных КР.

Характеристики выбранных приоритетов должны четко определять принципы функционирования сетевых устройств и использования КР в условиях перегрузки. Применение процедуры ранжирования потоков данных по числовым значениям их приоритета, учитывающие категории абонентов, вид сервиса, а также длительность установившихся сеансов позволит обеспечить требуемый уровень КО и максимизировать в условиях перегрузки количество допущенных приоритетных потоков данных. В свете изложенного, задача дифференциации сервисов представляется в виде многокритериальной, где в качестве первого критерия выступает приоритет пользователя относительно его занимаемой должности и возлагаемых на него функциональных задач (данный критерий назовем административным), второй – касается вида предоставляемого данному пользователю сервиса относительно требуемого КР для его качественного предоставления.

Важно заметить, что для решения задачи дифференциации отбираются только инфокоммуникационные сервисы реального времени, служебный трафик не учитывается. При таком подходе предоставляемые инфокоммуникационные сервисы в зависимости от их требований к уровню КО и категории пользователей, пользующихся ими, могут быть классифицированы следующим образом (таблица 3.2).

Таблица 3.2 – Классификация классов трафика относительно категории пользователей

Категории пользователей услуги / Класс предоставляемой услуги	Руководители корпорации	Сотрудники финансовых отделов, руководители филиалов	Обслуживающий персонал, не руководящий состав
Трафик реального времени (телефония)	Наивысший	Высокий	Средний
Мультимедийный трафик (видеосвязь, телепрезентации)	Наивысший	Средний	Средний
Передача данных	Высокий	Низкий	Минимальный
Сигнальный и управляющий трафик	Служебный		

Административный критерий классификации пользователей ЗКМСС ПАО АКБ «Авангард» сводится к выделению следующих категорий абонентов корпорации:

0 - руководители корпорации и их заместители;

1 - руководители отделов головного подразделения, региональных филиалов;

2 - обслуживающий персонал корпорации, сотрудники.

Введем следующие обозначения для назначения приоритета ПДРВ каждого класса трафика, предоставляемого в ЗКМСС:

Pr_i – приоритет *i*-го ПДРВ, характеризующий общий для класса услуг уровень его значимости;

kat – количество категорий пользователей в ЗКМСС, которым предоставляется данный класс услуг (0, 1, 2,);

kat_i^A – категория абонента, инициирующего установление *i*-го ПДРВ;

kat_i^B – категория абонента, кому инициирован *i*-ый ПДРВ;

S – количество услуг (сервисов), предоставляемых в ЗКМСС.

Приоритет *i*-ого ПДРВ может быть вычислен согласно следующего выражения:

$$Pr_i = \left(kat - kat_i^A \right) \times S + kat_i^B . \qquad (3.4)$$

Данный подход позволяет получить непересекающиеся множества Pr_i для всех классов услуги, т. е. услуги предоставляемые пользователям более высокой категории никогда не будут иметь значения Pr_i меньшие, чем у пользователя низкой категории. Кроме того, при таком подходе имеется возможность изменений диапазонов таких используемых переменных, как количество предоставляемых сервисов и число категорий пользователей.

Таким образом, полученные на основе приведенного выражения (3.4) значения Pr_i, присвоенные каждому отдельному потоку данных (наряду с дескриптором потока), позволяют выработать критерий при решении

поставленной в первом разделе оптимизационной задачи при организации управления допуском в условиях перегрузки.

Принятие решения о допуске нового потока к обслуживанию в ЗКМСС осуществляется на основе критериев, различающихся для ее состояний: наличия ресурсов сети для обслуживания и перегрузки сети или узла доступа.

Условие, по которому производится оценка состояния сети, сводится к проверке наличия КР для каждого нового устанавливаемого потока с учетом их агрегированного обслуживания в последующем. Критерий достаточности КР для обслуживания суммарного трафика n потоков базируется на сравнении требуемого КР для обслуживания предложенной нагрузки (n уже активных ПДРВ и вновь устанавливаемых) по усовершенствованной модели агрегированного потока и зарезервированного для данного класса трафика канального ресурса ЗКМСС:

$$\sum_{l=1}^{L} R_{\mathrm{VPN}\,l}^{\mathrm{СФП}}\ (n) \le R_S\,, \tag{3.5}$$

где L – количество VPN-туннелей для s-го предоставляемого класса сервиса, $R_{\mathrm{VPN}\,l}^{\mathrm{СФП}}(n)$ – пропускная способность для обслуживания агрегированного потока данных l-го VPN-туннеля, состоящего из n ПДРВ, вычисляемая на основе усовершенствованной модели СФП, R_S – КР, зарезервированный для предоставляемого класса сервиса s. В случае невыполнения критерия (3.5) считаем, что сеть функционирует в условии перегрузки [76].

За счет сведения данной задачи к однокритериальному виду задачу управления КР при условии, что обслуживаемые потоки обладают различными приоритетами и длительностью сеансов, можно отнести к классу оптимизационных задач «рюкзачного» типа. Для решения такого класса задач необходимо из множества вариантов решений выбрать единственное, для которого значение заданной целевой функции достигает экстремума [14,52]. Такого рода задачи в зависимости от размерности входных данных

относятся к классу NP-полных задач и имеют в настоящее время множество способов решения.

Существующие методы решения данной задачи можно подразделить на точные и приближенные. К точным методам относятся: простой перебор, метод ветвей и границ, динамическое программирование. К неточным (приближенным) относятся жадные и генетические алгоритмы. Проведенный в [24,26,30] сравнительный анализ существующих алгоритмов решения задачи «о рюкзаке» представлен в таблице 3.3.

Таблица 3.3 – Сравнительный анализ существующих алгоритмов решения задачи о рюкзаке

Метод	Сложность	Достоинства	Недостатки
Полный перебор	$O(n!)$	Простота реализации; точное решение	Входные данные невелики; временная сложность
Метод ветвей и границ	$\leq O(n!)$	Возможно значительное сокращение времени; простота реализации	Работает как полный перебор
Метод динамического программирования	$O(W \cdot n)$ W-вместимость рюкзака	Независимость от вида исходных данных; точное решение	Большой объем вычислительной работы
Жадный алгоритм	$O(n \cdot \log n)$	Высокая скорость; может работать с большими значениями n; простота реализации	Решение неточное
Генетический алгоритм	Ограничен по времени	Высокая скорость; может работать с большими значениями n; независимость от вида исходных данных	Не гарантирует нахождение оптимального решения

В условиях функционирования ЗКМСС, где размерность входных данных практической задачи оптимизации достаточно велика (для федерального уровня достигает зачастую более 100 ПДРВ), а время решения данной задачи ограничено требованиями по своевременности и доступности предоставляемых сервисов, оперативность метода является приоритетным свойством при выборе.

Вышеизложенные особенности условий решения поставленной задачи позволяют пренебречь точностью получаемых оценок и необходимостью поиска глобального оптимума и ограничиться выбором одного из методов класса «жадных» алгоритмов. Одним из таких методов является алгоритм Данцига для линейной одномерной задачи о «рюкзаке», подробно представленный в [24,93].

Теорема Данцига. Пусть переменные x_j, $j=1,2,...,m$, перенумерованы так, что $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_m$, где $\lambda_j = \frac{c_j}{a_j}$ – удельный вес предметов, c_j – вес j-го предмета, a_j – ценность j-го предмета. Тогда оптимальное решение $y^0 = \left(y_1^0, y_2^0, ..., y_m^0\right)$ имеет вид:

$$y_1^0 = y_2^0 = ... = y_{z-1}^0 = 1, \tag{3.6}$$

$$y_{z+1}^0 = y_{z+2}^0 = ... = y_m^0 = 0, \tag{3.7}$$

$$y_z^0 = \frac{R - \sum_{j=1}^{z-1} a_j}{a_z}, \tag{3.8}$$

где z определяется из условия:

$$\sum_{j=1}^{z-1} a_j \leq R \leq \sum_{j=1}^{z} a_j. \tag{3.9}$$

Применительно к условиям задачи вектор допущенных потоков данных к обслуживанию в VPN-туннеле примет вид:

$$\overline{D} = \left(d_1, d_2, ..., d_n\right), \tag{3.10}$$

$$d_1 = d_2 = ... = d_{z-1} = 1, \tag{3..11}$$

$$d_{z+1} = d_{z+2} = ... = d_n = 0, \tag{3.12}$$

$$\forall s \in \{S\} \quad d_z = \frac{R_s - \sum_{l=1}^{L} R_{\text{VPN}\,l}^{\text{СФП}}(n)}{Pr_s}, \tag{3.13}$$

где Pr_s – приоритет предоставляемого *s*-го класса сервиса.

В классическом представлении задача «о рюкзаке» формулируется следующим образом: пусть имеется *n* предметов, каждый из которых имеет ценность $Pr_j > 0$ и вес $a_j > 0$, $j = 1,2,...,m$. Имеется рюкзак, грузоподъемность которого есть *R*, при этом $\sum_{j=1}^{m} a_j > R$. Необходимо положить в «рюкзак» такой набор предметов, чтобы достичь оптимального значения целевой функции (максимальная ценность взятых предметов).

Для формального описания задачи введем следующие обозначения: $\overline{Y} = (y_1, y_2, ..., y_n)$ – вектор обслуживаемых в данный момент потоков данных; $\overline{D} = (d_1, d_2, ..., d_n)$ – вектор, который определяет те потоки, выполнение которых, может быть отменено для высвобождения ресурсов:

$$d_i = \begin{cases} 1, \text{ если поток данных допускается в сеть;} \\ 0, \text{ поток данных блокируется.} \end{cases} \quad (3.14)$$

Суммарная ценность и грузоподъемность определяется следующими выражениями:

$$f(x_1, x_2, ..., x_n) = \sum_{j=1}^{m} Pr_j \cdot d_j , \quad (3.15)$$

$$g(x_1, x_2, ..., x_n) = \sum_{j=1}^{m} a_j x_j . \quad (3.16)$$

Целевая функция задачи о «рюкзаке», заключающаяся в максимизации суммарной ценности взятых предметов, оценивается по выражению:

$$\sum_{j=1}^{m} Pr_j \cdot d_j \to \max . \quad (3.17)$$

Ограничение по грузоподъемности рюкзака имеет вид:

$$\sum_{l=1}^{L} R_{\text{VPN}\,l}^{\text{СФП}}(n) \le R_s . \quad (3.18)$$

Требуется: разработать алгоритм допуска потоков в транспортную сеть ЗКМСС в условиях перегрузки позволяющий реализовать процедуру управления допуском ПДРВ к транспортному ресурсу на основе дисциплины обслуживания вызовов с фиксированным абсолютным приоритетом. Сортировка потоков, обслуживаемых на рассматриваемом шаге потоков данных по значениям приоритетов Pr_i, позволит прекращать обслуживание низкоприоритетных потоков с учетом длительности сеанса. В процессе установления сеанса связи при недостаточности КР должны приостанавливаться соединения с наименьшим приоритетом, в случае одинакового приоритета должны блокироваться соединения с большей длительностью занятия КР.

3.3. Разработка алгоритма допуска потоков в транспортную сеть защищенной корпоративной мультисервисной сети связи

Алгоритм допуска потоков в транспортную сеть ЗКМСС разрабатывается на основании полученных математических зависимостей, приведенных в разделе 2. Данный алгоритм обеспечивает допуск потоков предоставляемого сервиса в соответствующий VPN-туннель при наличии ресурсов сети для обслуживания и в условиях перегрузки сети на основе дисциплины обслуживания с фиксированным абсолютным приоритетом [77].

В качестве исходных данных для работы алгоритма выступают:

l – l-тый VPN-туннель (определяется при конфигурировании VPN-шлюза);

Pr_i – приоритет i-го потока данных;

{N} – множество обслуживаемых в VPN-шлюзе потоков данных в текущий момент времени;

{M} – множество входящих потоков данных (поступающих на обслуживание в VPN-шлюз) в текущий момент времени;

R_S – резервируемый КР для s-го класса сервиса (VPN-туннеля);

S – количество классов сервисов.

Блок схема разрабатываемого алгоритма представлена на рисунке 3.1.

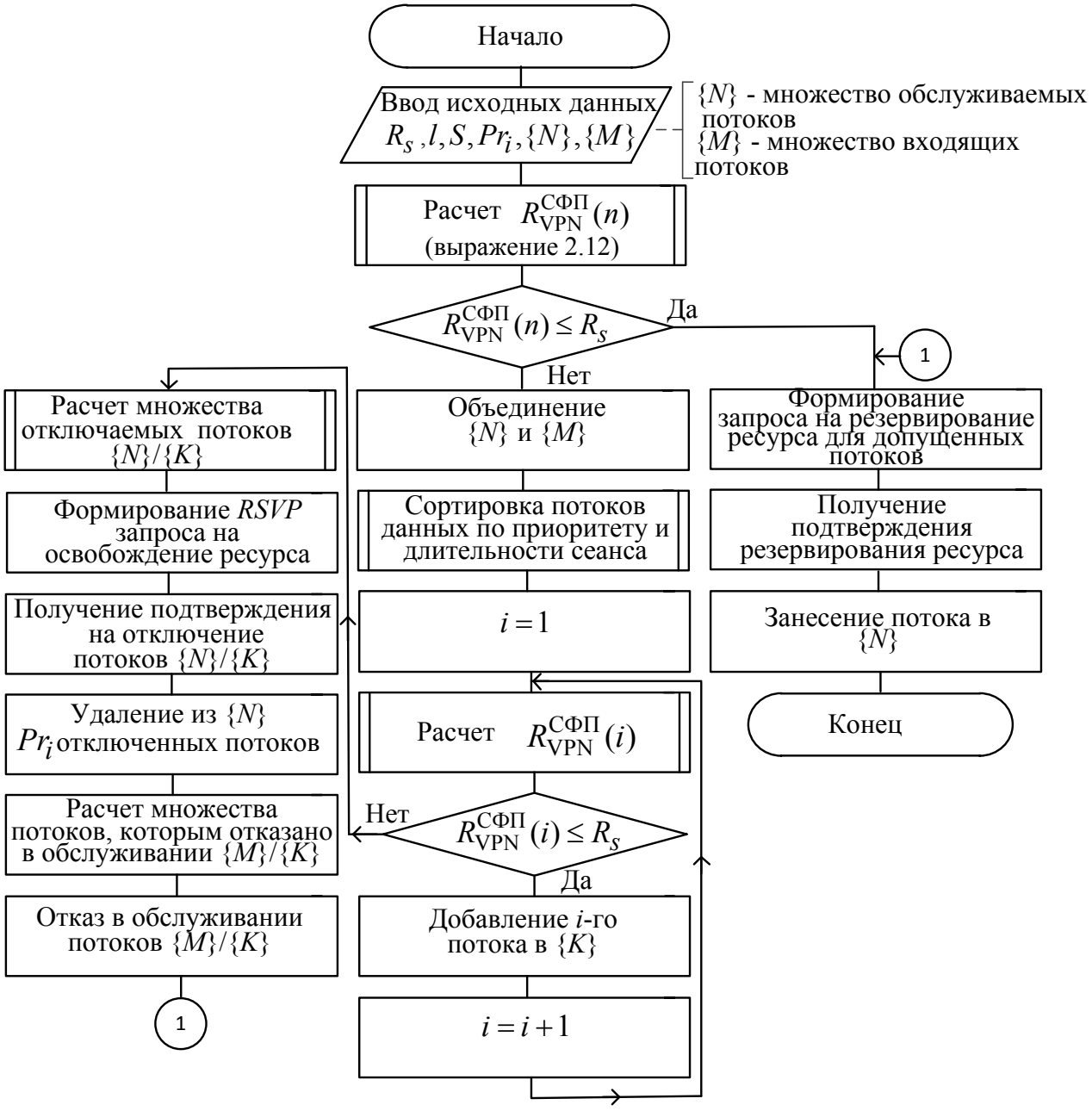


Рисунок 3.1 Схема алгоритма допуска потоков в транспортную сеть защищенной корпоративной мультисервисной сети связи

Критерий достаточности КР для обслуживания суммарного трафика *n* потоков базируется на сравнении требуемого КР для обслуживания предложенной нагрузки (множества обслуживаемых {N} и входящих {M} ПДРВ), вычисляемого с помощью разработанного алгоритма динамического

резервирования канального ресурса агрегированного потока данных и зарезервированного для данного класса трафика канального ресурса ЗКМСС:

Последовательность выполняемых алгоритмом действий может быть представлена пошагово:

Шаг 1. На данном шаге функционирования алгоритма в оперативную память VPN-шлюза вводятся исходные данные.

Шаг 2. Вычисляется требуемый КР для обслуживания агрегированного потока, включающего множество обслуживаемых и входящих в данный момент времени потоков данных предоставляемого сервиса, согласно выражения 2.12 для расчета ресурса агрегированного потока данных разработанного алгоритма динамического резервирования канального ресурса:

$$R_{\text{VPN}}^{\text{СФП}}(n) = \frac{\sum_{i=1}^{n} \alpha p_i \frac{\sum_{i=1}^{n} b_i - \gamma L_i}{\sum_{i=1}^{n} (\alpha p_i - \beta r_i)} + 2\gamma L_i}{t_{\text{ПМ}} + \frac{\sum_{i=1}^{n} b_i - \gamma L_i}{\sum_{i=1}^{n} (\alpha p_i - \beta r_i)} - \frac{\gamma L_i}{R_{\text{КС}}}}.$$

Шаг 3. Сравнение требуемого КР для обслуживания агрегированного потока в данном VPN-туннеле с допустимым КР, зарезервированным в канале связи для *l*-го VPN-туннеля – R_s на этапе планирования: $R_{\text{VPN}}^{\text{СФП}}(n) \le R_s$.

