Федеральное государственное бюджетное образовательное учреждение
высшего образования «Сибирский государственный университет
телекоммуникаций и информатики» (СибГУТИ)

На правах рукописи

Новиков Сергей Николаевич

МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ТЕХНОЛОГИЙ СЕТЕВОГО УРОВНЯ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ

Специальность: 05.13.19 – Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени доктора технических наук

Научный консультант:
доктор технических наук, профессор
Шувалов Вячеслав Петрович

Новосибирск – 2016

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Современное состояние и развитие телекоммуникационных систем, как в России, так и за рубежом, характеризуется стремлением производителей и провайдеров услуг к предоставлению пользователям (через единую точку доступа) неограниченного спектра приложений с гарантированным качеством обслуживания (Quality of Service, QoS).

Необходимо отметить, что решение данной проблемы имеет свою историю. В середине XX столетия А. А Харкевичем была высказана идея создания единой автоматизированной сети связи (ЕАСС) страны для «…удовлетворения потребностей в доставке различных видов информации для народного хозяйства и населения» [118]. Цель ЕАСС – максимально объединить, унифицировать и автоматизировать все средства связи СССР, что позволило бы значительно сократить финансовые и организационные ресурсы страны на подготовку кадров, проектирование, строительство и обслуживание телекоммуникационных систем. Однако реализация данной программы изначально была затруднена из-за использования аналоговых форм представления информации при ее передаче через ЕАСС.

В конце двадцатого столетия, с появлением новых форм представления информации и методов управления в телекоммуникационных системах, идея объединения и унификации различных служб электросвязи нашла свое отражение в создании цифровых сетей интегрального обслуживания (ЦСИО).

Первоначально предполагалось, что ЦСИО будет предоставлять пользователю возможность передачи информации в цифровом формате со скоростью $N \times 64$ кбит/с. В результате такие сети получили название узкополосные ЦСИО. Однако данное решение оказалось не способным

поддерживать высокоскоростные службы электросвязи, функционирующие в реальном масштабе времени.

С появлением технологии асинхронного метода передачи (Asynchronous Transfer Mode, ATM) [134], фундаментально отличающейся от других телекоммуникационных технологий, появилась возможность создания транспортного механизма для передачи всех видов информации с QoS. В результате такие телекоммуникационные системы получили название – широкополосные ЦСИО (рекомендации МСЭ-Т, серия I.700–799).

Конкуренция производителей, провайдеров услуг в борьбе за пользователей телекоммуникаций активизировала дальнейшее развитие интернет-протокол (Internet Protocol, IP) технологии. Как следствие, рабочей группой, проектировавшей IP (Internet Engineering Task Force, IETF), были разработаны технологии MPLS [168] (Multiprotocol Label Switching – мультипротокольная коммутация по меткам) и IP v.6.0 [167], позволяющие предоставить пользователю неограниченный спектр приложений и QoS.

В результате IP/MPLS и ATM стали базовыми технологиями для мультисервисных сетей связи (МСС) [39], которые имеют отличия, но имеют и много общего:

– любая пользовательская и служебная информация преобразуется в единую форму – цифровые блоки определенной длины (пакеты);

– к каждому цифровому блоку добавляется заголовок с данными о маршруте, который предварительно определен и гарантирует поддержание требуемых вероятностно-временных характеристик (скорость передачи информации, задержка во времени, временной джиттер, вероятность неправильного приема на сообщение/пакет/символ, вероятность отказа в обслуживании) передаваемой информации;

– передача пользовательских и служебных пакетов осуществляется путем асинхронного мультиплексирования в соответствующие пользовательские и служебные цифровые тракты и каналы;

– в пункте назначения пакеты объединяются, преобразуются в первоначальную форму и передаются пользователю для дальнейшей обработки.

Таким образом, представление всех видов информации в едином цифровом формате и выделение требуемых ресурсов сети, гарантирующих QoS, перед началом передачи пользовательской информации являются обязательными компонентами технологий IP/MPLS и ATM.

Естественно, что при уникальной возможности мультисервисных сетей связи предоставлять пользователям неограниченный спектр приложений в реальном масштабе времени возникает проблема защиты информации [69, 84, 122]. В этой связи исследовательской комиссией МСЭ-Т в 2003 г. были разработаны рекомендации X.805 «Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами» [181]. Значимость данного документа в том, что впервые определена методология организации информационной безопасности телекоммуникационных систем. Архитектура безопасности разделяет все ресурсы телекоммуникационных систем (каналы связи, программно-аппаратные комплексы, приложения и так далее) на независимые модули защиты информации. Каждый модуль характеризуется параметрами информационной безопасности, поддержание которых в актуальном (обновленном) состоянии является сложной финансовой, организационной, технической и **научной проблемой**.