Шаг 4. В случае выполнения условия $R_{\text{VPN}}^{\text{СФП}}(n) \le R_s$ множества обслуживаемых и входящих в данный момент времени потоков данных предоставляемого сервиса являются допущенными к дальнейшему обслуживанию, и от VPN-шлюза формируется запрос в канал связи на резервирование ресурса для допущенных потоков данных.

Шаг 5. После получения подтверждения на резервирование ресурса на VPN-шлюзе все входящие потоки заносятся в множество обслуживаемых

потоков {N} и осуществляется допуск потоков данных предоставляемого сервиса в сеть. Производится настройка системы управления потоками VPN-шлюза и перенастройка весовых коэффициентов планировщика по рассчитанным значениям требуемого КР $R_{\text{VPN}}^{\text{СФП}}(n)$ для соответствующего VPN-туннеля предоставляемого сервиса. Алгоритм завершает свою работу до поступления нового запроса на обслуживание.

Шаг 6. Невыполнение условия $R_{\text{VPN}}^{\text{СФП}}(n) \le R_s$ свидетельствует о недостаточности канального ресурса для обслуживания множества обслуживаемых {N} и входящих {M} в данный момент времени потоков данных предоставляемого сервиса, оцененного с помощью разработанного алгоритма динамического резервирования канального ресурса, что приводит к возникновению перегрузки сети. В данных условиях решается задача определения оптимального набора потоков данных с учетом их приоритетов и длительности сеанса, которые должны блокироваться, методом решения оптимизационной задачи «рюкзачного» типа. Сортировка потоков данных согласно предложенного метода сначала производится по значениям их приоритетов, а на втором этапе по длительности занятия КР.

При таком подходе в условиях перегрузки изначально блокируются низкоприоритетные потоки данных реального времени, для потоков данных одного приоритета должны блокироваться соединения с максимальной длительностью установленных сеансов связи.

Шаг 7. Производится объединение множеств обслуживаемых {N} и входящих {M} в данный момент времени потоков данных предоставляемого сервиса.

Шаг 8. Производится сортировка потоков по приоритету и длительности сеанса в объединенном множестве обслуживаемых и входящих в данный момент времени потоков данных предоставляемого сервиса.

Шаг 9. Выбирается первый поток $i = 1$ из множества отсортированных потоков для вычисление требуемого КР.

Шаг 10. Производится вычисление требуемого КР для обслуживания первого потока из множества отсортированных потоков согласно выражения для расчета ресурса агрегированного потока данных усовершенствованной математической модели на основе СФП.

Шаг 11. При выполнении условия $R_{\text{VPN}}^{\text{СФП}}(i) \le R_S$ первый поток из множества отсортированных потоков помещается в множество потоков, допущенных к обслуживанию в условии перегрузки {K}. Производится переход к номеру потока $i = 2$.

Шаг 12. Производится вычисление требуемого КР для обслуживания агрегированного потока, состоящего из первого и второго потока из множества отсортированных потоков, согласно выражения для расчета ресурса агрегированного потока данных разработанного алгоритма динамического резервирования канального ресурса.

Шаг 13. При выполнении условия $R_{\text{VPN}}^{\text{СФП}}(i) \le R_S$ второй поток из множества отсортированных потоков помещается в множество потоков, допущенных к обслуживанию в условии перегрузки {K}. Производится переход к номеру потока $i = 3$.

Далее повторяются шаги 10-13 и при выполнении условия $R_{\text{VPN}}^{\text{СФП}}(i) \le R_S$ осуществляется помещение соответствующих потоков в множество потоков допущенных к обслуживанию в условии перегрузки {K}. Данные действия выполняются до тех пор, пока условие $R_{\text{VPN}}^{\text{СФП}}(i) \le R_S$ не перестанет выполняться. В результате будет сформировано множество допущенных к обслуживанию потоков в условии перегрузки сети {K}.

Оставшиеся потоки из множества отсортированных потоков подвергаются отключению (если являются обслуживаемыми потоками {N}) или отказу в обслуживании (если являются входящими потоками {M}).

Шаг 13. При невыполнении условия $R_{\text{VPN}}^{\text{СФП}}(i) \le R_S$ рассчитывается множество отключаемых потоков путем вычитания из множества

допущенных потоков в условии перегрузки {K} множества обслуживаемых потоков {N}.

Шаг 14. Производится формирование RSVP-запроса на освобождение ресурса для отключаемых потоков на терминальные аппараты, генерирующие данные соединения.

Шаг 15. После получения подтверждения на отключение потоков производится удаление данных потоков из множества обслуживаемых потоков.

Шаг 16. Расчет множества потоков, которым отказано в обслуживании, осуществляется путем вычитания из множества допущенных потоков в условии перегрузки {K} множества входящих потоков {M}.

Шаг 17. Производится отказ в обслуживании рассчитанного множества потоков.

Шаг 18. После определения оптимального набора потоков данных с учетом их приоритетов, которые должны блокироваться, от VPN-шлюза формируется запрос в КС на резервирование ресурса для допущенных потоков данных в условии перегрузки {K}.

Шаг 19. После получения подтверждения на резервирование ресурса на VPN-шлюзе все потоки, допущенные к обслуживанию в условии перегрузки {K}, заносятся в множество обслуживаемых потоков {N} и осуществляется допуск потоков данных предоставляемого сервиса в сеть. Производится настройка системы управления поотоками VPN-шлюза и перенастройка весовых коэффициентов планировщика по рассчитанным значениям требуемого КР $R_{\text{VPN}}^{\text{СФП}}(n)$ для соответствующего VPN-туннеля предоставляемого сервиса. Алгоритм завершает свою работу до поступления нового запроса на обслуживание.

Разработанный алгоритм предназначен для реализации в виде специального программного обеспечения, загружаемого из оперативной памяти и исполняемого в виде фонового процесса в VPN-шлюзе [66,72].

Результатом работы алгоритма является формирование управляющих воздействий по допуску в VPN-туннели ПДРВ на этапе установления соединения с учетом влияния процедуры шифрования на их параметры.

Разработанный алгоритм обладает свойством детерминированности. Это означает, что предписания алгоритма (процедуры) настолько точны и отчетливы, что не допускают двусмысленных толкований. Они единственным и вполне определенным путем всякий раз приводят к искомому результату [17,38].

Массовость разработанного алгоритма означает, что алгоритм может быть применен не только к единственным исходным данным или набору данных, но и к целому классу похожих задач.

Результативность или выполнимость алгоритма означает, что при любых допустимых исходных данных и точном выполнении всех предписаний алгоритм приведет к искомому результату за конечное число шагов. Но поскольку это требование может не учитывать реальных условий, в частности, при быстром изменении исходных данных при решении оптимизационной задачи, поэтому говорят о «потенциальной» выполнимости.

Дискретность разработанного алгоритма доказывается тем, что алгоритмический процесс разделен на отдельные элементарные действия (процедуры), возможность выполнения которых не вызывает сомнения. В результате получается совокупность предписаний, обозначающих структуру алгоритма.

Эффективность алгоритма определяется минимальным временем нахождения оптимального решения с минимальными затратами ресурсов памяти. Максимальные временные затраты при функционировании алгоритма допуска потоков в транспортную сеть ЗКМСС затрачиваются на решение оптимизационной задачи [4].

С целью получения быстрого решения оптимизационной задачи выбран метод Данцига, относящийся к «жадным» алгоритмам, т.е. на каждом

шаге выбирается локально-оптимальное решение, в результате чего итоговое решение не всегда будет оптимальным.

Вычислительная сложность разработанного алгоритма определяется наиболее трудозатратными процедурами с точки зрения времени их выполнения. В разработанном алгоритме к данной процедуре относится вложенный цикл при расчете требуемого КР ЗКМСС для обслуживания трафика, поступающего в VPN-туннель, при предоставлении защищенных услуг реального времени. В результате асимптотическая сложность разработанного алгоритма может быть представлена следующим выражением: $O(n \log n)$.

3.4. Разработка имитационной модели сегмента защищенной корпоративной мультисервисной сети связи

Для исследования свойств разработанного алгоритма применены средства имитационного моделирования, в частности среда моделирования Network Simulator-3 (NS-3) [11,25], позволяющая задать требуемую топологическую структуру сети связи, построенную с использованием стека протоколов TCP/IP. В NS-3 в качестве системного языка используется C++, позволяющий обеспечить высокую производительность, работу с пакетами потока на низком уровне абстракции модели и модификацию ядра NS-3 с целью поддержки новых алгоритмов и протоколов. Симулятор NS-3 предоставляет возможность использования множества сетевых протоколов, в том числе и дисциплины обслуживания пакетов в очередях.

При построении концептуальной модели сегмента ЗКМСС на начальном этапе необходимо выявить наиболее значимые процессы, протекающие в технической системе, влияющие на численные значения выходных параметров [1,8]:

– обработка поступающих в маршрутизатор пакетов,

– буферизация пакетов на выходе маршрутизатора,

– отправка пакета в канал связи.

При обработке пакета в маршрутизаторе целесообразно ограничиться следующими подпроцессами: считыванием служебной информации из заголовка пакета, удалением части служебной информации, определением по таблице маршрутизации исходящего порта маршрутизатора, добавлением новой служебной информации.

Задержка передачи пакета измеряется как время, прошедшее с момента прихода первого байта пакета на входной порт маршрутизатора до момента появления этого байта на выходном порту. Задержка складывается из времени, затрачиваемого на буферизацию пакета, а также времени, затрачиваемого на обработку пакета маршрутизатором – просмотр адресной таблицы, принятие решения о фильтрации или продвижении и получения доступа к среде выходного порта.

В NS-3 система управления допуском и способы управления передачей пакетов являются компонентой канала связи между узлами коммутации, поэтому функционально политика обслуживания трафика моделируется линией связи с заданными характеристиками пропускной способности, задержки и размером буфера [110]. Структура исследуемого фрагмента ЗКМСС представлена на рисунке 3.2.

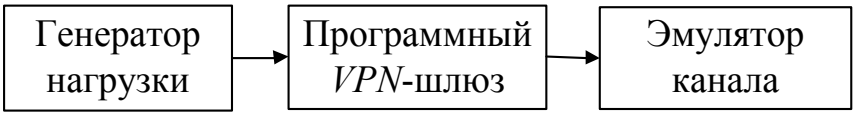


Рисунок 3.2 – Схема исследуемого на имитационной модели сегмента защищенной корпоративной мультисервисной сети связи

На вход программного VPN-шлюза подключаются агенты – источники нагрузки трех сервисов реального времени, количество которых может варьироваться. Каждый агент генерирует нагрузку по выборкам длин пакетов и межпакетному интервалу, характерным для рассматриваемых услуг. Это позволяет сформировать нагрузку в виде потоков данных с параметрами

мгновенной пиковой скорости передачи данных и средней скорости передачи данных.

Нагрузочные характеристики моделируемой защищенной корпоративной сети связи представлены в таблице 3.4.

Таблица 3.4 – Нагрузочные характеристики моделируемой защищенной корпоративной сети связи

Услуга	N^{TA} ед.	Z^{TA} Эрл	p Мбит/с	r Мбит/с	L Байт	Арендуемый канальный ресурс, Мбит/с
IP-телефония	250	0,4	0,126	0,107	254	100
Видеотелефония	70	0,2	1,74	1,22	1392	

Между источниками и получателями устанавливаются логические соединения, по которым передаются IP-пакеты с фиксацией точного времени отправления и получения каждого пакета, разница между которыми и характеризует задержку передачи из конца в конец.

Пропускная способность каналов связи между узлами коммутации может изменяться в зависимости от целей исследования и составляет 100 Мбит/с (для федерального уровня ЗКМСС ПАО АКБ «Авангард»).

В программе NS-3 модель IP-пакета состоит из заголовка и поля данных. Заголовок модели IP-пакета включает в себя общий заголовок (cmn header), IP заголовок (ip header), RTP заголовок (rtp header). Общий заголовок модели пакета cmn header содержит уникальный идентификатор (unique id - uid) и время дискретизации (time stamp - ts) пакета. Идентификатор представляет собой совокупность параметров - uid (f, Pr_i, flag), которые включают в себя номер потока информации f, приоритет услуги Pr_i и флаг начала (окончания) соединения flag. Вместо анализа полей IP и RTP заголовков в программе NS-3 используется общий заголовок cmn header, поля которого содержат достаточный набор параметров (uid и ts) для контроля основных характеристик процесса передачи пакета. При этом, в данной модели пакетов IP и RTP заголовки представляют собой поля,

заполненные данными, которые моделируют общий размер заголовка реального IP пакета. В поле данных data описанной модели пакета передается блок данных прикладного уровня, отправляемый генератором потока информации [19].

Так как задача оценивания необходимой производительности маршрутизатора при проектировании сети производится с расчетом на пиковую возможную нагрузку, то при известных параметрах нагрузки и производительности маршрутизатора возможно произвести оценку максимально достижимой задержки обработки пакета. Данная задержка в последующем рассматривается как неизменная величина.

Находясь в очереди, пакет подвергается задержке ожидания дальнейшей передачи по линии связи к следующему маршрутизатору. Время задержки ожидания зависит от числа пакетов, стоящих в очереди, и может значительно варьироваться в различных маршрутизаторах на пути пакета.

В обобщённом виде структурная логическая схема модели, представленной на рисунке 3.2, состоит из генератора трафика (на уровне пакетов), входного буфера маршрутизатора, задерживающего пакеты на некоторое постоянное время, имитирующего процесс обработки заголовков пакетов маршрутизатором, выходного буфера, размер которого определяется в зависимости от вида предоставляемых услуг и требований к уровню КО обслуживающего прибора.

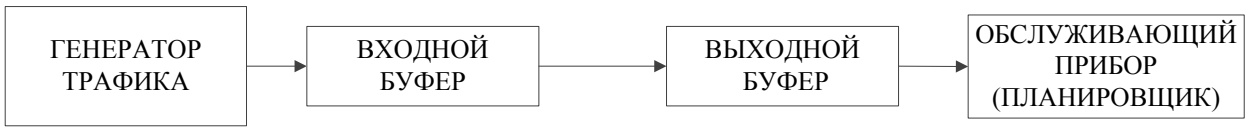


Рисунок 3.3 – Структурная логическая схема имитационной модели сегмента защищенной корпоративной мультисервисной сети связи

Моделирующий алгоритм представлен на рисунке 3.4.

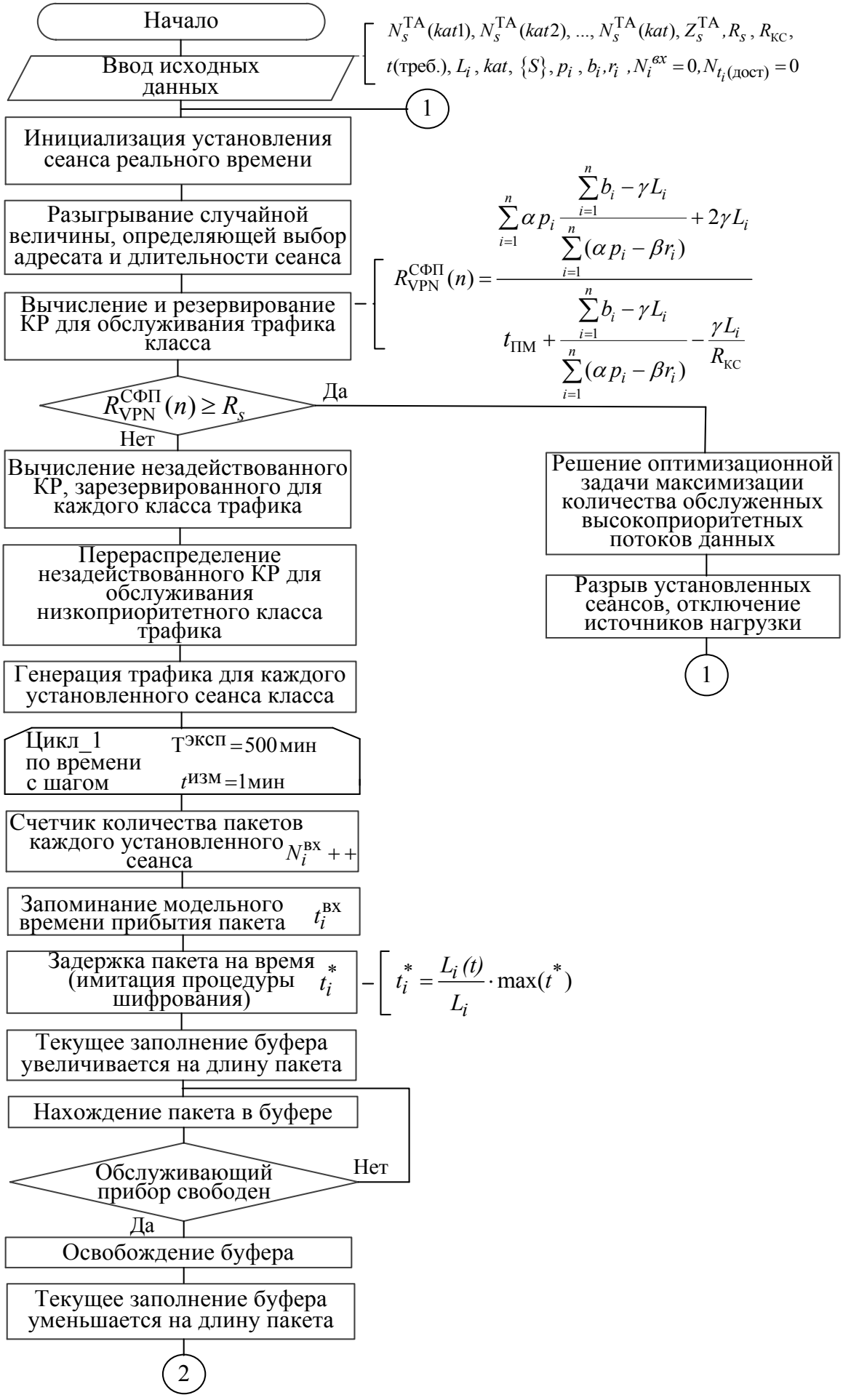

Начало
Ввод исходных данных
$N_s^{TA}(kat1), N_s^{TA}(kat2), ..., N_s^{TA}(kat), Z_s^{TA}, R_s, R_{КС},$
$t(треб.), L_i, kat, \{S\}, p_i, b_i, r_i, N_i^{вх}=0, N_{t_i(дост)}=0$
1
Инициализация установления сеанса реального времени
Разыгрывание случайной величины, определяющей выбор адресата и длительности сеанса
Вычисление и резервирование КР для обслуживания трафика класса
$R_{VPN}^{СФП}(n)=\frac{\sum_{i=1}^{n}\alpha p_i \frac{\sum_{i=1}^{n} b_i-\gamma L_i}{\sum_{i=1}^{n}(\alpha p_i-\beta r_i)}+2\gamma L_i}{t_{ПМ}+\frac{\sum_{i=1}^{n} b_i-\gamma L_i}{\sum_{i=1}^{n}(\alpha p_i-\beta r_i)}-\frac{\gamma L_i}{R_{КС}}}$
$R_{VPN}^{СФП}(n) \geq R_s$
Да
Нет
Вычисление незадействованного КР, зарезервированного для каждого класса трафика
Перераспределение незадействованного КР для обслуживания низкоприоритетного класса трафика
Генерация трафика для каждого установленного сеанса класса
Цикл_1 по времени с шагом
$T^{эксп}=500$ мин
$t^{изм}=1$ мин
Счетчик количества пакетов каждого установленного сеанса $N_i^{вх}++$
Запоминание модельного времени прибытия пакета $t_i^{вх}$
Задержка пакета на время (имитация процедуры шифрования) t_i^*
$t_i^*=\frac{L_i(t)}{L_i}\cdot\max(t^*)$
Текущее заполнение буфера увеличивается на длину пакета
Нахождение пакета в буфере
Обслуживающий прибор свободен
Нет
Да
Освобождение буфера
Текущее заполнение буфера уменьшается на длину пакета
2
Решение оптимизационной задачи максимизации количества обслуженных высокоприоритетных потоков данных
Разрыв установленных сеансов, отключение источников нагрузки
1

Рисунок 3.4 – Моделирующий алгоритм

Особенность функционирования имитационных моделей, являющихся стохастическими математическими моделями, заключается в том, что реакция отклика модели (численное значение выходных параметров модели) представляет собой также случайную величину, изменяющуюся по некоторому вероятностному закону при воспроизведении многократных «прогонов» в течение времени проведения эксперимента [9,18,23,40]. Каждый прогон имитационной модели заключается в оценивании уровня КО каждого установленного сеанса связи, вычислении в динамике требуемого КР и его резервировании на маршрутизаторах «из конца в конец». Время проведения измерения уровня КО, определяемое рекомендацией МСЭ-Т *Y*.1541, принимается равным одной минуте $t^{\text{изм}} = 1\text{мин}$. В результате проведения эксперимента $T^{\text{эксп}} = 500\text{мин}$ получается выборка экспериментальных данных исследуемых параметров, объем которой равен количеству выполненных прогонов. При этом достижимое время задержки обработки пакета при передаче $t_i(\text{дост})$ сравнивается с требуемым значением $t_i(\text{треб})$, равным значению верхней задержки обработки пакетов в ПМ $t_{\text{ПМ}}$. Вывод о достижимом уровне КО каждого установленного сеанса связи делается на основании сравнения максимального значения вероятности потери пакетов для каждого потока с требуемым значением, определенным рекомендацией Y.1541 (коэффициент потери пакетов для 0-класса качества обслуживания $P_{loss}=10^{-3}$).

Исходные данные для проведении имитационного эксперимента при предоставлении услуги IP-телефонии при функционировании федерального уровня ЗКМСС ПАО АКБ «Авангард» (модель СМО M/M/1): $N_s^{\text{ТА}} = 250$, поток вызовов – простейший (Эрланговский), т.е. закон распределения промежутка времени между соседними вызовами показательный, т.к. количество терминалов превышает 100 [17,80,87].

Результаты имитационного моделирования при предоставлении услуги IP-телефонии в федеральном уровне ЗКМСС представлены на рисунке 3.5.

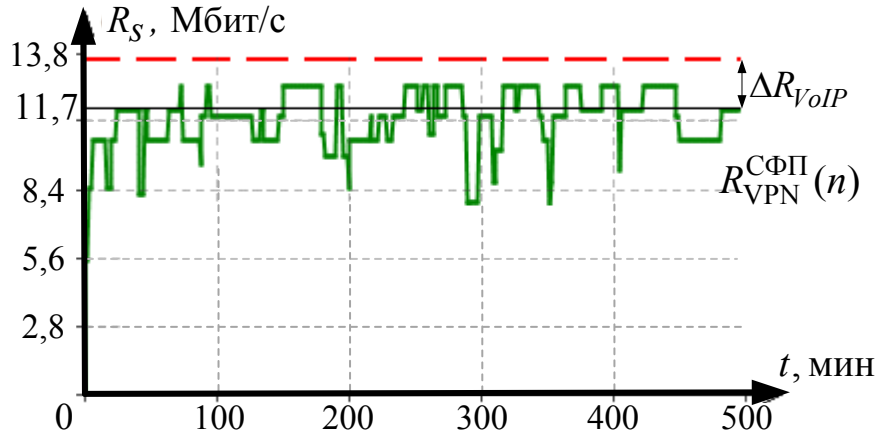


Рисунок 3.5 – Зависимость выделяемого канального ресурса от времени при предоставлении услуги IP-телефонии

Исследование предложенного алгоритма для услуги видеотелефонии со следующими исходными данными: $N_s^{\text{TA}} = 70$, $t_s^{\min} = 5$мин, $t_s^{\max} = 30$мин, закон распределения длительности сеанса – равномерный.

Результаты имитационного моделирования при предоставлении услуги видеотелефонии в федеральном сегменте ЗКМСС представлены на рисунке 3.6.

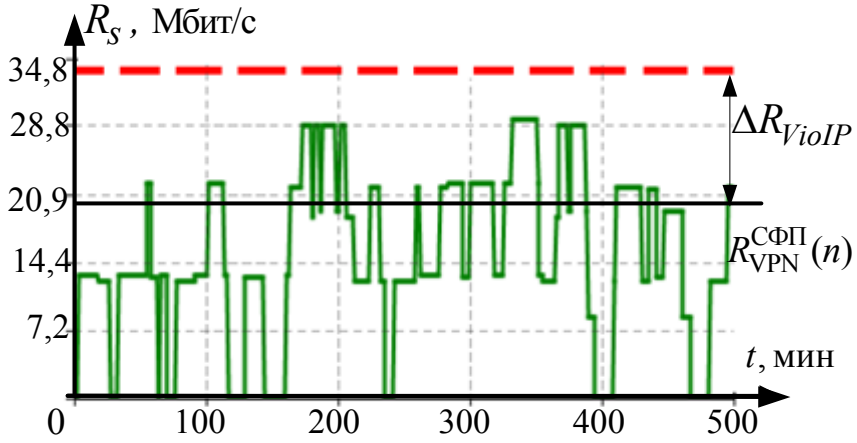


Рисунок 3.6 – Зависимость выделяемого канального ресурса от времени при предоставлении услуги видеотелефонии

На графиках 3.5, 3.6 можно оценить эффект от применения данного алгоритма. Оценка эффекта использования КР в отсутствии перегрузки

зависит от нагрузочных характеристик, применяемых при моделировании функционирования сегмента ЗКМСС [38,85,89].

Пунктирной линией на обоих графиках обозначен максимальный КР, резервируемый на этапе планирования сети с применением моделей теории телетрафика, для предоставления услуг IP-телефонии и видеотелефонии с требуемым качеством на уровне вероятности потерь вызовов, принятой равной 0,03 для ЗКМСС.

Проведем расчет эффекта использования арендуемого КР федерального уровня ЗКМСС при аренде канала с пропускной способностью 100 Мбит/с и одновременном предоставлении услуг IP-телефонии и видеотелефонии и услуги передачи данных (выхода в Интернет). Из графиков видно, что КР до применения разработанного модельно-алгоритмического инструментария «жестко» резервируется для обслуживания трафика каждого класса: 13,8 Мбит/с для трафика IP-телефонии, 34,8 Мбит/с для трафика видеотелефонии, 51,4 Мбит/с – для предоставления услуги выхода в Интернет. Данные получены на основе традиционного подхода при проектировании сети с использованием формулы Эрланга.

В каждый момент времени для обслуживания предложенной нагрузки услуг реального времени с требуемым качеством достаточно выделить ресурс, рассчитанный по разработанному алгоритму динамического резервирования канального ресурса агрегированного потока данных реального времени на основе СФП, обозначенный ломаной линией. Разность между пунктирной и ломаной линиями определяет незадействованный КР трафиком каждого сервиса. Прямой сплошной линией обозначено усредненное значение задействованного КР в течение времени проведения опыта.

Эффект от применения разработанного алгоритма в отсутствии перегрузки заключается в возможности перераспределения незадействованного КР, резервируемого для услуг IP-телефонии, видеотелефонии в пользу услуги выхода в Интернет. Поскольку услуга выхода в Интернет является услугой отложенной доставки данных, не

предъявляющей «жестких» требований к КР, увеличение объема КР выражается в снижении времени доставки блоков данных и возможности загрузки арендуемого канала связи до предела.

Незадействованный КР в течение длительности одного прогона имитационного эксперимента для услуги IP-телефонии составил приблизительно: $\Delta R_{VoIP} = 13,8 - 11,7 = 2,1$ Мбит/с ≈ 15% относительно резервируемого КР, видеотелефонии: $\Delta R_{VioIP} = 34,8 - 20,9 = 13,9$ Мбит/с ≈ 40%. Суммарный незадействованный КР составил приблизительно 16 Мбит/с ≈ 33% относительно суммарного резервируемого КР для услуги IP-телефонии и видеотелефонии, равного 48,6 Мбит/с. Степень использования резервируемого на этапе планирования КР федерального сегмента можно повысить на 33 % относительно суммарного резервируемого КР для услуги IP-телефонии и видеотелефонии в течение 500 мин функционирования ЗКМСС. Выражение для расчета технического эффекта:

$$\delta^{\text{исп}}(t) = \frac{\sum_{s=1}^{n} \Delta R_s}{\sum_{s=1}^{n} R_s} \cdot 100\%,$$

где $\Delta R_s = R_s - \sum_{l=1}^{L} R_{\text{VPN}\,l}^{\text{СФП}}(n)$ – незадействованный канальный ресурс, зарезервированный для предоставления s-го предоставляемого сервиса.

Оцененный эффект является частной опытной реализацией. Минимальный и максимальный частные эффекты представлен в таблице 3.5.

Таблица 3.5 – Технический эффект от применения модельно-алгоритмического инструментария в отсутствии перегрузки

Высвобожденный канальный ресурс при предоставлении услуги IP-телефонии, Мбит/с	Высвобожденный КР при предоставлении услуги видеотелефонии, Мбит/с	Эффект от перераспределения канального ресурса
1,74 – 3,31, 13 – 24 %	10,9 – 15,1, 32 – 44%	25 – 40%

Значения ΔR_{VioIP} и ΔR_{VoIP} были получены при выполнении 20 прогонов имитационной модели. Количество генерируемых потоков при выполнении каждого прогона менялось, поэтому ломаная линия, обозначающая ресурс, рассчитанный по усовершенствованной математической модели агрегированного потока данных реального времени на основе СФП, имеет разный вид. Соответственно значения ΔR_{VoIP} и ΔR_{VioIP} имеют значения в диапазоне 1,74 – 3,31 и 10,9 – 15,1 для всех совершенных прогонов.

Таким образом, в результате проведения эксперимента внедрение разработанного модельно-алгоритмического инструментария позволяет повысить степень использования арендуемого КР ЗКМСС в отсутствии перегрузки при одновременном предоставлении в канале связи высокоприоритетных услуг реального времени и низкоприоритетных услуг – передачи данных на 33 % относительно суммарного резервируемого КР для услуги IP-телефонии и видеотелефонии для федерального уровня ЗКМСС.

Для исследования свойств алгоритма динамического управления КР в условии перегрузки для услуги IP-телефонии при тех же параметрах источников нагрузки создавались следующие условия перегрузки: арендуемый КР 100 Мбит/с; от 20 источников генерировалась нагрузка высшего приоритета; от 35 – среднего приоритета и 45 – низшего приоритета для каждой из рассматриваемых услуг.

Результаты функционирования алгоритма в режиме управления допуском ПДРВ в транспортную сеть представлены на рисунке 3.7, откуда видно, что до наступления перегрузки (100 с) в канале связи обслуживаются потоки всех трех приоритетов. После момента времени (100 с) отмечается отказ в обслуживании потоков меньшего приоритета при выделении ресурсов как потокам высшего, так и среднего приоритетов. С появлением новых заявок на установление соединения на 170 секунде отмечается полное прекращение обслуживания низкоприоритетных потоков, а на 215 секунде – процесс перераспределения ресурсов уже между потоками высшего и среднего приоритетов, где за счет прекращения обслуживания потоков

среднего приоритета допускаются к обслуживанию высокоприоритетные потоки.

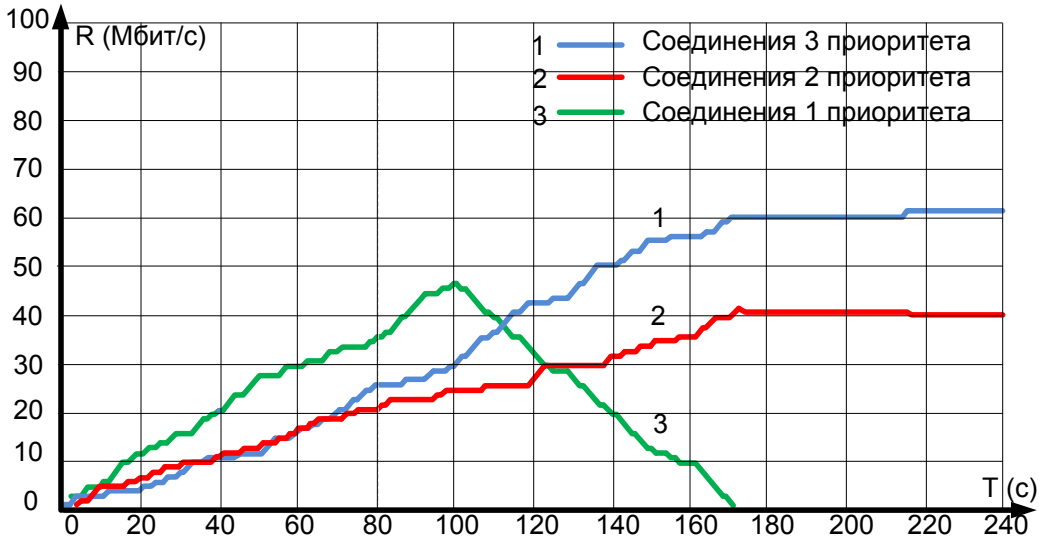


Рисунок 3.7 – Динамика работы алгоритма допуска в условиях перегрузки

Очевидно, что динамика работы предложенного алгоритма в условиях перегрузки полностью подтверждает логику работы, заложенную при формировании и обосновании критериев оптимального перераспределения пропускной способности канала связи.

При предоставлении услуг IP-телефонии, видеотелефонии и услуги выхода в Интернет при возникновении перегрузки оценивался технический эффект от применения разработанного алгоритма и реализации приоритетного допуска потоков данных к транспортному ресурсу сети. В качестве показателя оценивания степени использования КР ЗКМСС при возникновении перегрузки (нештатное функционирование сети) выбрана вероятность потерь вызовов приоритетных пользователей. Принято допущение, что нагрузка, создаваемая абонентами высших категорий, при возникновении перегрузки обслуживается с гарантированным качеством. При этом разработанный алгоритм допуска потоков в транспортную сеть позволяет за счет выбора оптимального набора допущенных к обслуживанию потоков с учетом их приоритетов и длительности сеанса, а также

резервирования КР на основе разработанного алгоритма динамического резервирования канального ресурса агрегированного потока данных уменьшить вероятность потерь вызовов от приоритетных пользователей. При наличии категорий пользователей в ЗКМСС, которым предоставляется данный класс услуг (0 – руководители корпорации и их заместители, 1 – начальники отделов, 2 – рядовые сотрудники), нагрузка, создаваемая абонентами высшей категории (№0) обслуживается с гарантированным качеством, вероятность потерь вызовов от пользователей категории №1 уменьшается. Полученные при проведении эксперимента на имитационной модели данные сведены в таблицу 3.6.