Значительный вклад в решение вопросов, связанных с созданием теоретического и практического задела в построении защищенных телекоммуникационных систем, внесли работы известных ученых А.П. Алферова, Д.П. Зегжда, П.Д. Зегжда, А.С. Кузьмина, А.А. Молдовяна, Н.А. Молдовяна, Б.Я. Рябко, А.А. Шелупанова, В.В. Ященко, W. Diffie, N. Ferguson, B. Forouzan, M. Hellman, B. Schneier, A. Shamir, C. Shannon, V. Stollings и многих других.

В последнее десятилетие, начиная с публикации W. Lou и Y. Fang [150], ведутся активные исследования возможности обеспечения конфиденциальности информации в мобильных сетях за счет механизмов сетевого уровня модели взаимосвязи открытых систем [44, 55, 131, 132, 150, 163, 174]. Данный подход

имеет ряд преимуществ. Во-первых, чем масштабней сеть связи, тем больше ее ресурсов можно задействовать для обеспечения конфиденциальности пользовательской информации. Во-вторых, пользователь не обязательно должен иметь дополнительное специальное программно-аппаратное обеспечение.

По мнению автора, использование территориально-распределенных ресурсов МСС (баз данных, криптографических программно-аппаратных комплексов, каналов связи и так далее) является одним из путей обеспечения целостности, доступности и конфиденциальности информации. В этом случае пользователю достаточно определить свой профиль защиты информации – количественные или качественные оценки параметров информационной безопасности. Система управления, проведя мониторинг свободных ресурсов мультисервисной сети связи, реализует не только соединение, поддерживающее QoS для выбранного приложения, но и заявленный пользователем профиль защиты информации [135, 136].

Реализация данного подхода возможна за счет механизмов сетевого уровня модели взаимосвязи открытых систем (протоколов маршрутизации и сигнализации), в основу которых легли результаты научных исследований Г.П. Башарина, В.А. Богатырева, А.В. Бутрименко, В.М. Вишневского, С.Л. Гинзбурга, В.С. Гладкого, Б.С. Гольдштейна, И.М. Гуревича, А.В. Ершова, Г.П. Захарова, А.Е. Кучерявого, В.Г. Лазарева, А.Н. Назарова, М. Шварца, М.А. Шнепс-Шнеппе, Г.Г. Яновского, D. Barber, D. Bertsekas, D. Davies, R. Gallager, M. Gerla, L. Kleinrock, W. Price, C. Solomonides и многих других ученых.

Научная проблема, решению которой посвящена диссертация, – создание методологических основ, применения технологий сетевого уровня (протоколов маршрутизации и сигнализации) мультисервисных сетей связи для защиты информации.

Актуальность данной проблематики подтверждается тем фактом, что она затрагивает технологии, которые имеют важное социально-экономическое значение и важное значение для обороны страны и безопасности государства

(критические технологии) – распоряжение Правительства РФ от 14 июля 2012 г. № 1273–р (19 пункт: «Технологии поиска, сбора, хранения, обработки, предоставления, распространения и защиты информации»).

Тематика работы подержана администрацией Новосибирской области (совместный проект администрации Новосибирской области и ФГОБУ ВПО «СибГУТИ», 2004 г., руководитель проекта Новиков С.Н.), грантами фонда фундаментальных и прикладных научных исследований ФГОБУ ВПО «СибГУТИ» (приказы: № 2/190–11 от 28.02.2011 г.; № 2/168–12 от 21.02.2012 г.; № 2/225–13 от 20.02.2013 г.; № 2/398–14 от 21.03.2014 г.).

Цель работы – создание методологических основ и инструментария для реализации защиты информации с использованием технологий сетевого уровня мультисервисных сетей связи. Для достижения указанной цели в диссертации необходимо применительно к мультисервисным сетям связи решить следующие **задачи**:

1. Провести анализ современного состояния проблемы обеспечения конфиденциальности, целостности, доступности информации и маршрутизации.
2. Разработать методологические основы построения системы обеспечения конфиденциальности, целостности и доступности информации на базе протоколов сетевого уровня.
3. Исследовать методы маршрутизации на возможность использования ресурсов мультисервисных сетей связи для обеспечения конфиденциальности, целостности и доступности информации.
4. Разработать инструментарий (методики, модели, алгоритмы, программные продукты) исследования методов маршрутизации в условиях внешних деструктивных воздействий.
5. Исследовать влияние используемых методов маршрутизации на качество обслуживания приложений в условиях внешних деструктивных воздействий.

6. Разработать инструментарий (методики, методы, алгоритмы), обеспечивающий защиту информации без снижения качества обслуживания приложений, за счет ресурсов, распределенных в мультисервисных сетях связи.

Объектом исследования является защита информации в мультисервисных сетях связи.