Таблица 3.6 – Технический эффект от применения модельно-алгоритмического инструментария при возникновении перегрузки при $\pi^1 = 0,03$

Услуга	Резервируемый канальный ресурс на этапе проектирования сети, Мбит/с	Канальный ресурс, вычисленный на основе $R_{\text{VPN}}^{\text{СФП}}(n)$, Мбит/с	$\Delta\pi^1$ после применения МАИ	Технический эффект, %
Видеотелефония	34,8	32,3	0,008	27 %
IP-телефония	13,8	13,7	0,004	13 %

Используя значение КР, полученное с помощью разработанного алгоритма динамического резервирования канального ресурса агрегированного потока данных на основе СФП, в выражении первой формулы Эрланга получены измененные значения вероятностей потерь вызовов. Данное изменение составило для услуги видеотелефонии приблизительно 0,008, что составляет приблизительно 27% относительно нормированного значения. Для услуги IP-телефонии – 0,004, 13%. Очевидно, что при резервировании КР, полученного с использованием разработанного алгоритма динамического резервирования канального ресурса агрегированного потока данных на основе СФП, равного КР, вычисленному при проектировании сети с использованием формулы Эрланга (для услуги IP-

телефонии = 13.8 Мбит/с, для услуги видеотелефонии = 34,8 Мбит/с), количество одновременно обслуживаемых потоков увеличится и соответственно вероятность потерь вызовов уменьшится на полученные изменения, представленные в таблице 3.6.

3.5. Выводы по третьему разделу

1. На основе разработанного алгоритма динамического резервирования канального ресурса агрегированного потока данных реального времени в данном разделе сформирована система критериев эффективности использования КР ЗКМСС для условий наличия КР сети для обслуживания предложенной нагрузки от сети доступа и «перегрузки» сети. В основе принятия решения о допуске нового ПДРВ в транспортную сеть лежит процедура сравнения имеющегося КР и требуемого КР для агрегированного потока с учетом нового ПДРВ, поступающего на обслуживание.

2. Разработан подход к назначению приоритетов потокам данных, в котором учтены категории пользователей и класс предоставляемых услуг, что в отличие от существующего инструментария позволяет решить задачу приоритетного обслуживания ПДРВ в условиях перегрузки и определить наилучший вариант использования имеющегося КР транспортного уровня ЗКМСС.

3. Решение оптимизационной многокритериальной задачи о рюкзаке с несогласованными критериями в разработанном алгоритме основано на ее сведении к однокритериальной с применением метода главного критерия и использовании метода Данцига для решения последней. Предлагаемый порядок их применения в алгоритме позволяет за счёт отсечений области допустимых решений достичь уменьшения количества перебираемых вариантов и произвести тем самым быстрый поиск допустимого решения за счет частичного перебора усеченного упорядоченного множества.

Раздел 4

Разработка комплекса алгоритмов согласования трафика с VPN-туннелем

4.1. Введение

Для реализации динамического резервирования КР арендуемого канала связи ЗКМСС необходимо обеспечить протокольное взаимодействие между VPN-шлюзом сети доступа и ПМ транспортной сети [36,37]. С этой целью в настоящем разделе рассматривается комплекс алгоритмов классификации и сглаживания трафика, управления планировщиком маршрутизатора, внедренные в систему управления потоками внутреннего маршрутизатора VPN-шлюза. Данные алгоритмы совместно с алгоритмом допуска потоков в сеть позволят гибко использовать пропускную способность арендуемого канала связи и повысить степень его использования как в условиях штатного функционирования сети доступа, так и в условиях возникновения перегрузки. Структурная схема модернизированного VPN-шлюза сети доступа защищенной корпоративной мультисервисной сети связи представлена на рисунке 4.1.

Первым этапом процесса управления допуском потоков данных в VPN-туннель к обслуживанию в транспортном сегменте ЗКМСС является идентификация новой заявки на установление соединения с определением параметров потока данных и требований к КО.

Управление допуском осуществляется в VPN-шлюзе. При этом процедура трансляции параметров потока и требований к КО трафика VPN-туннеля реализуется посредством формирования служебного запроса RSVPagr, для чего используются два идентичных типа сообщений PATHagr и RESVagr.

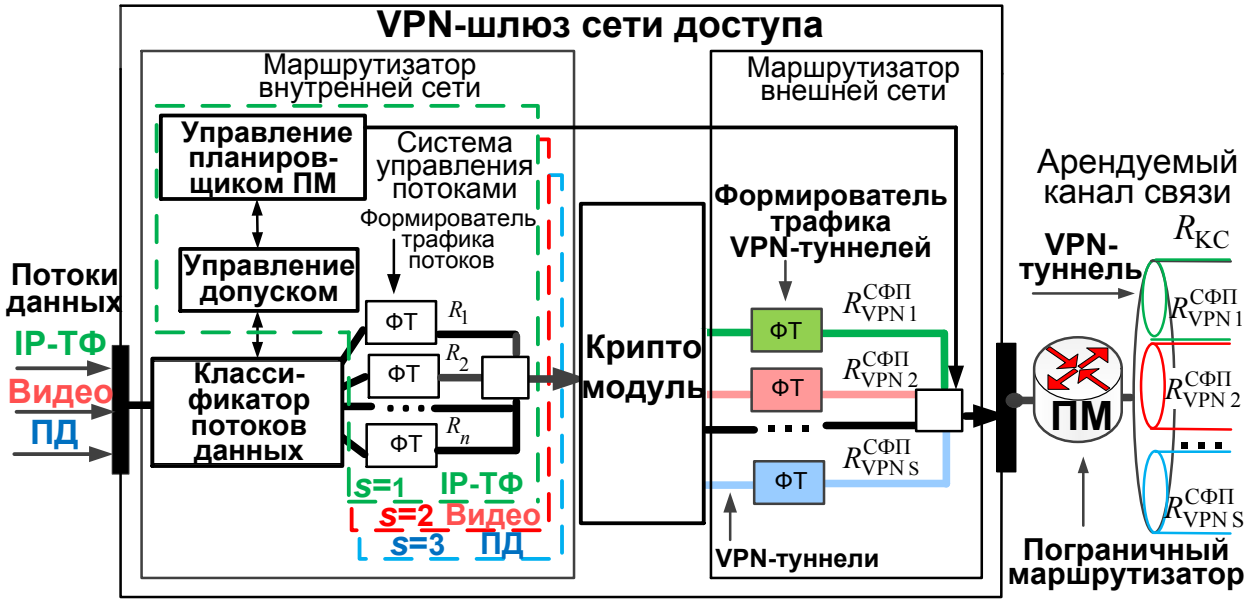


Рисунок 4.1 – Структурная схема модернизированного VPN-шлюза сети доступа защищенной корпоративной мультисервисной сети связи

Каждое сообщение RSVP состоит из общего заголовка (рисунок 4.2), за которым следует тело сообщения, состоящее из переменного числа объектов переменной длины [42,100]. Для каждого типа сообщения RSVP существует набор правил допустимого выбора типов объектов.

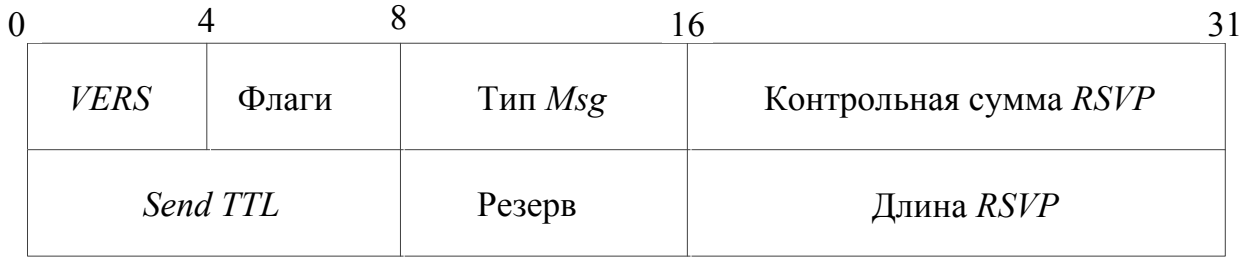


Рисунок 4.2 – Формат общего заголовка RSVP

В составе общего заголовка основные поля характеризуют версию протокола – Vers (4 бита), флаги (4 бита), тип сообщения – Msg (8 бит). Наибольший интерес для реализации системы управления доступом в ЗКМСС представляет сообщение PATHagr. Так как в настоящее время не предусмотрена процедура передачи служебных сообщений через средство

шифрования, то взаимодействие осуществляется только в сети доступа между приложением терминального оборудования и средством шифрования. Контрольная сумма RSVP составляет 16 бит. Поле Send_TTL (8 бит) заполняется значением TTL для протокола IP, с которым было послано сообщение. Длина RSVPagr (16 бит) характеризует полную длину RSVP сообщения в байтах, включая общий заголовок и объекты переменной длины, которые за ним следуют. Каждый объект состоит из одного или более 32-битных слов с 4-байтовым заголовком. Формат объектов представлен на рисунке 4.3.

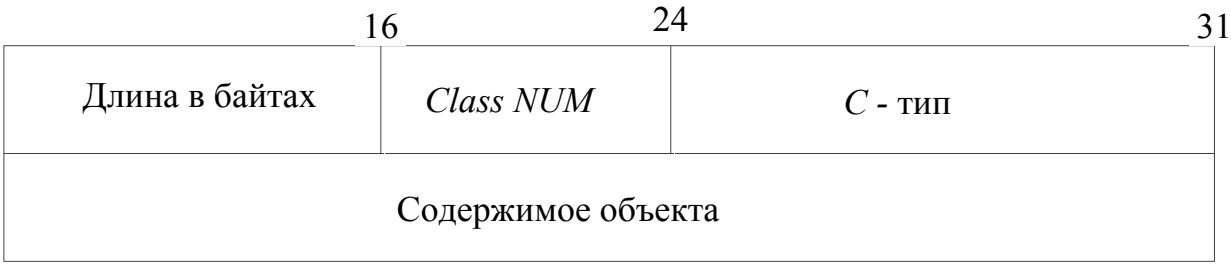


Рисунок 4.3 –. Формат объектов

Поле C-Type определяет тип объекта, который уникален в пределах класса Class-Num. Идентификация объекта осуществляется по полю Class-Num. Каждый класс объекта имеет свое имя и предназначен для передачи следующей информации:

– NULL имеет код Class-Num равный нулю, а его C-тип игнорируется. Объект NULL может появиться где угодно в последовательности объектов. Его содержимое получателем игнорируется;

– SESSION содержит IP-адрес места назначения (DestAddress), идентификатор протокола IP, и обобщенный номер порта назначения для того, чтобы специфицировать сессию для других объектов, которые следуют далее. Этот класс должен присутствовать в любом сообщении PATH и RSVP;

– RSVP HOP несет в себе IP-адрес узла, поддерживающего протокол RSVP, который послал это сообщение, и дескриптор логического выходного

интерфейса (LIH). Этот класс характеризует предшествующий узел (previoushop);

– TIME VALUES содержит значение периода обновления, используемого отправителем сообщения. Необходим в каждом сообщении PATH и RESV;

– STYLE определяет стиль резервирования, а также зависящую от стиля информацию, которая не включена в объекты FLOWSPEC или FILTER SPEC. Необходим в каждом сообщении RESV;

– FLOWSPEC определяет желательный уровень качества обслуживания в сообщениях Resv;

– FILTER SPEC определяет субнабор информационных пакетов сессии, которые должны получить желательный уровень качества обслуживания (специфицированный объектом FLOWSPEC) в сообщениях RESV;

– SENDER TEMPLATE содержит IP-адрес отправителя и, может быть, некоторую дополнительную информацию, идентифицирующую отправителя. Необходим в сообщениях PATH;

– SENDER TSPEC определяет характеристики информационного трафика отправителя. Необходим в сообщениях PATH;

– ADSPEC несет в себе данные о требованиях к качеству обслуживания в сообщении PATH;

– ERROR SPEC специфицирует ошибку в сообщениях PATH Err, RESV Err, или подтверждение в сообщении RESV CONF;

– POLICY DATA несет в себе информацию, которая позволит локальному модулю, определяющему политику, принять решение допустимо ли административно соответствующее резервирование. Может присутствовать в сообщениях PATH, RESV, PATH Err или RESV Err;

– INTEGRITY несет в себе данные для аутентификации исходного узла и для верификации содержимого сообщения RSVP;

– SCOPE несет в себе список ЭВМ-отправителей, к которым должно быть переадресовано данное сообщение. Может присутствовать в сообщениях RESV, RESV Err или RESV Tear;

– RESV CONFIRM несет в себе IP-адрес получателя, который запросил подтверждение. Может присутствовать в сообщениях RESV или RESVConf.

С точки зрения установления соединения в ЗКМСС наиболее важным для рассмотрения является сообщение PATHagr, передаваемое от VPN-шлюза и формируемое на прикладном уровне. Это сообщение содержит объект SENDER TEMPLATE, определяющий адрес отправителя, и объект SENDER TSPEC, специфицирующий характеристики трафика потока. Среди этих характеристик специфицированы мгновенная пиковая скорость передачи, средняя скорость передачи, максимальная допустимая задержка, вероятность потери пакета, максимальный размер пачки и т.п. Адрес получателя передается в объекте SESSION. Рассчитанное значение требуемого КР для обслуживания агрегированного потока данных VPN-туннеля с помощью разработанного алгоритма динамического резервирования канального ресурса агрегированного потока используется в качестве пикового возможного значения скорости поступления трафика с выхода VPN-шлюза. Как было отмечено, объект SENDER TEMPLATE может содержать и дополнительную информацию, характеризующую отправителя. В данном случае это значения приоритета каждого ПДРВ относительно класса услуги и категории вызывающего и вызываемого абонентов. Таким образом, все параметры, характеризующие поток VPN-туннеля и требования к КО могут быть переданы от VPN-шлюза с помощью сообщения RSVP PATH agr.

После анализа данных объектов SENDER TEMPLATE и SESSION в VPN-шлюзе становятся известными IP-адрес VPN-шлюза получателя, а также номера портов отправителя и получателя, в общем случае формируя так называемый «Socet». В случае установления соединения по сокету становится возможным классифицировать все пакеты, относящиеся к данному соединению.

4.2. Алгоритм классификации трафика

Для выполнения функции определения требуемого КР для каждого VPN-туннеля на этапе установления сеансов требуется классифицировать поступающие потоки данных на основе анализа полей заголовков IP-пакетов - IP-адресов отправителя и получателя внешних VPN-шлюзов, на основании которых определяется порядковый номер VPN-туннеля для каждой предоставляемой инфокоммуникационной услуги и передача порядковых номеров активных VPN-туннелей в оперативное запоминающее устройство маршрутизатора.

Классификация потоков данных, выполняемая на этапе установления сеансов связи до процедуры шифрования, должна производить их количественный учет, присваивать порядковые номера потокам данных для последующих операций их сортировки и определения потоков, подлежащих блокированию, и потоков, которым должно быть отказано в обслуживании в условиях перегрузки. С этой целью разработан классификатор потоков данных, который может быть реализован программно за счет создания списков доступа, исходными данными для которых являются параметры объектов SENDER TEMPLATE и SESSION, транслируемые оконечными терминальными аппаратами [65.68].

Блок схема последовательности действий, производимых классификатором потоков данных, представлена на рисунке 4.4.

С целью последующего выполнения процедуры соответствия установленных и поступающих на обслуживание новых потоков данных в разрабатываемый алгоритм внедряется процедура запоминания времени установления каждого сеанса.

Рисунок 4.4 – Схема последовательности действий, производимых разработанным классификатором потоков данных

Разработанный алгоритм отличается от существующих выбранным классифицирующим функциональным признаком (определение и сопоставление каждого сеанса связи VPN-туннелю, а также возможность фиксирования и запоминания времени установления сеанса связи, что в последующем позволит определять время занятия КР каждого установленного сеанса связи и в условиях перегрузки возвращать численные значения на вход алгоритма сортировки).

4.3. Алгоритм сглаживания трафика

Для обеспечения качества обслуживания потоков данных, передаваемых по всем VPN-туннелям, в отсутствии перегрузки реализован алгоритм сглаживания трафика, выполняющий задачу формирования трафика VPN-туннелей каждого класса сервиса, поступающих из КМ, в соответствии с параметрами изменившейся нагрузки по классам трафика, и передачи пакетов VPN-туннелей в выходной порт VPN-шлюза. Данный алгоритм реализован на основе разработанного и запатентованного способа сглаживания приоритетного трафика данных и устройства для его осуществления [73,98]. В заявленном способе эта задача решается за счет проведения анализа входных потоков данных, поступающих на обслуживание в VPN-туннели.

Размер буфера (общей «корзины с маркерами»), зарезервированного для агрегированного потока данных каждого предоставляемого сервиса разделяется на три «субкорзины» с учетом заявленных характеристик входного трафика данных классов сервиса так, что сумма размеров «субкорзин» равна размеру общей «корзины». Оцениваются параметры пакетов из входного трафика данных для класса сервиса: длина пакетов и класс сервиса. Производится оценка количества маркеров в каждой «субкорзине» на текущий момент времени, с учетом скорости их поступления, и количества маркеров, переходящих из любой заполненной «субкорзины» в любую другую незаполненную «субкорзину», в соответствии с заданной скоростью их перехода между соответствующими «корзинами с маркерами». Очередные поступившие маркеры из «субкорзины», заполненной маркерами, перенаправляются в «субкорзину», не заполненную маркерами.

Сравнивается длина каждого последующего пакета с количеством маркеров, находящихся в «субкорзине». Если длина пакета меньше количества маркеров в «субкорзине», то пакет передается к последующему блоку маршрутизатора с одновременным вычитанием количества маркеров

согласно длине пакета из соответствующей «субкорзины». В противном случае пакет передается на хранение в соответствующую «субкорзину» ожидания (логический буфер) при условии достаточного свободного места соответствующей «субкорзины» согласно класса трафика и ожидает в нем до тех пор, пока количество маркеров в «субкорзине» не станет больше или равным длине пакета. В последующем ожидающий в субкорзине пакет передается для обслуживания в выходной порт маршрутизатора с одновременным вычитанием количества маркеров согласно длине данного пакета из соответствующего «субкорзины».

В результате изменения нагрузки по классам сервисов и информационным направлениям и изменения интенсивности поступления пакетов VPN-туннелей с выхода КМ изменяется скорость вычитания маркеров из соответствующей «субкорзины». Для компенсации вычитаемых со сверх запланированной скоростью маркеров реализована возможность перехода маркеров из любой заполненной «субкорзины» в любую другую незаполненную «субкорзину» соответствующих VPN-туннелей классов сервиса. Происходит перезаполнение субкорзин для VPN-туннелей классов сервиса маркерами из других субкорзин до величины, необходимой для обслуживания данного VPN-туннеля. При этом скорость перехода маркеров из любой заполненной «корзины» в любую другую незаполненную «корзину» задается заранее и может применяться с различными коэффициентами в зависимости от текущей интенсивности сброса маркеров в субкорзине, которая предполагается для передачи маркеров другой субкорзине. Если добавленного количества маркеров будет недостаточно, происходит передача пакетов на хранение в соответствующую «субкорзину» ожидания. Благодаря постановке и хранению пакетов в буфере ожидания и последующей их передаче для обслуживания, достигается уменьшение дисперсии скорости передачи обслуженного трафика данных, что приводит к сглаживанию обслуженного трафика данных.

Блок схема последовательности действий, производимых разработанным блоком сглаживания трафика, представлена на рисунке 4.5.

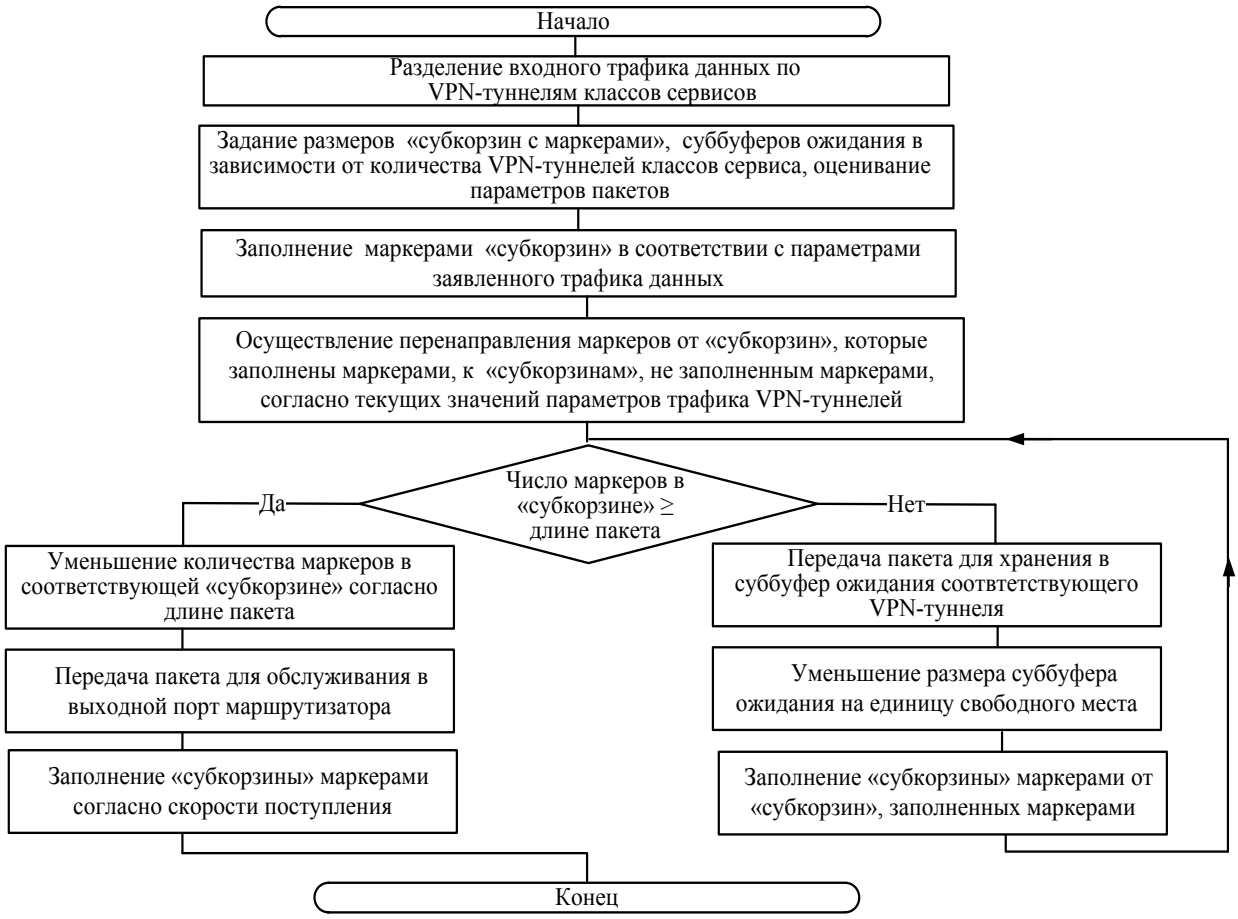


Рисунок 4.5 – Схема алгоритма сглаживания трафика

Внедрение в архитектуру VPN-шлюза, применяемого в ЗКМСС, разработанного блока, функционирующего на основе запатентованного способа, позволяет обеспечить качество обслуживания потоков данных, передаваемых по всем VPN-туннелям, и повысить при этом эффективность использования резервируемого для VPN-туннелей КР.

4.4. Алгоритм управления планировщиком пограничного маршрутизатора

Перераспределение пропускной способности между сервисами в отсутствии перегрузки достигается посредством выполнения алгоритма управления планировщиком ПМ, вычисляющего веса очередей пакетов механизма WFQ и обеспечивающего переконфигурирование планировщика в

соответствии с изменяющейся обстановкой по нагрузке информационных направлений и классов трафика с целью предоставления незадействованного КР, зарезервированного для высокоприоритетных услуг, в интересах низкоприоритетных [71].

Обратное изъятие переданного на время ресурса в случае увеличения высокоприоритетной нагрузки не должно приводить к снижению КО низкоприоритетного трафика. Этого можно достичь, только если в низкоприоритетный класс трафика отнесены услуги передачи данных. На примере ЗКМСС ПАО АКБ «Авангард», рассматриваемой в диссертации, к таким видам сервисов можно отнести услуги передачи данных, электронной почты, предоставления выхода в Интернет.

Схема алгоритма управления планировщиком ПМ представлена на рисунке 4.6.

Последовательность выполняемых алгоритмом действий может быть представлена пошагово:

Шаг 1. На данном шаге функционирования алгоритма в оперативную память VPN-шлюза от системы управления допуском системы управления потоками внутреннего маршрутизатора VPN-шлюза поступают следующие исходные данные: $R_{\text{КС}}$ - пропускная способность арендованного канала связи в соответствии с SLA, R_s - пропускная способность, выделяемая под класс сервиса, $R_{\text{VPN}\,l}^{\text{СФП}}(n)$ - пропускная способность, выделяемая для l-го VPN-туннеля s-го класса сервиса.

Шаг 2. Для каждого s-го класса сервиса выполняется вычисление незадействованного канального ресурса согласно выражения:

$$\Delta R_s = R_s - \sum_{l=1}^{L} R_{\text{VPN}\,l}^{\text{СФП}}(n).$$

Шаг 3. Вычисляется вес очереди планировщика маршрутизатора WFQ для обслуживания трафика данного сервиса:

$$\omega_s = \frac{\sum_{l=1}^{L} R_{\text{VPN}\,l}^{\text{СФП}}(n)}{R_{\text{КС}}}.$$

Шаг 4. Полученный вес заносится в оперативную память VPN-шлюза.

Шаг 5. Выполняется переход к следующему классу сервиса.

Шаг 6. Выполняется вычисление незадействованного канального ресурса для данного класса сервиса и его веса.

Шаг 7. Выполняется переход к следующему s-му классу сервиса и повторяются шаги 2 – 4 для всех S классов сервиса, обслуживание которых реализуется в данной ЗКМСС.

Шаг 8. После вычисления весов для S классов сервиса выполняется вычисление незадействованного КР для данного арендованного канала связи $\sum_{s=1}^{S} \Delta R_s$, используемого для низкоприоритетного сервиса.

Шаг 9. Выполняется вычисление веса для низкоприоритетного сервиса

$$\varphi_s = \frac{\sum_{s=1}^{S} \Delta R_s}{R_{\text{КС}}}.$$

Шаг 10. Программный модуль управления планировщиком ПМ, внедренный в систему управления потоками внутреннего маршрутизатора VPN-шлюза, формирует запрос на переконфигурирование планировщика ПМ ЗКМСС в соответствии с новыми весами ω_s, φ_s.

Шаг 11. Выполняется переконфигурирование планировщика ПМ и осуществляется допуск потоков данных сервисов реального времени и низкоприоритетного сервиса в соответствии с текущей на данный момент нагрузкой используемых классов сервиса. Алгоритм заканчивает свою работу.

Функционирование алгоритма осуществляется при каждом изменении нагрузки для предоставляемых классов сервиса.

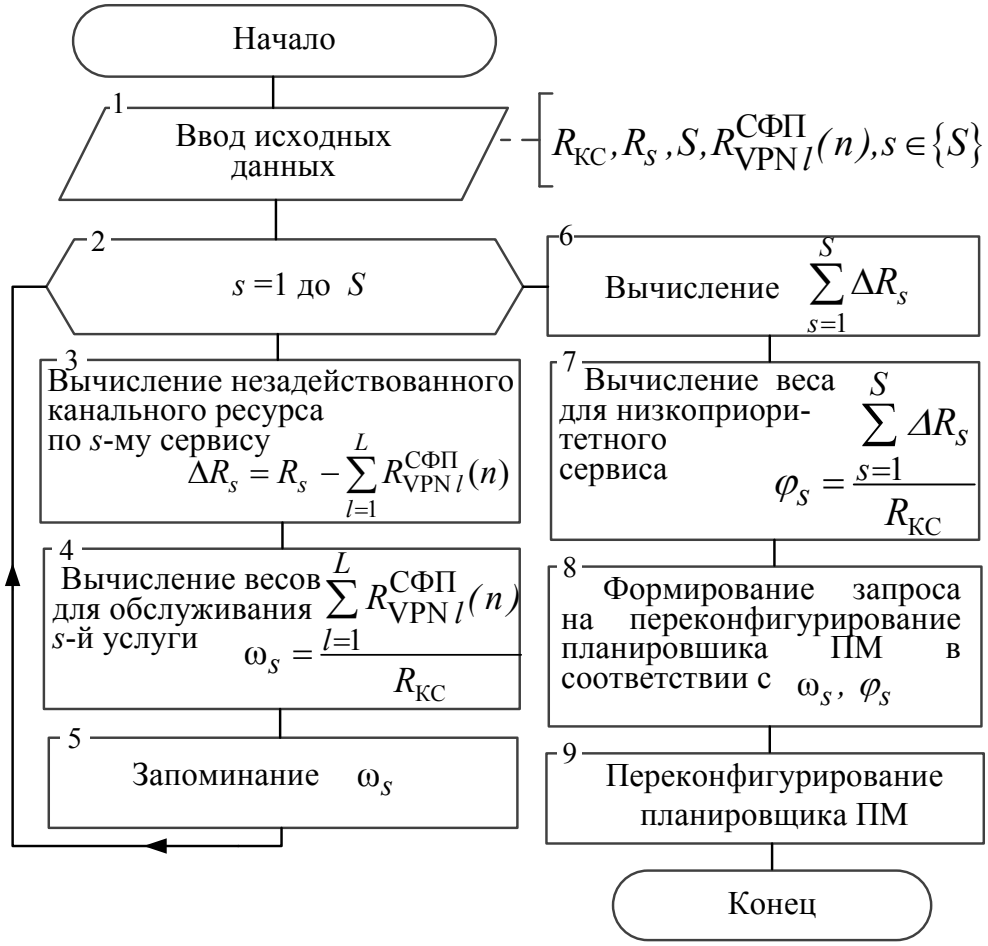


Рисунок 4.6 – Схема алгоритма управления планировщиком пограничного маршрутизатора

4.5. Оценка времени выполнения процедуры сортировки потоков данных в VPN-шлюзах

В условиях перегрузки наиболее критичным и значимым параметром обеспечения КО на уровне сеансов связи выступает время ожидания установления соединения (занятия КР) [12,20]. Данные значения регламентированы соответствующими рекомендациями по строительству и проектированию сетей и могут быть применимы, в том числе и для ЗКМСС, или могут быть заранее определены заказчиком, эксплуатирующим сеть ПАО АКБ «Авангард».

За время ожидания установления соединения (занятия КР) принимается время с начала передачи информации о занятии абонентской линии до

момента получения пользовательским (оконечным) оборудованием от оконечного узла сети связи сигнала готовности к приему номера (время отклика узла связи) – показатель функционирования сетей связи, техническая норма которого (не более 2 с.) представлена в Приказе Министерства информационных технологий и связи РФ от 27 сентября 2007 г. №113 "Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования" [35,50].

Время выполнения процедуры сортировки с учетом времени переконфигурирования маршрутизаторов, т.е. реализации внутрипротокольного взаимодействия между VPN-шлюзом и ПМ, не должно превышать требуемое время ожидания соединения.

Для оценивания времени ожидания установления соединения (занятия КР) произведен анализ затрачиваемого времени на выполнение процедуры сортировки данных в VPN-шлюзе в зависимости от размерности входных данных. Данная процедура выполняется разработанным и реализованным в системе управления потоками маршрутизатора внутренней сети VPN-шлюза алгоритмом допуска потоков данных в сеть в условиях перегрузки.

Анализ времени выполнения алгоритма сортировки произведен на применяемом в ЗКМСС ПАО АКБ «Авангард» криптографическом оборудовании аппаратно-программного комплекса Континент IPC-10 и Континент IPC-25 для регионального уровня, Континент IPC-100, IPC-400 – для федерального уровня при различных уровнях загрузки процессора криптографического оборудования $\rho = 0,4$, $\rho = 0,6$, соответствующих среднему и предельно допустимому уровню загрузки данного оборудования.

Для выбора оптимального алгоритма сортировки потоков данных произведен анализ существующих алгоритмов. Данные алгоритмы классифицируются исходя из сферы применения: выполнение операций с массивами, целиком помещающимися в оперативной памяти с произвольным доступом к любой ячейке (внутренняя сортировка); выполнение операций в запоминающих устройствах большого объёма, но не с произвольным доступом, а последовательным (упорядочение файлов) (внешняя

сортировка); потребность в дополнительной памяти или её отсутствие; потребность в знаниях о структуре данных, выходящих за рамки операции сравнения, или отсутствие таковой.

Задача сортировки в общем случае предполагает, что единственной обязательно наличествующей операцией для элементов является сравнение. С этой точки зрения необходимо рассмотреть алгоритмы устойчивой и неустойчивой сортировки. Под устойчивой (стабильной) сортировкой понимается сортировка, которая не меняет относительный порядок сортируемых элементов, имеющих одинаковые ключи. Она практически всегда может быть достигнута путём удлинения исходных ключей за счёт дополнительной информации об их первоначальном порядке. Наличие устойчивости не является обязательным для правильности сортировки и может не соблюдаться, так как для её обеспечения всегда необходимы дополнительная память и время [45,51,50,60].

В условиях функционирования ЗКМСС ПАО АКБ «Авангард» размерность входных данных для задачи сортировки достаточно велика (для федерального уровня достигает 100 ПДРВ), а время решения данной задачи ограничено требованиями по своевременности и доступности предоставляемых сервисов. В таком случае оперативность сортировки является приоритетным свойством при выборе алгоритма. Исходя из этого, с точки зрения быстродействия и эффективности использования памяти, наиболее приемлемыми являются алгоритмы неустойчивой сортировки. К ним относятся сортировка выбором, сортировка расчёской, сортировка Шелла, пирамидальная сортировка, плавная сортировка, быстрая сортировка, интроспективная сортировка, терпеливая сортировка.

На основании проведенного анализа видов сортировки, исходя из классификации по сфере применения и с учетом вычислительной сложности определено, что наиболее подходящим алгоритмом сортировки для решаемой в рамках данной диссертации задачи подходит алгоритм быстрой сортировки – сортировки Хоара (Quicksort), являющийся одним из самых быстрых известных универсальных алгоритмов сортировки массивов. К

основным достоинствам данного алгоритма относятся простота в реализации, оптимальная вычислительная сложность $O(n \cdot log(n))$, необходимость $O(log(n))$ дополнительной памяти для своей работы, хорошее сочетание с механизмами кэширования и виртуальной памяти, возможность естественного распараллеливания (сортировки выделенных подмассивов в параллельно выполняющихся подпроцессах), возможность эффективной модификации для сортировки по нескольким ключам, что особенно важно при решении задачи первичной сортировки по приоритетам и последующей сортировки по длительности сеанса, возможность работы на структурах с последовательным доступом, допускающих эффективный проход как от начала к концу, так и от конца к началу [2,85].

Оценивание времени выполнения процедуры сортировки потоков данных в VPN-шлюзе в рамках данной работы выполнялось на аппаратном эмуляторе на основе процессора, используемого в криптографических устройствах, применяемых в ЗКМСС ПАО АКБ «Авангард». Результаты проведенного модельного эксперимента в зависимости от производительности и коэффициента загрузки VPN-шлюза представлены в таблице 4.1.