Предметом исследования является совокупность методов и средств для создания системы защиты информации на основе протоколов сетевого уровня мультисервисных сетей связи.

Научная новизна работы**.**

1. *Впервые* предложена методология, *позволяющая* обеспечить защиту информации на базе протоколов сетевого уровня мультисервисных сетей связи (пункты 1, 5, 6, 13 области исследований паспорта специальности 05.13.19), включающая:

– *подход* к обеспечению конфиденциальности информации, который *в отличие* от аналогов использует многократное асимметричное шифрование ключами меньшей длины, что *позволяет* уменьшить время шифрования в l^{c-1} раз, где l – количество асимметричных шифрований, c – постоянная, значение которой определяется криптографическими алгоритмами шифрования;

– *критерий* выбора сетевых ресурсов (маршрутов) с точки зрения обеспечения целостности и доступности передаваемой информации в мультисервисных сетях связи при минимальной стоимости;

– *способ и алгоритм* обеспечения целостности информации, которые *в отличие* от известных используют параллельные (многопутевые) методы маршрутизации, учитывают вероятностно-стоимостные параметры маршрутов и *позволяют* уменьшить время задержки передачи информации;

– *алгоритм* обеспечения доступности информации в мультисервисных сетях связи, *отличающийся* от известных тем, что параллельные соединения устанавливаются в соответствии с разработанным критерием выбора сетевых ресурсов (маршрутов), *позволяющим* выбирать маршруты с точки зрения

обеспечения доступности передаваемой информации в мультисервисных сетях связи при минимальной стоимости.

2. Предложена *новая классификация* методов маршрутизации, *отличающаяся* наличием независимых процедур, включающих: формирование плана распределения информации на сети; выбор исходящих трактов передачи информации в узлах коммутации. Классификация *позволяет*: выявить множество вариантов реализации последовательных и параллельных (многопутевых) методов маршрутизации; провести целенаправленный анализ и синтез методов маршрутизации, которые будут эффективно функционировать в условиях штатной эксплуатации и *внешних деструктивных воздействий* на элементы мультисервисной сети связи (пункты 5, 6 области исследований паспорта специальности 05.13.19).

3. Предложен *новый метод* маршрутизации («Гибридный»), *отличающийся* от известных тем, что в зависимости от степени воздействия внешних деструктивных факторов на мультисервисную сеть связи, используется «Логический», «Статистический» или «Лавинный» методы. Это *позволяет* сократить объем передаваемой служебной информации в мультисервисной сети связи во время ввода узлов коммутации в эксплуатацию, штатной эксплуатации и *в условиях внешних деструктивных воздействий* на элементы сети (пункты 5, 6 области исследований паспорта специальности 05.13.19).

4. *Инструментарий* (методики, математические модели, алгоритмы, программные продукты) для анализа методов маршрутизации в мультисервисных сетях связи, который *в отличие* от известных, *учитывает* входной самоподобный трафик и *внешние деструктивные воздействия* на элементы мультисервисной сети связи и *позволяет* выявить те методы маршрутизации, которые будут наиболее эффективно функционировать *в условиях* штатной эксплуатации и *внешних деструктивных воздействий* на элементы сети (пункты 5, 6, 8 области исследований паспорта специальности 05.13.19).

5. *Способ* проверки графа сети на связность, *отличающийся* тем, что анализируемый граф «разбивают» на подграфы; каждый подграф проверяют на

связность «стягиванием» смежных вершин к первоначально выбранной, до тех пор, пока подграф не представится в виде одиночной точки или множества точек; в результате формируется суперграф, который проверяется на связность «стягиванием» смежных вершин, к первоначально выбранной, до тех пор, пока суперграф не представится в виде одиночной точки (исходный граф связен) или множества точек (исходный граф не связен); это *позволяет* уменьшить алгоритмическую сложность решения задачи в $\sqrt{S}$ (S – количество вершин графа) по сравнению с известными способами (пункт 9 области исследований паспорта специальности 05.13.19).

6. *Инструментарий* (методики, методы, алгоритмы), *позволяющий* за счет применения предлагаемых:

– параллельных (многопутевых) методов маршрутизации;
– подхода к обеспечению конфиденциальности информации;
– критерия, позволяющего выбирать сетевые ресурсы (маршруты);
– способа обеспечения целостности информации;
– алгоритма обеспечения доступности информации

обеспечить конфиденциальность, целостность, доступность информации и показатели качества обслуживания приложений мультисервисной сети связи (пункты 1, 5, 6, 8, 13 области исследований паспорта специальности 05.13.19).