Таблица 4.1 – Затрачиваемое время на выполнение процедуры сортировки потоков данных в средстве управления потоками VPN-шлюза

Криптографическое оборудование	Время, мс					
	$\rho = 0,4$			$\rho = 0,6$		
	10 ПД	50 ПД	100 ПД	10 ПД	50 ПД	100 ПД
Континент IPC 10	26	72	-	31	112	-
Континент IPC 25	14	58	-	23	88	-
Континент IPC 100	6	24	62	11	37	84
Континент IPC 400	2	13	45	9	21	67

Полученные численные значения не могут позволить оценить КО на уровне сеансов связи для высокоприоритетных абонентов, т.к. необходимо провести дополнительный анализ переконфигурирования планировщика ПМ, реализующего функцию допуска потока в транспортную сеть ЗКМСС.

4.6. Оценка времени переконфигурирования пограничного маршрутизатора

Для оценки времени переконфигурирования ПМ проведен анализ применяемого на ПМ транспортной сети с коммутацией пакетов сетевого оборудования регионального уровня Cisco 3845, Juniper SRX-650 и федерального уровня – Cisco 3945, Juniper MX-80.

Переконфигурирование ПМ осуществляется как в нештатном режиме функционирования сети (условия перегрузки) для осуществления допуска поступающего потока данных от высокоприоритетного абонента, так и в штатном режиме (отсутствие перегрузки) для перераспределения незадействованного КР, зарезервированного для высокоприоритетных услуг, в интересах низкоприоритетных, а также обратного изъятия переданного на время ресурса в случае увеличения высокоприоритетной нагрузки.

Перераспределение КР осуществляется между сервисами в соответствии с вычисляемыми весами очередей пакетов в зависимости от изменившейся обстановки по нагрузке информационных направлений и классов трафика. При этом программный модуль управления планировщиком маршрутизатора, внедренный в систему управления потоками внутреннего маршрутизатора VPN-шлюза, позволяет сформировать RSVP запросы на переконфигурирование планировщика ПМ ЗКМСС в соответствии с новыми весами. Для обеспечения требований по времени ожидания соединения проведена оценка времени переконфигурирования пограничных маршрутизаторов, построенных на базе сетевого оборудования, применяемого в ТСКП. В применяемом на ПМ ТСКП сетевом оборудовании Cisco 3845, Juniper SRX-650, Cisco 3945, Juniper MX-80 поддерживаются

протоколы быстрой перемаршрутизации VRRP (Virtual Reroute Protocol), обеспечивающие переконфигурирование маршрутизаторов не более чем за 50 мс. Доказано, что внесение однократной задержки на ПМ менее 50 мс не окажет влияния на уровень КО. Таким образом, в качестве временного критерия принятия решения о переконфигурировании маршрутизатора принимается максимально допустимая вносимая задержка, которая не должна превысить 50 мс.

С целью оценивания вносимой задержки при различных уровнях загрузки сетевого оборудования проведено тестирование существующего сетевого оборудования при выполнении перераспределения КР при отсутствии перегрузки при среднем и предельно допустимом уровне загрузке оборудования $\rho = 0,4$ и $\rho = 0,6$ соответственно.

Таблица 4.2 – Затрачиваемое время на выполнение процедуры переконфигурирования ПМ при коэффициенте загрузки $\rho = 0,4$

Сетевое оборудование	Частота процессора, ГГц	Объем оперативной памяти, Гбайт	Размерность входных данных ($\rho = 0,4$)		
			10 ПД	50 ПД	100 ПД
			Время,мс	Время, мс	Время, мс
Cisco 3845 (3945)	1,4	0,512	6	17	46
Juniper SRX-650	1,1	0,8	11	24	57
Juniper MX-80	1,3	2	7	13	38

Таблица 4.3 – Затрачиваемое время на выполнение процедуры переконфигурирования ПМ при коэффициенте загрузки $\rho = 0,6$

Сетевое оборудование	Частота процессора, ГГц	Объем оперативной памяти, Гбайт	Размерность входных данных ($\rho = 0,6$)		
			10 ПД	50 ПД	100 ПД
			Время, мс	Время, мс	Время, мс
Cisco 3845 (3945)	1,4	0,512	13	28	64
Juniper SRX-650	1,1	0,8	21	46	87
Juniper MX-80	1,3	2	9	24	47

Следовательно, при уровне загрузке $\rho = 0,4$ производительность процессорных элементов применяемого на ПМ сетевого оборудования позволяет за время менее 50 мс выполнить переконфигурирование ПМ в соответствии с обстановкой по нагрузке информационных направлений и классов трафика в текущий момент времени. Исключение составляет маршрутизатор Juniper SRX-650 при обслуживании 100 ПД. Выполнение требования по времени переконфигурирования данных маршрутизаторов возможно при снижении загрузки сетевых коммутационных устройств за счет снижения скорости передачи низкоприоритетного трафика.

При уровне загрузке $\rho = 0,6$ вносимая задержка на маршрутизаторе Cisco 3845 превышает критическое значение, что свидетельствует о возможном снижении уровня обслуживаемого трафика. В случае применения данного оборудования на федеральном уровне допустимая загрузка оборудования не должны превышать 40 % также за счет низкоприоритетного трафика. Время ожидания соединения с учетом времени переконфигурирования ПМ и времени сортировки потоков данных при реализации разработанного алгоритма допуска потоков данных в сеть в условиях перегрузки представлены в таблице 4.4 и 4.5.

Таблица 4.4 – Время ожидания соединения при коэффициенте загрузки $\rho = 0,4$

Криптографическое оборудование	Сетевое оборудование	$\rho = 0,4$		
		Время ожидания соединения, мс		
		10 ПД	50 ПД	100 ПД
Континент IPC 10	Cisco 3845 (3945) Juniper SRX-650 Juniper MX-80	32 37 34	89 96 85	-
Континент IPC 25	Cisco 3845 (3945) Juniper SRX-650 Juniper MX-80	20 25 21	75 82 71	-
Континент IPC 100	Cisco 3845 (3945) Juniper SRX-650 Juniper MX-80	12 17 13	41 48 37	108 119 100
Континент IPC 400	Cisco 3845 (3945) Juniper SRX-650 Juniper MX-80	8 13 9	30 37 26	91 102 84

Таблица 4.5 – Время ожидания соединения при коэффициенте загрузки $\rho = 0,6$

Криптографическое оборудование	Время ожидания соединения	$\rho = 0,6$		
		Время ожидания соединения, мс		
		10 ПД	50 ПД	100 ПД
Континент IPC 10	Cisco 3845 (3945) Juniper SRX-650 Juniper MX-80	44 52 40	140 158 136	-
Континент IPC 25	Cisco 3845 (3945) Juniper SRX-650 Juniper MX-80	36 44 32	116 134 112	-
Континент IPC 100	Cisco 3845 (3945) Juniper SRX-650 Juniper MX-80	24 32 20	65 83 61	148 171 131
Континент IPC 400	Cisco 3845 (3945) Juniper SRX-650 Juniper MX-80	22 30 18	49 47 45	131 154 114

Из таблиц 4.4 и 4.5 видно, что время с начала передачи информации о занятии абонентской линии до момента получения пользовательским (оконечным) оборудованием от оконечного узла сети связи сигнала готовности к приему номера (время отклика узла связи), т.е. время ожидания установления соединения (занятия КР) для рассмотренных типов сетевого и криптографического оборудования удовлетворяет заданному требованию – не более 2 с. Проведенный анализ доказал применимость и работоспособность разрабатываемого модельно-алгоритмического обеспечения на всем диапазоне исходных данных**.**

Таким образом, разработанный комплекс алгоритмов согласования трафика с VPN-туннелем позволяет реализовать динамическое управление арендуемым канальным ресурсом транспортной сети за счет классификации, сглаживания, управления планировщиком пограничного маршрутизатора.

4.7. Выводы по четвёртому разделу

1. В данном разделе диссертации предложен вариант модернизированного VPN-шлюза сети доступа защищенной корпоративной мультисервисной сети связи, отличающийся от существующих введением в состав VPN-шлюзов дополнительных функциональных элементов: классификатора потоков данных, программного модуля конфигурирования планировщика, устройства сглаживания трафика.

2. Внедрение разработанных дополнительных функциональных элементов позволяет реализовать комплекс алгоритмов, обеспечивающих взаимодействие между VPN-шлюзом сети доступа и пограничным маршрутизатором транспортной сети, что позволяет гибко использовать пропускную способность арендуемого канала связи за счет переконфигурирования планировщика пограничного маршрутизатора при отсутствии перегрузки по информационным направлениям и классам трафика.

3. За счет применения алгоритма классификации трафика, поступающего от терминальных аппаратов пользователей на вход внутреннего маршрутизатора VPN-шлюза, реализуется идентификация потоков данных для каждой предоставляемой инфокоммуникационной услуги и определение их соответствия VPN-туннелям согласно списков доступа.

4. Реализация алгоритма сглаживания агрегированного потока данных позволяет в отсутствии перегрузки повысить эффективность использования канального ресурса ЗКМСС при обеспечения качества обслуживания потоков данных, передаваемых по всем VPN-туннелям.

Заключение

В диссертационной работе решена актуальная научная задача, заключающаяся в разработке модельно-алгоритмического обеспечения, учитывающего влияние СКЗИ на объемно-временные характеристики ПДРВ, позволяющего обеспечить гарантированный уровень КО и повысить при этом степень использования КР за счет реализации процедур управления допуском в условии перегрузки и управления канальным ресурсом транспортной сети в ее отсутствии.

Основные результаты диссертационного исследования состоят в следующем.

1. Экспериментальное исследование применимости существующих математических моделей, позволяющих выявить зависимость достижимого уровня качества обслуживания потоков данных реального времени от конфигурации системы управления нагрузкой, планировщика обслуживания пакетов при описании параметров агрегированных потоков на выходе VPN-шлюза, доказало их неадекватное функционирование.

2. Предметно-классификационный анализ условий функционирования защищенных корпоративных мультисервисных сетей связи показал, что для эффективного использования арендуемых ресурсов транспортной сети коммутации пакетов целесообразно учитывать влияние процедуры шифрования данных в VPN-шлюзах на параметры трафика, генерируемого терминальным оборудованием.

3. Разработанный алгоритм динамического резервирования канального ресурса агрегированного потока данных реального времени VPN-туннеля позволяет выявить зависимости между достижимым уровнем качества обслуживания потоков данных реального времени, зарезервированным канальным ресурсом и конфигурацией механизмов системы управления потоками, интегрированной в VPN-шлюз.

3 Разработанный алгоритм допуска потоков в сеть позволяет учесть приоритеты и длительность сеанса поступающих на обслуживание потоков данных сервисов реального времени и уменьшить вероятность потерь вызовов от высокоприоритетных пользователей. При функционировании сети в условии перегрузки выигрыш (по значению вероятности потерь вызовов) от применения алгоритма может достигать до 30%.

4 Разработанный комплекс алгоритмов согласования трафика с VPN-туннелем совместно с алгоритмом допуска потоков в сеть дает возможность повысить степень использования канального ресурса: в условиях штатного функционирования сети доступа за счет перераспределения незадействованного канального ресурса между предоставляемыми инфокоммуникационными сервисами, а в условиях возникновения перегрузки за счет решения задачи выбора оптимального набора допущенных к обслуживанию потоков с учетом их приоритетов. При отсутствии перегрузки повышение степени использования резервируемого на этапе планирования сети канального ресурса федерального сегмента может достигать до 40 %.

Направлениями дальнейших исследований являются:

- разработка системы управления трафиком в ЗКМСС, учитывающей особенности инфокоммуникационного обеспечения привилегированных пользователей в условиях воздействия дестабилизирующих факторов;

- разработка модели шифрованного агрегированного потока данных реального времени, учитывающей влияние VPN-шлюзов на параметры трафика в различных режимах шифрования и аутентификации;

- разработка алгоритма динамического перераспределения канального ресурса транспортной сети ЗКМСС, учитывающего надежность обслуживающих приборов транспортной сети и дрейф параметров арендуемых каналов связи.

Список сокращений и условных обозначений

ЕСЭ – единая сеть электросвязи

ЗКМСС – защищенная корпоративная мультисервисная сеть связи

КР – канальный ресурс

КО - качество обслуживания

МПИ – межпакетный интервал

МСЭ-Т – международный союз электросвязи по телефонии

ПАО – публичное акционерное общество

ПДРВ – потоки данных реального времени

ПО – программное обеспечение

СВ – случайная величина

СКЗИ – средство криптографической защиты информации

СФП – суммарная функция поступления

ТА – терминальный аппарат

ЭМВОС – эталонная модель взаимодействия открытых систем

AH (Authentication Header) – протокол (стандарт), обеспечивающий аутентификацию пакетов и выявление их воспроизведения;

CAC (Connection Admission Control) – управление допуском соединений в сеть

CBQ (Class Based Queuing) – алгоритм по классам обслуживания

ESP (Encapsulating Security Payload) – протокол (стандарт), обеспечивающий конфиденциальность, аутентификацию источника и целостность данных, а также сервис защиты от воспроизведения пакетов;

FIFO (First in first out) – первый пришел первый ушел

MBAC (Measurement-based CAC) – управление допуском соединений в сеть, основанное на измерениях нагрузки

MPLS (Multi-Protocol Label Switching) – многопротокольная коммутация по меткам

NC (Network Calculus) –сетевое исчисление

NGN (Next Generation Network) – концепция построения сетей связи

следующего поколения

PBAC (Parameter-based CAC) – параметрическое управление допуском соединений в сеть

PHB (Per Hop Behavior) – правила обработки пакетов

RSVP (Resource Reservation Protocol) – протокол резервирования ресурсов

SPI (Security Parameter Index) – индекс параметра безопасности

SLS (Service Level Specifications) – спецификация уровня обслуживания

TE (Traffic Engineering) – управление трафиком

VPN (Virtual Private Network) – виртуальная частная сеть

WFQ (Weighted Fair Queuing) – алгоритм взвешенной справедливой очередности

n – количество потоков данных реального времени

i – порядковый номер потока данных реального времени

s – класс сервиса потока данных реального времени

k – порядковый номер канала связи

$t(\text{дост})$ – достижимая максимальная сквозная задержка пакета i-го потока данных s-го класса трафика «из конца в конец», сек.

$t(\text{треб})$ – требуемая максимальная сквозная задержка пакета i-го потока данных s-го класса трафика «из конца в конец», сек.

$N_s^{TA}(\text{kat}1)$ – количество терминальных аппаратов s-го предоставляемого сервиса 1 категории абонентов, единицы

$N_s^{TA}(\text{kat}2)$ – количество терминальных аппаратов s-го предоставляемого сервиса 2 категории абонентов, единицы

$t_{\text{Ш}}$ – максимальная задержка обработки пакета потока данных в VPN-шлюзе вследствие шифрования информации, сек.

$t_{\text{ПМ}}$ – максимально допустимая задержка обработки пакета потока данных в пограничном маршрутизаторе, сек.

$t_{\text{КС}}$ – максимальная задержка обработки пакета при его передаче по арендуемому каналу связи, сек.

l – порядковый номер VPN-туннеля

p – пиковая скорость генерации пакетов, байт/с

r – средняя скорость генерации пакетов, байт/с

b – размер буфера («корзины»), байт

L – максимальный размер пакета данных, байт

α, β, γ – коэффициенты влияния процедуры шифрования информации на мгновенную пиковую, среднюю скорость передачи данных и длины пакетов каждого s-го предоставляемого сервиса, доли единиц

$R_{\text{КС}}$ – пропускная способность канала связи, байт/с

$V(n)$ – суммарная важность n обслуживаемых потоков данных реального времени, определяет количество обслуживаемых ПДРВ

$\delta^{\text{исп}}(t)$ – показатель оценивания степени использования канального ресурса защищенной корпоративной мультисервисной сети связи при отсутствии перегрузки, %

ΔR_s – незадействованный канальный ресурс, зарезервированный для предоставления s-го класса сервиса, байт/с

R_s – максимальный резервируемый канальный ресурс на этапе планирования сети для каждого предоставляемого класса сервиса, байт/с

$Tb = (r, b, p, L)$ – алгоритм «корзина маркеров», реализуемый формирователем трафика

$A_i(t)$ – количество нагрузки i-го потока, поступившей в систему за период времени (0, t], байт

t – время, определяющее максимальный размер пачки пакетов в буфере сетевого устройства и максимальную длительность передачи пачки пакетов с пиковой скоростью генерации блоков данных p, сек.

$W_i(t)$ – функция обслуживания, определяющая минимальный объем данных, переданных в канал связи с выхода пограничного маршрутизатора при резервировании пропускной способности для i-го потока данных R_i, байт

$t_{\text{зап}\,i}$ – время запаздывания в обслуживании пакета в пограничном маршрутизаторе, сек.

R_i – канальный ресурс, резервируемый для обслуживания i-го потока данных реального времени, байт/с

$A_{\text{СФП}}(t)$ – суммарная функция поступления для аналитического описания агрегированного потока данных, байт

$R_{\text{изол}}(n)$ – канальный ресурс для агрегированного потока данных на основе модели изолированного обслуживания, байт/с

$R_{\text{СФП}}(n)$ – канальный ресурс для агрегированного потока данных на основе модели суммарной функции поступления, байт/с

$t_{\text{ПМ}}$ – минимально требуемая задержка к обработке пакета в пограничном маршрутизаторе среди n потоков данных, сек.