Теоретическая значимость исследования обоснована тем, что:

– изложены положения, расширяющие набор методов, применяемых при создании защищенных телекоммуникационных систем, в частности, в обеспечении конфиденциальности, целостности и доступности информации за счет использования протоколов сетевого уровня модели взаимосвязи открытых систем без снижения качества обслуживания приложений мультисервисных сетей связи;

– изложены положения, относящиеся к сетевому уровню модели взаимосвязи открытых систем, и выявлены новые методы маршрутизации,

эффективно функционирующие *в условиях* штатной эксплуатации и *внешних деструктивных воздействий* на элементы сети;

– определены факторы, влияющие на уменьшение вероятности отказа в обслуживании заявок за счет применения параллельных (многопутевых) методов маршрутизации *в условиях внешних деструктивных воздействий* на элементы мультисервисных сетей связи;

– проведена модернизация существующих математических моделей маршрутизации, основанная на учете самоподобия входного трафика и *внешних деструктивных воздействий* на элементы мультисервисной сети связи.

Практическая значимость результатов.

1. Разработан инструментарий (методики, методы, алгоритмы), позволяющий реализовать конфиденциальность, целостность и доступность информации с обеспечением показателей качества обслуживания приложений мультисервисной сети связи.

2. Многократное асимметричное шифрование ключами меньшей длины позволяет обеспечить конфиденциальность информации при меньшем времени ее шифрования в l^{c-1} раз, где l – количество асимметричных шифрований, c – постоянная, значение которой определяется криптографическими алгоритмами шифрования.

3. Разработан инструментарий (методики, модели, алгоритмы, программные продукты), включающий:

– математическую модель для оценки влияния методов формирования плана распределения информации на объем сетевых ресурсов в *условиях внешних деструктивных воздействий* на элементы мультисервисной сети связи;

– математическую модель маршрутизации в условиях входного самоподобного трафика и *внешних деструктивных воздействий* на элементы мультисервисной сети связи;

– методику определения плана распределения информации на однородной ячеистой сети связи большой размерности;

– упрощенную имитационную модель маршрутизации в *условиях внешних деструктивных воздействий* на элементы мультисервисной сети связи.

Инструментарий позволяет выявить методы маршрутизации, которые будут эффективно функционировать *в условиях* штатной эксплуатации и *внешних деструктивных воздействий* на элементы мультисервисной сети связи.

4. Программная реализация разработанного способа проверки графа сети на связность позволяет уменьшить время решения задачи в $\sqrt{S}$ (S – количество вершин графа) по сравнению с известными способами.

5. Установлено, что в условиях внешних деструктивных воздействий на элементы мультисервисной сети связи (выход из строя более 30% элементов) параллельные (многопутевые) методы маршрутизации позволяют (усредненные данные) понизить среднюю вероятность отказа на обслуживание заявок пользователей до 20%.

6. Разработаны рекомендации по применению методов маршрутизации для обеспечения конфиденциальности, целостности и доступности информации в мультисервисных сетях связи.

Реализация и внедрение результатов исследований. Значение полученных результатов исследования для практики подтверждается тем, что:

– в рамках выполнения хоздоговорных НИР, грантов фонда фундаментальных и прикладных, научных исследований СибГУТИ (приказы: № 2/190-11 от 28.02.2011 г.; № 2/168-12 от 21.02.2012 г.; № 2/225-13 от 20.02.2013 г.; № 2/398-14 от 21.03.2014 г.) *разработаны* алгоритмы [2, 3, 4], математические модели и их программные реализации [6, 7, 35, 128], документы, поясняющие применение и техническое описание перечисленных алгоритмов и программ

приняты: в гос. фонд алгоритмов и программ СССР [5, 96]; в отраслевой фонд алгоритмов и программ координационного центра информационных технологий министерства образования РФ; объединенный фонд электронных ресурсов «Наука и Образование» института научной информации и мониторинга РАО и *внедрены* в

организациях: ООО «ЦИБ-Сервис» (г. Барнаул) при разработке защищенных телекоммуникационных систем связи; ООО «СИБ» (г. Новосибирск) в разработках защищенной системы видео конференцсвязи в Правительстве Республики Тыва; ООО «Предприятие «Элтекс» (г. Новосибирск) в процесс проектирования и разработки сетевого коммутационного оборудования (коммутаторов и маршрутизаторов), а так же *использованы*:

ООО «Газпром трансгаз Томск» (г. Томск) при проектировании систем управления сетями связи; в управлении информационного и документационного обеспечения губернатора Иркутской области и Правительства Иркутской области (г. Иркутск) при обеспечении безопасности каналов связи органов государственной власти, имеющих доступ к корпоративной сети передачи данных;