$R_{\text{VPN}}^{\text{СФП}}(n)$ – канальный ресурс, резервируемый для шифрованного агрегированного потока данных VPN-туннеля на основе суммарной функции поступления, байт/с

Z^{TA} – нагрузочная характеристика потоков данных при предоставлении услуг защищенной IP-телефонии и видеотелефонии, Эрл

Pr_i – приоритет i-го ПДРВ, характеризующий общий для класса услуг уровень его значимости, единицы

d_i – индикатор, который определяет порядковые номера потоков данных, выполнение которых может быть отменено для высвобождения канального ресурса, единицы

kat – количество категорий пользователей в ЗКМСС, которым предоставляется данный класс услуг, единицы

kat_i^A – категория абонента, инициирующего установление i-го ПДРВ, единицы

kat_i^B – категория абонента, кому инициирован i-ый ПДРВ, единицы

$T^{эксп}$ – время проведения эксперимента на имитационной модели, мин.

t_s^{min} – минимальное время длительности сеанса *s*-го класса сервиса, сек.

t_s^{max} – максимальное время длительности сеанса *s*-го класса сервиса, сек.

ΔR_{VoIP} – незадействованный КР для услуги IP-телефонии, байт/с

ΔR_{VioIP} – незадействованный КР для услуги видеотелефонии, байт/с

Список литературы

1. Абросимов, Л.И. Методология анализа вероятностно-временных характеристик вычислительных сетей на основе аналитического моделирования [Текст] : дис. … д-ра тех. наук : 05.13.13 / Абросимов Леонид Иванович. – М., 1996. – 415 с.

2. Абчук, В.А. Справочник по исследованию операций / В.А. Абчук, Б.Ю. Матвейчик. – М. : Воениздат, 1979. – 368 с.

3. Аджалов, В.И. Метод управления с динамической настройкой ресурсов узлов коммутации для передачи пакетов данных информационных потоков / В.И. Аджалов, А.С. Курапов // Радиотехника и электроника. – 2002. – Т. 4. – № 3. – С. 334-342.

4. Айвазян, С.А. Прикладная статистика: Исследование зависимостей : справ. изд. / С.А. Айвазян, И.С. Енюков, Л.Д. Мешалкин. – М. : Финансы и статистика, 1985. – 487 с.

5. Бакланов, И.Г. NGN : принципы построения и организации / И.Г. Бакланов. – М.: Эко-Трендз, 2008. – 400 с.

6. Биячуев, Т.А. Безопасность корпоративных сетей / Т.А. Биячуев, Л.Г. Осовецкий. – СПб : СПб ГУ ИТМО, 2004. – 161 с.

7. Бондаренко, А.Д. Интеллектуальные системы сетевого управления / А.Д. Бондаренко. – BYTE. 2005. – №10. – С. 48-52.

8. Бондаренко, А.Д. Проектирование интеллектуальных систем управления компьютерными сетями / А.Д. Бондаренко, Ю.Л. Леохин // Вестник Московского государственного университета леса. – 2007. – №2. – С. 180-186.

9. Бродский, Ю.И. Лекции по математическому и имитационному моделированию / Ю.И. Бродский; Фед. исследовательский центр Информатика и управление РАН. – М. : Директмедиа Паблишинг, 2015. – 240 с.

10. Буранова, М.А. Исследование статистических характеристик самоподобного телекоммуникационного трафика / М.А. Буранова // Инфокоммуникационные технологии. – 2012. – Т. 10, № 4. – С. 35-40.

11. Вавилов, А.А. Имитационное моделирование производственных систем / А.А. Вавилов, Д.Х. Имаев, В. И. Плескунин. – М.: Машиностроение, 1983. – 416 с.

12. Васильев, А.В. Системно-сетевые решения по внедрению технологий NGN на российских сетях связи / А.В. Васильев, С.П. Соловьев, А.Е. Кучерявый // Электросвязь. – 2005. – № 3. – С. 4–7.

13. Введение в многокритериальную оптимизацию: учеб.-метод. пособие. / А.Г. Коротченко [и др.] ; Нижегородский гос. ун-т им. Н.И. Лобачевского. – Н. Новгород : ННГУ, 2017. – 55 с.

14. Галимьянова, Н.Н. Отношения оптимальных значений целевых функций Задачи о ранце и ее линейной релаксации / Н. Н. Галимьянова, А.А. Корбут, И.Х. Сигал // Известия РАН. Теория и системы управления. – 2009. – № 6. – С. 62–69.

15. Гальцев, А.А. Системный анализ трафика для выявления аномальных состояний сети [Текст] : дис. … канд. техн. наук : 05.13.01 / Гальцев Алексей Анатольевич. – 2013.– 116 с.

16. Гвишиани, Д.М. Многокритериальные задачи принятия решений / Д.М. Гвишиани, С.В. Емельянова. – М. : Машиностроение, 1978. – 192 с. : ил.

17. Гермейер, Ю. Б. Введение в теорию исследования операций / Ю.Б. Гермейер. – М. : Наука, 1971. – 384 с.

18. Горбунов, А.Р. Парадигмы имитационного моделирования: новое в решении задач стратегического управления (объединенная логика имитационного моделирования) / А.Р. Горбунов, Н.Н. Лычкина // Бизнес-информатика. Национальный исследовательский университет Высшая школа экономики. – 2007. – № 2. – С. 60-66.

19. Емельянов, В.В. Имитационное моделирование систем / В.В. Емельянов, С.И. Ясиновский. – М. : Издательство МГТУ им. Баумана, 2009. – 583 с.

20. Ершов, В.А. Метод расчета вероятности потерь информационных ячеек на узле быстрой коммутации пакетов с асинхронно-временным мультиплексированием / В.А. Ершов // Управление в распределенных системах. М. : Наука, – 1993. – С. 21-26.

21. Ершова, Э.Б. К вопросу оценки качества обслуживания в сети NGN / А.Н. Костин // TComm: Телекоммуникации и транспорт. – 2010. – №7. – С. 66 – 71.

22. Захватов, М.А. Построение виртуальных частных сетей на базе технологии MPLS / М.А. Захватов // Издательский дом «Вильямс». – 2001. – 47 с.

23. Иванов, Е.В. Имитационное моделирование средств и комплексов связи и автоматизации : учеб. пособие / Е.В. Иванов ; Воен. ак. связи. – СПб. : ВАС, 1992. – 206 с.

24. Игошин, В.И. Теория алгоритмов / В.И. Игошин. – М. : ИНФРА-М, 2013. – 318 с.

25. Карпов, Ю.Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic / Ю.Г. Карпов. – СПб : БХВ-Петербург, 2006. – 400 с.

26. Каталевский, Д.Ю. Основы имитационного моделирования и системного анализа в управлении : учеб. пособие / Д.Ю. Каталевский ; ФГБОУ ВПО Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации. – М. : Издательский дом Дело РАНХиГС, 2015. – 496 с., ил.

27. Кини, Р.Л. Принятие решений при многих критериях: Предпочтения и замещения / Р.Л Кини, Х. Райфа. – М. : Радио и связь, 1981. – 164 с.

28. Кобзарь, А.И. Прикладная математическая статистика. Для инженеров и научных работников / А. И. Кобзарь. – М. : Физматлит, 2006. – 618 с.

29. Коваленко, О.Н. Совершенствование метода оперативного распределения пропускной способности каналов мультисервисной сети с

целью повышения эффективности их использования [Текст] : дис. … канд. техн. Наук : 05.12.13 / Коваленко Ольга Николаевна. – Новосибирск, 2009. – 155 с.

30. Коган, Д.И. Динамическое программирование и дискретная многокритериальная оптимизация : учеб. пособие / Д.И. Коган ; Нижегородский гос. ун-т им. Н.И. Лобачевского. – Н. Новгород : ННГУ, 2005. – 260 с.

31. Концептуальные положения по построению мультисервисных сетей на ВСС России // Министерство Российской Федерации по связи и информатизации. – М., 2001. – Вер. 4. – 32 с.

32. Корнеенко, В.П. Методы оптимизации: / В.П. Корнеенко. – М. : Высш. шк., 2007. – 64 с. : ил.

33. Корнышев, Ю.Н. Теория телетрафика / Ю.Н. Корнышев, А.П. Пшеничников, А.Д. Харкевич. – М. : Радио и связь, 1996. – 270 с.

34. Короткое, Е.С. Алгоритм профилирования и формирования трафика корпоративной информационной системы / Е.С. Короткое, В.П. Мочалов // Корп. инф. системы 2004 : материалы межд. науч.-практ. конф. / Юж.-рос. гос. техн. ун-т.– Новочеркасск, 2004. – С 31-36.

35. Костин, А.А. Методы проектирования систем управления телекоммуникационными сетями и услугами / А.А. Костин // Электросвязь. – 2003. – № 2. – С.21-23.

36. Костин, А.А. Модель системы интегрированного управления телекоммуникационными сетями и услугами / А.А. Костин // Электросвязь. – 2002. – №10. – С.22-26.

37. Костин, А.А. Планирование управления телекоммуникациями / А.А. Костин // Сети и системы связи. – 2002. – №11. – С. 88-94.

38. Крупский, В.Н. Математическая логика и теория алгоритмов / В.Н. Крупский, В.Е. Плиско. – М. : ИЦ Академия, 2013. – 416 с.

39. Кудрявцева Е.Н., Росляков А.В. Применение теории сетевого исчисления к исследованию систем массового обслуживания с обратной связью // T-Comm: Телекоммуникации и транспорт. – 2015. – No1. – С. 17-21.

40. Кузнецова, Т.А. Сравнение программных средств имитационного моделирования систем массового обслуживания / Т.А. Кузнецова, В.А. Мещеряков // Омск. гос. тех. ун-т : материалы межд. науч.-практ. конф. / Омск. фонд национальной стратегии развития. – Омск, 2015. – С.187-192.

41. Кулябов, Д.С. Архитектура и принципы построения современных сетей и систем телекоммуникаций : учеб. пособие / Д.С. Кулябов, А.В. Королькова ; Рос. ун-т дружбы народов. – М. : РУДН, 2008. – 281 с.

42. Курапов, А.С. Влияние протокола резервирования ресурсов RSVP на качество передачи информации в IP сети / А.С. Курапов // Материалы 42 (XLII) науч. конф. / Московский физ.-техн. ин-т. – Москва-Долгопрудный, 1999. – Ч. 2. – С. 10-11.

43. Курапов, А.С. Исследование способов контроля общих параметров качества обслуживания потоков видеоинформации / А.С. Курапов // Цифровая обработка сигналов и ее применение : материалы 4 межд. конф. / Ин-т проблем упр. им. В.А. Трапезникова. – Москва, 2002. – Т. 1. – С. 48-50.

44. Курапов, А.С. Разработка и исследование способа управления пакетной передачей потоков видеоинформации с динамической настройкой ресурсов узлов коммутации [Текст] : дис. … канд. техн. наук : 05.12.13 / Курапов Александр Сергеевич. – М., 2002. – 146 с.

45. Курочкин, И.И. Проект добровольных распределенных вычислений Netmax@home по имитационному моделированию телекоммуникационных сетей / И.И. Курочкин // Вычислительная механика и современные прикладные программные системы (ВМСППС'2015) : материалы 19 (XIX) межд. конф. / Московский ав. ин-т (национальный исследовательский университет). – Москва, 2015. – С. 149-151.

46. Кутненко, В.В. Разработка и анализ распределенных систем интерактивной мультимедиа и графики в глобальных сетях [Текст] : дис. … канд. техн. наук : 05.13.13 / Кутненко Василий Васильевич. – М., 2004. – 186 с.

47. Кучерявый, Е.А. Управление трафиком и качество обслуживания в сети Internet / Е.А. Кучерявый. – СПб. : Наука и техника, 2004. – 336 с.

48. Кучук, Г.А. Метод оперативной оценки статистических характеристик агрегированного трафика / Г.А. Кучук // Авиационно-космическая техника и технология. – 2013. – № 7. – С. 211–214.

49. Лазарев, А.А. Методы и алгоритмы решения задач теории расписаний для одного и нескольких приборов и их применение для задач комбинаторной оптимизации [Текст] : дис. … д-ра физ.-мат. наук : 05.13.01 / Лазарев Александр Алексеевич. – М., 2007. – 220 с.

50. Лазарев, В.Г., Лазарев Ю.В. Динамическое управление потоками информации в сетях связи: / В.Г. Лазарев, Ю.В. Лазарев. – М. : Радио и связь, 1983. – 216 с.

51. Левин, В.И. Анализ времени передачи информации по сетевому каналу / В.И. Левин // Автоматика и вычислительная техника. – 1991. – № 2. – С. 17-24.

52. Левин, М.Ш. Эвристический алгоритм для многокритериальной блочной задачи о рюкзаке / М.Ш. Левин, А.В. Сафонов // Информатика и управление. – 2009.– № 4. – С. 53-64.

53. Лемешко, А.В. Модель и метод предотвращения перегрузки с активным управлением очередью на узлах телекоммуникационной сети / А.В. Лемешко, М.В. Семеняка // Проблемы телекоммуникаций. – 2014. – С. 91–104.

54. Лисиенко, О.Г. Моделирование сложных вероятностных систем : учеб. пособие / В. Г. Лисиенко [и др.]; Уральский фед. ун-т. – Екатеринбург: УРФУ, 2011. – 200 с.

55. Лысиков, А. А. Использование методов Network Calculus для решения задачи планирования VPN / А. А. Лысиков // Тез. докл. на XXII Российской НТК ПГУТИ, Самара, 2015. – С. 36-37.

56. Лысиков, А. А. Теория Network Calculus и ее применение к исследованию систем автоматики и электроники / А. А. Лысиков, А. В. Росляков // Тез. докл. на V Международной молодежной научной школе-конференции «Современные проблемы физики и технологий», МИФИ, Москва, 2016. – Ч.1. – С. 184-186.

57. Лысиков, А. А. Теория сетевого исчисления и ее применение к VPN / А. А. Лысиков, А. В. Росляков // Тез. докл. на XVII Международной НТК "Проблемы техники и технологий телекоммуникаций", Самара, 2016 г. – С. 37-41.

58. Лысиков, А.А. Исследование граничных значений задержек трафика VPN с учетом конкурирующих потоков / А.А. Лысиков // Инфокоммуникационные технологии. – 2017. – Т. 15. – № 1. – С. 40-49.

59. Лысиков, А.А. Программный пакет планирования виртуальных частных сетей на основе теории сетевого исчисления / А.А. Лысиков // Международный журнал прикладных и фундаментальных исследований. – 2016. – Т. 11. – № 3. – С. 375-379.

60. Лычкина, Н.Н. Имитационное моделирование экономических процессов / Н.Н. Лычкина. – М.: ИНФРА-М, 2012. – 254 с.

61. Марьенков, А.Н. Повышение безопасности компьютерных систем и сетей на основе анализа сетевого трафика / А.Н. Марьенков, И.М. Ажмухамедов // Инфокоммуникационные технологии. – 2010. – Т. 8. – № 3. – С.106-108.

62. Миронов, О.Ю. Математическая модель узла группирования потоков данных реального времени, учитывающая изменение длин генерируемых пакетов, пиковой и средней скорости передачи данных, задержки обработки пакетов в процессе шифрования / О.Ю. Миронов // T-Comm: Телекоммуникации и транспорт. – 2018. – Т. 12. – № 8. – С. 77-87.

63. Миронов, О.Ю. Математическое представление доступа потоков данных в сети передачи данных системы управления единой системы газоснабжения РФ / О.Ю. Миронов, Ю.И. Игнатов, В.Г. Кучук // Современные проблемы информатизации : материалы 21 (XXI) межд. откр. науч. конф. / Воронежский гос. тех. ун-т. – Воронеж, 2015. – С. 327-333.

64. Миронов, О.Ю. Моделирование потоков данных реального времени в защищенных корпоративных мультисервисных сетях связи на основе детерминированного сетевого исчисления / О.Ю. Миронов, Д.В. Шелковый, О.О. Басов // Научные ведомости Белгородского

государственного университета – Экономика. Информатика. – 2018. – Т. 45. – № 3. – С. 584-594.

65. Миронов, О.Ю. Модуль перераспределения ресурсов : свидетельство о государственной регистрации программы для ЭВМ. № 2017615487 от 17.05.2017 РФ / О.Ю. Миронов [и др.]. – № 2017612501 ; заявл. 21.03.2017 ; зарегистрировано в Реестре программ для ЭВМ 17.05.2017.

66. Миронов, О.Ю. Модуль управления допуском потоков данных : свидетельство о государственной регистрации программы для ЭВМ. № 2017615514 от 17.05.2017 РФ / О. Ю Миронов [и др.] – № 2017612492 ; заявл. 21.03.2017 ; зарегистрировано в Реестре программ для ЭВМ 17.05.2017.

67. Миронов, О.Ю. Обеспечение гарантированного обслуживания потоков данных в мультисервисных сетях связи промышленного назначения / О.Ю. Миронов // «ИНФОКОМ - 2015» : материалы 8 (VIII) межд. мол. науч.-практ. конф. / Сев.-кав. филиал МТУСИ. – Ростов-на-Дону, 2015. – С. 202–205.

68. Миронов, О.Ю. Обеспечение качества обслуживания блоков данных в инфокоммуникационных сетях технологического управления / О.Ю. Миронов // «ИНФОКОМ - 2013»: материалы межд. мол. науч.-практ. конф. / Сев.-кав. филиал МТУСИ. – Ростов-на-Дону, 2013. – С. 144–147.

69. Миронов, О.Ю. Обеспечение приоритетного обслуживания потоков данных в режиме перераспределения сетевых ресурсов распределенной информационной системы / О.Ю. Миронов, В.А. Дунаев, К.Ю. Петрухин // Современные проблемы информатизации : материалы (22) XXII межд. откр. науч. конф. / Воронежский гос. тех. ун-т. – Воронеж, 2017. – С. 268-273.