– в рамках выполнения госбюджетных НИР *разработаны:* обобщенная, функциональная модель маршрутизации в МСС; классификация методов маршрутизации для сетей связи; методы маршрутизации; математическая модель маршрутизации в МСС; методика обеспечения совокупности параметров, обеспечивающих защиту информации (конфиденциальность, целостность и доступность) за счет ресурсов МСС, *и внедрены* в учебный процесс СибГУТИ при проведении всех видов занятий для студентов специальности «Информационная безопасность телекоммуникационных систем» в дисциплинах «Телекоммуникационные технологии с гарантированным качеством обслуживания», «Моделирование систем», «Защита и мониторинг мультисервисных сетей связи», «Основы проектирования защищенных телекоммуникационных систем», «Живучесть телекоммуникационных систем», в рамках которых издано 3 учебных пособия с грифом УМО,

а так же *использованы* при подготовке учебно-методических комплексов проекта Европейской Комиссии TEMPUS JEP_26032_2005, в рамках которых издано учебное пособие для студентов магистратуры направления «Телекоммуникации».

Методология и методы исследования. Для достижения поставленной цели использовался математический аппарат теории вероятностей, теории массового обслуживания, теории графов и статистическое моделирование сложных систем.

Положения, выносимые на защиту.

1. *Методология*, основанная на протоколах сетевого уровня мультисервисных сетей связи, позволяет обеспечить базовые параметры информационной безопасности (конфиденциальность, доступность, целостность) (пункты 1, 5, 6, 13 области исследований паспорта специальности 05.13.19).

2. *Подход* к обеспечению конфиденциальностм информации, использующий многократное асимметричное шифрование ключами меньшей длины позволяет уменьшить время шифрования в l^{c-1} раз, где l – количество асимметричных шифрований, c – постоянная, значение которой определяется криптографическими алгоритмами шифрования (пункт 13 области исследований паспорта специальности 05.13.19).

3. *Критерий* выбора параллельных маршрутов обеспечивает целостность и доступность информации в мультисервисных сетях связи при минимальной стоимости (пункт 6 области исследований паспорта специальности 05.13.19).

4. *Способ и алгоритм*, использующие параллельные (многопутевые) методы маршрутизации и учитывающие вероятностно-стоимостные параметры маршрутов, позволяют по совокупности принятых символов обеспечить целостность информации и уменьшить время задержки при ее передаче (пункты 5, 6, 8 области исследований паспорта специальности 05.13.19).

5. *Алгоритм* формирования параллельных соединений в соответствии с предложенным критерием выбора сетевых ресурсов, учитывающий вероятностно-стоимостные параметры маршрутов, обеспечивает заданную доступность информации в мультисервисных сетях связи (пункты 5, 6 области исследований паспорта специальности 05.13.19).

6. *Классификация* маршрутизации позволяет: выявить множество вариантов реализации последовательных и параллельных (многопутевых) методов маршрутизации; провести целенаправленный анализ и синтез тех

методов маршрутизации, которые будут эффективно функционировать *в условиях* штатной эксплуатации и *внешних деструктивных воздействий* на элементы мультисервисной сети связи (пункты 5, 6 области исследований паспорта специальности 05.13.19).

7. *Метод* маршрутизации «Гибридный», являющийся обобщением «Логического», «Статистического» и «Лавинного» методов, позволяет сократить объем передаваемой служебной информации в мультисервисной сети связи во время ввода узлов коммутации в эксплуатацию, штатной эксплуатации и *в условиях внешних деструктивных воздействий* на элементы сети (пункты 5, 6 области исследований паспорта специальности 05.13.19).

8. *Инструментарий* (методики, модели, алгоритмы, программные продукты), включающий:

– математическую модель для оценки влияния методов формирования плана распределения информации на объем сетевых ресурсов в *условиях внешних деструктивных воздействий* на элементы мультисервисной сети связи;

– математическую модель маршрутизации в условиях входного самоподобного трафика и *внешних деструктивных воздействий* на элементы мультисервисной сети связи;

– методику определения плана распределения информации на однородной ячеистой сети связи большой размерности;

– упрощенную имитационную модель маршрутизации в *условиях внешних деструктивных воздействий* на элементы мультисервисной сети связи,

позволяет проводить анализ методов маршрутизации с целью выявления тех методов маршрутизации, которые будут наиболее эффективно функционировать *в условиях* штатной эксплуатации и *внешних деструктивных воздействий* на элементы мультисервисной сети связи (пункты 5, 6, 8 области исследований паспорта специальности 05.13.19).

9. *Способ* проверки графа сети на связность по сравнению с известными имеет в $\sqrt{S}$ раз меньшую алгоритмическую сложность (S – количество вершин

анализируемого графа) (пункт 9 области исследований паспорта специальности 05.13.19).

10. *Инструментарий*, включающий методики, методы и алгоритмы, позволяет обеспечить конфиденциальность, целостность и доступность информации за счет применения новых методов маршрутизации с сохранением качества обслуживания высокоскоростных приложений мультисервисных сетей связи, функционирующих в реальном масштабе времени (пункты 1, 5, 6, 8, 13 области исследований паспорта специальности 05.13.19).