70. Миронов, О.Ю. Проблемы внедрения NGN-технологий в корпоративные инфокоммуникационные системы / О.Ю. Миронов, И.А. Саитов, И.А. Орлов // Информационные системы и технологии – ФГБОУ ВПО «Госуниверситет-УНПК». – 2012. – № 4 (72). – С. 111-116.

71. Миронов, О.Ю. Программный модуль управления планировщиком пограничного MPLS маршрутизатора VPN : свидетельство о государственной регистрации программ для ЭВМ № 2018617168 Российская Федерация / О. Ю Миронов [и др.] – № 2018614940 ; заявл. 03.05.2018 ; зарегистрировано в Реестре программ для ЭВМ 19.06.2018 г.

72. Миронов, О.Ю. Расчет ресурсов для группового потока данных : свидетельство о государственной регистрации программ для ЭВМ. № 2017614736 от 26.04.2017 РФ / О. Ю. Миронов [и др.] – № 2017612481 ; заявл. 21.03.2017 ; зарегистрировано в Реестре программ для ЭВМ 26.04.2017.

73. Миронов, О.Ю. Способ сглаживания приоритетного трафика данных и устройство для его осуществления: патент на изобретение / О.Ю. Миронов [и др.], заявитель и патентообладатель Государственное казенное образовательное учреждение высшего профессионального образования Академия ФСО России. – № 2601604. заявл. 02.09.2015; решение о выдаче патента 14.10.2016 г.

74. Миронов, О.Ю. Управление доступом потоков данных в мультисервисных сетях связи, развернутых в интересах мониторинга Единой системы газоснабжения России с учетом эффекта группирования потоков // О.Ю. Миронов // Телекоммуникации. – 2016. – № 5. – С. 42-48.

75. Миронов, О.Ю. Управление доступом потоков данных в мультисервисных сетях связи промышленного назначения / О.Ю. Миронов // «Научная сессия ТУСУР – 2015» : материалы 20 (XX) всерос. науч.-тех. конф. / Томск. гос. ун-т систем управления и радиоэлектроники. – Томск, 2015. – С. 127-129.

76. Миронов, О.Ю. Управление доступом потоков данных к сетевым ресурсам распределенных информационных систем / О.Ю. Миронов, Ю.Н. Игнатов, Е.А. Кудрявцев // Современные проблемы информатизации : материалы 22 (XXII) межд. откр. науч. конф. / Воронежский гос. тех. ун-т. – Воронеж, 2017. – С. 37-41.

77. Миронов, О.Ю. Управление доступом потоков данных реального времени в защищенных корпоративных мультисервисных сетях связи / О.Ю. Миронов // Технологии информационного общества : материалы 12 (XII) межд. отрасл. науч.-тех. конф. / Московский тех. ун-т связи и информатики. – Москва, 2018. – С. 70-73.

78. Мочалов, Д.В. Анализ системы управления услугами NGN-мультисервисных сетей / Д.В. Мочалов, Д.В. Владимиров, Т.А. Плахутина // Вестник Сев.-Кав. ГТУ. – 2011. – № 2 (27). – С. 27-29.

79. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК РФ // Акты (приказы, распоряжения и другие акты) ФСТЭК России. – М. : 2013. – № 21. – 18 с.

80. Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы. Качество услуг электросвязи: концепции, модели, цели и планирование надежности работы – Термины и определения, связанные с качеством услуг электросвязи : рекомендация МСЭ-Т серии Е. 800 // Сектор стандартизации электросвязи МСЭ. – 2008. – 8 с.

81. Окулов, С.М. Программирование в алгоритмах / С.М. Окулов. – М. : Бином. Лаборатория знаний, 2013. – 384 с.

82. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. пособие / В.Г. Олифер, Н.П. Олифер. – СПб : Питер 4-е изд., 2010. – 944 с.

83. Паяин, С.В. Методика динамического управления загрузкой канала связи в корпоративных сетях с гарантированной доставкой данных [Текст] : дис. … канд. техн. наук : 05.13.17 / Паяин Семен Владимирович. – М., 2009. – 112 с.

84. Петров, В.В. Структура телетрафика и алгоритм обеспечения качества обслуживания при влиянии эффекта самоподобия [Текст] : дис. … канд. техн. наук : 05.12.13 / Петров Виталий Валерьевич. – М., 2004. – 143 с.

85. Петухов, Г.Б. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем / Г.Б. Петухов, В.И. Якунин. – М. : АСТ, 2006. – 504 с.

86. Пушнин, А.В. Критерии оценки эффективности сложных систем / А.В. Пушнин, В.И. Финаев // Межведомственный тематический научный сборник "Синтез алгоритмов сложных систем". – 1998. – № 9. – С. 261 – 264.

87. РД 45.120-2000 : Городские и сельские телефонные сети : нормы технологического проектирования // Министерство Российской Федерации по связи и информатизации. – М. 2000.– 128 с.

88. Росляков, А. В. Разработка модели VPN сети с использованием теории Network Calculus / А. В. Росляков, А. А. Лысиков // Тез. докл. на XXII Российской НТК ПГУТИ, Самара, 2015. – С. 35-36.

89. Росляков, А.В. Виртуальные частные сети. Основы построения и применения / А.В. Росляков. – М. : Эко-Трендз, 2006. – 304 с.

90. Росляков, А.В. Применение теории стохастических сетевых исчислений к анализу характеристик VPN / А.В. Росляков, А.А. Лысиков // T-Comm : Телекоммуникации и транспорт. – 2013. – Т. 7. – № 7. – С. 106-108.

91. Семенов, Ю.В. Проектирование сетей связи следующего поколения / Ю.В. Семенов. – СПб. : Наука и техника, 2005. – 240 с.

92. Сети последующих поколений – Структура и функциональные модели архитектуры : рекомендация МСЭ-Т Y.2001 / Сектор телекоммуникаций МСЭ. – 2004. – 12 с.

93. Сигал, И.Х. Введение в прикладное дискретное программирование : модели и вычислительные алгоритмы / И.Х. Сигал, А.П. Иванова. – М. : ФИЗМАТЛИТ 2е изд., 2007. – 304 с.

94. Сигал, И.Х. Задача о рюкзаке: теория и вычислительные алгоритмы / И.Х. Сигал.– М. : МИИТ, 1999. – 148 с.

95. Симонина, О.А. Модели расчета показателей QoS в сетях следующего поколения [Текст] : автореферат дис. … канд. тех. наук : 05.12.13 / Симонина Ольга Александровна. – Санкт-Петербург, 2005. – 18 с.

96. Соколов, А.Н. Методы анализа задержек IP-пакетов в сети следующего поколения [Текст] : автореф. дис. … канд. тех. наук : 05.12.13 / А.Н Соколов. – Москва, 2011. – 19 с.

97. Степанов, С.Н. Основы телетрафика мультисервисных сетей : учеб. пособие / С.Н. Степанов. – М. : Эко-Трэндз, 2010. – 392 с.: ил.

98. Трегубов, Р.Б. Программа измерения показателей качества функционирования сети связи : свидетельство о государственной регистрации программ для ЭВМ. № 2018610011 от 09.01.2018 РФ / Р.Б. Трегубов [и др.] – № 2017661070 ; заявл. 01.11.2017 ; зарегистрировано в Реестре программ для ЭВМ 09.01.2018.

99. Федорин, А.Н. Об одной задаче выбора ограниченного представительного подмножества объектов / А.Н. Федорин // Системы управления и информационные технологии. – 2008. – № 1.3 (31). – С. 416-420.

100. Фокин, В.Г. Управление телекоммуникационными сетями : учеб. пособие / В.Г. Фокин ; Сиб. гос. ун-т телекоммуникаций и информатики. – Новосибирск : СибГУТИ, 2001. – 112 с.

101. Чернышевская, Е.И. Метод обеспечения гарантированного качества обслуживания в IP-сетях / Е.И. Чернышевская, И.Ю. Селянина // Век качества. – 2010. – № 6. – С.70-72.

102. Шангин, В.Ф. Комплексная защита информации в корпоративных системах / В.Ф. Шангин. – М. : Издательский дом «Форум», 2015. – 592 с.

103. Шаройко, О.В. Методы и средства учета и динамического регулирования уровня загрузки ресурсов телекоммуникационных сетей [Текст] : дис. … канд. техн. наук : 05.13.11 / Шаройко Олег Владимирович. – Ростов-на-Дону, 2006 г. – 162 с.

104. Шедоева, С.В. Исследование и разработка методов оценки пропускной способности элементов мультисервисных сетей на этапе установления соединений [Текст] : дис. … канд. техн. наук : 05.12.13 / Светлана Васильевна Шедоева. – Новосибирск, 2004. – 153 с.

105. Шелковый, Д.В. Исследование математической модели узла коммутации защищенной корпоративной мультисервисной сети связи / Д.В. Шелковый, А.Б. Фокин, С.А. Корнилов // Экономика и менеджмент систем управления. – 2017. – Т. 24. – № 2.2. – С. 291–300.

106. Шелковый, Д.В. Модель узла коммутации корпоративной мультисервисной сети связи / Д.В. Шелковый [и др.] // Научные ведомости Белгородского государственного университета. – 2017. – № 42. – С. 148–157.

107. Шелухин, О.И. Моделирование информационных систем: учеб. пособие / О.И. Шелухин. – М.: Горячая линия-Телеком, 2012. –516 с. : ил.

108. Шмелев, И.В. Исследование и разработка метода оперативного управления мультисервисной сетью для потоков трафика с фрактальными свойствами [Текст] : дис. … канд. техн. наук : 05.12.13 / Шмелев Иван Вячеславович. – М., 2005. – 155 с.

109. Шринивас, В. Качество обслуживания в сетях IP : учеб. пособие / В. Шринивас. – М. : издательский дом "Вильямс", 2003. – 368 с.

110. Network Simulator NS-3 [Электронный ресурс]– Режим доступа : http://www.isi.edu/nsnam/ns, свободный. – Загл. с экрана.

111. A Generalized Processor Sharing Approach to Flow Control in Integrated Services Networks: The Multiple Node Case / A.K. Parekh, R.G. Gallager IEEE // ACM Transaction on Networking. – June 1993. – vol.1. – no.3. – pp.344–357.

112. Armitage, G. Quality of Service in IP networks. Foundations for a Multi-Service Internet / G. Armitage. – MTP, 2000. – 188 p.

113. Blake, S. An Architecture for Differentiated Services / D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss. – RFC 2475, December, 1998. – 25 p.

114. Boudec, J. Network calculus. A theory of deterministic queuing systems for the internet / J. Boudec, T. Patrick // Online version of the book Springer Verlag – lncs 2050 Version March 14. – 2012. – 255 p.

115. Braden, R. Integrated Services in the Internet Architecture: Overview / R. Braden, D. Clark, S.Shenker. – RFC 1633, June 1994. – 32 p.

116. Braden, R. Resource Reservation Protocol (RSVP) –Version 1 Functional Specification / R. Braden, L. Zhang, S. Berson. – RFC 2205, September 1997. – 25 p.

117. Chenker, S. Specification of Guaranteed Quality of Service / S. Chenker, C. Patridge, R. Guerin. – RFC 2212, September 1997. – 41 p.

118. Cruz, R.L. A calculus for network delay. Network elements in isolation. IEEE Transactions on Information Theory / R.L. Cruz // Volume: 37, Issue: 1, January. – 1991. – pp. 382-391.

119. Cruz, R.L. Consequences of rate control in exhaustive service pollicing systems / R.L. Cruz, M.c. Chuah. – Conf. Inform. Sci., Syst., Johns Hopkins University, Baltimore, MD, Mar. 1993. – pp. 119–125.

120. Ehrlich, M. Quality-of-Service monitoring of hybrid industrial communication networks / M. Ehrlich, A. Neumann, A. Biendarra, J. Jasperneite // Automatisierungstechnik, volume 67, number 1, 2019. – pp. 69–78.

121. Enyedi, G. An Algorithm for Computing IP/LDP Fast Reroute Using Maximally Redundant Trees (MRT-FRR). RFC 7811 [Electronic resource] / G. Enyedi, A. Csaszar, A. Atlas, C. Bowers, A. Gopalan. – 2016. – Режим доступа : http://www.faqs.org/rfcs/rfc7811. – Загл. с экрана.

122. Georgadis, L. Efficient Support of Delay and Rate Guarantees in an Internet / L. Georgadis, R. Guerin, A. Parekh // in Proceedings of ACM SIGCOMM, August 1996**. –** pp. 106–116.

123. Gunleifsen, H., Kemmerich, T., Gkioulos V. Dynamic setup of IPsec VPNs in service function chaining / H. Gunleifsen, T. Kemmerich, V. Gkioulos // Computer Networks, volume **160**, 2019. – pp. 77–91.

124. Heinanen J. Assured Forwarding PHB Group. RFC 2597 [Electronic resource] / J. Heinanen, F. Baker, W. Weiss, J. Wroclawski. – 1999. – Режим доступа : http://www.ietf.org/rfc/rfc2597.txt. – Загл. с экрана.

125. Iraschko, R. Next-Generation Video Network Design Tenets: Building a Better Video Delivery Service / R. Iraschko, J. Slevinsky // IEEE Consumer Electronics Magazine, volume 8, number 4, 2019. – pp. 22—27.

126. Jiang, Y. Stochastic Network Calculus. Springer / L. Yuming, Liu. // 9 Verlag. – 2008. –229 p.

127. Kamoun, F. IP/MPLS networks with hardened pipes: service concepts, traffic engineering and design considerations / F. Kamoun, F. Outay // J. Ambient Intelligence and Humanized Computing, volume 10, number 7. – pp. 2577—2584

128. Mason, A. IPSec Overview [Electronic resource] / A. Mason. // Cisco Press. – 2002. – Режим доступа : http://www.ciscopress.com/store/cisco-isp-essentials-9781587050411. – Загл. с экрана.

129. Nikolaus, P. h-Mitigators: Improving your stochastic network calculus output bounds / P. Nikolaus, J.B. Schmitt, M. Schütze // Computer Communications, volume 144, 2019. – pp. 188–197.

130. Plevyak T. Next Generation Telecommunications Networks, Services, and Management / Plevyak T. – New York: Wiley-IEEE Press, 2010. – 328p.

131. Recommendation Y.1540. Internet protocol data communication service - IP packet transfer and availability performance parameters / ITU-T. – Geneva. – 2016. – 48 p.

132. Recommendation Y.1541. Network performance objectives for IP-based services / ITU-T. – Geneva. – 2011. – 55 p.

133. Samrah, A.S. Improving quality of service for internet protocol television and voice over internet protocol over long-term evolution networks / A.S. Samrah, A.T. Khalil, H.M. Ibrahim // IJCNDS, volume 22, number 4, 2019. – pp. 409—446

134. Sathyan J. Fundamentals of EMS, NMS and OSS/BSS / Sathyan J. – New York: Auerbach Publications, 2010. – 588p.

135. Schmitt, J. On the Aggregation of Deterministic Service Flows. / J. Schmitt, M. Karsten, R. Steinmetz // In Proceedings of the Seventh IEEE/IFIP International Workshop on Quality of Service (IWQoS’99), London, UK, 1999.

136. Sitaraman, H. Signaling RSVP-TE Tunnels on a Shared MPLS Forwarding Plane / H. Sitaraman, V P. Beeram, T. Parikh, T. Saad // RFC, volume 8577, 2019. – pp. 1–24.

137. Venugopal, S. A Taxonomy of Data Grids for distributed data sharing, management and processing / S. Venugopal, R. Buyya, K. Ramamohanarao // ACM Computing Surveys : ACM Press, New York, USA. – March 2006. – Vol. 38. – No. 1. – pp. 106–119.

138. Wang, H. RC performance analysis based on model optimization with the aid of network calculus / H. Wang, J. Hu, W. Niu. // Photonic Network Communications, volume 37, number 2, 2019. – pp. 253–260.

139. Zhang, P., Y. Liu, J. Shi, Y. Huang, Y. Zhao. A Feasibility Analysis Framework of Time-Sensitive Networking Using Real-Time Calculus / P. Zhang, Y. Liu, J. Shi, Y. Huang, Y. Zhao // IEEE Access, volume 7, 2019. – pp. 90069–90081.

Приложение

Утверждаю

Зам.Управляющего ОпО № 0910
«Центральный» ПАО АКБ «Авангард»
г. Орёл

Ю.А. Ветрова

«17» июня 2019 г.

АКТ

об использовании результатов диссертационных исследований
Миронова Олега Юрьевича

Комиссия в составе председателя: заместителя управляющего ОпО №0910 «Центральный» ПАО АКБ «Авангард» Ветровой Юлии Алексеевны и членов комиссии: начальника операционного отдела Сиротининой Елены Николаевны , начальника отдела автоматизации и ПО Кудряшова Сергея Николаевича подтверждает, что результаты диссертационных исследований Миронова О.Ю., а именно разработанные модель и комплекс алгоритмов управления нагрузкой используются при планировании канального ресурса регионального сегмента защищенной корпоративной мультисервисной сети связи ПАО АКБ «Авангард».

Разработанная математическая модель агрегированного потока данных позволяет рассчитать требуемый канальный ресурс для меняющейся нагрузки без снижения качества обслуживания предоставляемых инфокоммуникационных сервисов. Полученный эффект от перераспределения ресурса в условиях штатного функционирования сети, а также от выбора оптимального набора допущенных к обслуживанию потоков в условиях возникновения перегрузки (нештатный режим) соответствует представленным в диссертации результатам исследований.

Председатель комиссии:

Заместитель управляющего Ветрова Ю.А.

Члены комиссии:

Начальник операционного отдела Сиротинина Е.Н.

Начальник отдела автоматизации и ПО Кудряшов С.Н.

«17» июня 2019 г.