Степень достоверности и апробация результатов исследования подтверждается тем, что результаты получены на сертифицированном оборудовании и программном обеспечении. Показана воспроизводимость результатов исследований в различных условиях. Теория построена на известных, проверяемых данных и фактах, в том числе для предельных случаев, согласуется с опубликованными экспериментальными данными других исследователей по данной тематике. Использованы и обобщены результаты исследований ведущих специалистов в области защиты информации телекоммуникационных систем и управления мультисервисными сетями связи. Установлено количественное совпадение численных результатов, полученных с помощью математического, имитационного моделирования и натурных экспериментов.

Основные результаты работы докладывались и обсуждались на конференциях, форумах:

– *международных* – семинар «Перспективы развития современных средств и систем телекоммуникаций» (Новосибирск, 2000 г.; Омск, 2001 г.); IV НТК «Современные информационные технологии» (Новосибирск, 2000 г.); форум по проблемам науки, техники и образования (Москва, 2001 г., 2002 г.); НТК «Актуальные проблемы электронного приборостроения» (Новосибирск, 2002г.); 6th International conference on actual problems of electronic instrument engineering proceedings, APEIE – 2002 (Novosibirsk, 2002); НТС «Перспективы развития современных средств и систем телекоммуникаций» (Санкт-Петербург, 2002 г.; Томск, 2003 г.; Екатеринбург, 2005 г.); 4-rd, 5-th International Workshop «Electron

Devices and Materials» (Erlagol, 2003, 2004); The IEEE Siberian Conference on Control and Communications, SIBCON (Tomsk, 2003, 2005); X конференция «Проблемы функционирования информационных сетей» (Новосибирск, 2008 г.); НТК «Инновационная экономика и промышленная политика региона» (ЭКОПРОМ-2009) (Санкт-Петербург, 2009 г.); VII НПК (Санкт-Петербург, 30 сентября – 3 октября 2009 г.); Leipzig University of Applied Sciences. Science Days (Germany, Leipzig, 2009);

– *всероссийских, республиканских* – Республиканская НТК «Методы управления технической диагностикой и восстановлением работоспособности элементов сетей связи» (Ташкент, 1988 г.); Российская НТК «Информатика и проблемы телекоммуникаций» (Новосибирск, 2000 г., 2001 г., 2002 г., 2008 г.); XII, XIII, XV Всероссийская НПК «Проблемы информационной безопасности государства, общества и личности» (Томск-Барнаул, 2010 г.; Томск-Новосибирск, 2012 г.; Томск-Иркутск, 2014 г.); Российская НТК «Обработка сигналов и математическое моделирование» (Новосибирск, 2012 г.); Российская НТК «Современные проблемы телекоммуникаций» (Новосибирск, 2013 г., 2015 г.); Всероссийская научно-техническая интернет-конференция с международным участием «Надежность функционирования и информационная безопасность телекоммуникационных систем железнодорожного транспорта» (Омск, 2013 г.).

Публикации. Всего по теме диссертации опубликовано 66 работ, в том числе: 14 статей в научных журналах и изданиях, рекомендованных ВАК РФ; один патент на способ изобретения; 10 свидетельств на программы для электронных вычислительных машин, зарегистрированных в установленном порядке; 6 работ включены в библиографические базы Web of Science и Scopus; 2 рецензируемых монографии; 4 рецензируемых учебных пособия, в том числе 3 с грифом УМО.

Личное участие автора в полученных результатах. В диссертации использованы результаты, в которых автору принадлежит основная роль в

постановке, решении задач и в обобщении полученных результатов. Некоторые из публикаций написаны в соавторстве с аспирантами научной группы автора (Буров А.А., Жарикова В.О., Киселев А.А., Солонская О.И.).

Структура работы. Диссертация состоит из введения, шести глав, заключения, приложений, содержит 235 страницы и включает 55 рисунков, 6 таблиц, список литературы из 184 наименований.

1 Анализ современного состояния обеспечения конфиденциальности, целостности и доступности информации в мультисервисных сетях связи

1.1 Термины и определения предметной области «Защита информации»

Основополагающими международными стандартами в области информационной безопасности являются стандарты, определяющие: архитектуру безопасности взаимосвязи открытых систем [145, 180]; концепции информационной безопасности открытых систем [146, 182]; основные составляющие обеспечения информационной безопасности (ITU-T Recommendation X.810 ÷ 815, ISO/IEC 10181-2 ÷ 7).

Для мультисервисной сети связи, ориентированной на предоставление пользователям неограниченного спектра приложений с QoS, важным документом, определяющим ее архитектуру безопасности, является ITU-T Recommendation X.805 Security Architecture for Systems providing end-to-end Communications (Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами) [181].

Архитектура безопасности (рисунок 1.1) разделяет все ресурсы телекоммуникационных систем (ТКС) (каналы связи, программно-аппаратные комплексы, приложения и так далее) на независимые:

1) функциональные плоскости защиты:

– контроля – для передачи служебной информации с целью мониторинга состояния ресурсов ТКС;

– управления – для передачи служебной информации с целью текущего управления ресурсами ТКС;

– пользователя – для передачи пользовательской информации;

2) уровни защиты:

– приложений – весь спектр приложений МСС (электронная коммерция, поисковые службы, открытый доступ к институтам управления государством, видеоконференции, дистанционное обучение, воспитание, реклама, развлечения и так далее);

– сервисов – весь спектр услуг ТКС, которые провайдеры предоставляют своим пользователям (доступ в Интернет, службы динамической конфигурации хостов, имен доменов, услуги телефонии, QoS, службы позиционирования и так далее);

– инфраструктуры – структурообразующие элементы ТКС (линии связи, каналообразующая аппаратура, маршрутизаторы, коммутаторы, серверы и так далее).

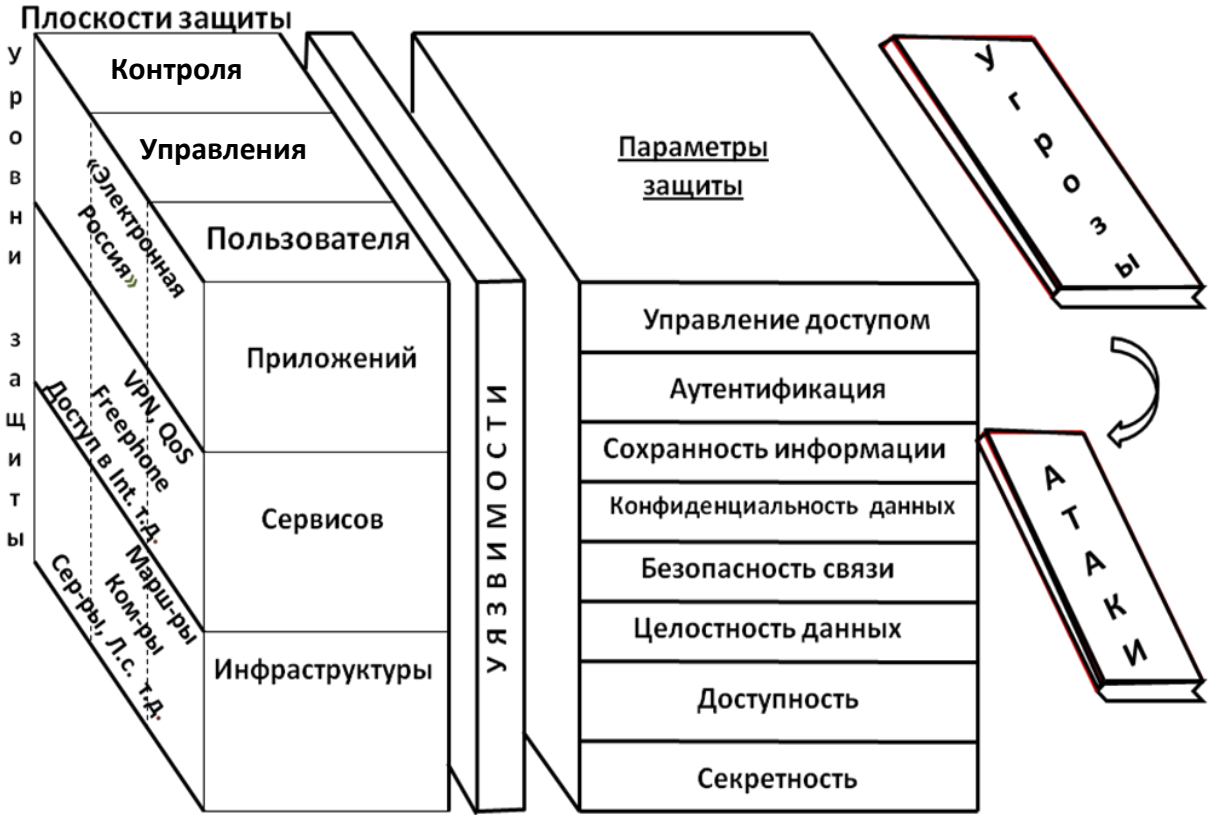


Рисунок 1.1 – Архитектура безопасности ТКС

На пересечении плоскостей и уровней формируется девять независимых модулей защиты ТКС. Каждый модуль, содержащий соответствующие программно-аппаратные средства, характеризуется восемью параметрами (измерениями) защиты:

- управление доступом;
- аутентификация;
- сохранность информации;
- конфиденциальность данных;
- безопасность связи;
- целостность данных;
- доступность;
- секретность.

Таким образом, можно утверждать следующее – для защиты информации от угроз и атак нарушителей, направленных на:

- уничтожение информации;
- искажение или изменение информации;
- кражу, удаление или потерю информации;
- раскрытие информации;
- прерывание обслуживания,

необходимо выполнить требования 72-х параметров (измерений) защиты (9 модулей, каждый из которых содержит 8 параметров защиты).

Базовыми параметрами (измерениями) защиты информации принято считать конфиденциальность, целостность и доступность [98, с.3].

Конфиденциальность данных – «Свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса» [24, с. 1] или «Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право» [98, с. 3].

Доступность информации – «Состояние информации, при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно» [98].

Целостность информации – «Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право» [99, с.2].

1.2 Анализ основных подходов по обеспечению конфиденциальности информации

Обеспечение конфиденциальности основывается на криптографических способах защиты информации, подробно представленных в многочисленных работах, в том числе [101, 117, 119, 123, 124].

Существует два принципиальных подхода:

– шифрование с одним (секретным) ключом (симметричные алгоритмы шифрования);

– шифрование с двумя (открытым и секретным) ключами (асимметричные алгоритмы шифрования).

В первом случае, как правило, время зашифрования/расшифрования прямо пропорционально длине ключа и сложности алгоритмов шифрования. Недостатком данного подхода является наличие закрытого канала связи для доставки пользователям сеансового секретного ключа.

В асимметричных криптосистемах данный недостаток отсутствует. Однако зависимость времени шифрования $t_{\text{ш}}$ от длины ключа L_k имеет нелинейный характер [123] и в общем случае определяется как

$$t_{\text{ш}} = A \cdot L_k^c + B, \tag{1.1}$$

где A, B и c – постоянные, значения которых определяются криптографическими алгоритмами. При больших значениях L_k время шифрования резко возрастает, что является неприемлемым для высокоскоростных приложений, функционирующих в реальном масштабе времени [144]. Поэтому на практике применяют «гибридную» систему шифрования. Асимметричные алгоритмы используются для организации закрытого канала связи (для доставки пользователям сеансовых секретных ключей симметричных алгоритмов

шифрования). Симметричные алгоритмы используются непосредственно для шифрования данных между пользователями.

У данного подхода есть недостаток. Пользователи должны обладать определенными знаниями в области защиты информации и иметь дополнительное специальное криптографическое программно-аппаратное обеспечение, применение которого может быть ограничено вследствие временных, технологических, финансовых или иных затрат.

В работах [43, 44, 54, 55, 150, 151, 163] предложен подход, обеспечивающий конфиденциальность информации за счет применения пороговой схемы разделения секрета и механизмов сетевого уровня модели взаимосвязи открытых систем (МВОС) – многопутевой маршрутизации.

Основная идея состоит в разделении сообщения M на несколько частей n по секретной схеме с последующей отправкой этих частей по n независимым маршрутам к получателю информации. Таким образом, если даже какое-то небольшое количество маршрутов будет подвержено атакам со стороны нарушителей, то секретное сообщение в целом не будет рассекречено и по $n' \le n$ доставленным получателю частям будет восстановлено.

На сегодняшний день известно несколько классов пороговых схем разделения секрета: Шамира (на основе степенного многочлена) [172]; на эллиптической кривой [58]; Блэкли (использование точек многомерного пространства) [137]; Карнин-Грин-Хеллмана (на основе скалярного произведения) [148]; Асмута-Блума (с использованием простых чисел) [133].

Пороговые схемы разделения секрета нашли широкое применение при решении многих задач: разделенное хранение данных; безопасная коллективная подпись; управление ключами в протоколах, содержащих большое количество участников и во многих других. В данном случае решается задача динамического распределения данных по сети с целью обеспечения конфиденциальности информации.

Основное назначение мультисервисных сетей связи состоит в предоставлении пользователям неограниченного спектра приложений, в том

числе высокоскоростных, функционирующих в реальном масштабе времени. Данное обстоятельство накладывает на реализацию механизма пороговой схемы разделения секрета временное ограничение – алгоритмическую сложность.

За последние три десятилетия вопросам исследования схем разделения секрета (в том числе оценки алгоритмической сложности) посвящено большое количество работ (например, [123, 130] и многие другие). В работе [97] проведены натурные эксперименты с целью анализа алгоритмической сложности, перечисленных пороговых схем разделения секрета, результаты которых сведены в таблицу 1.1.

Таблица 1.1 – Алгоритмическая сложность пороговых схем разделения секрета

№	Пороговая схема разделения секрета	Алгоритмическая сложность	
		Этап	
		Разделения секрета	Восстановление секрета
1	Шамира	$O(n' \times n)$	$O(n'^2)$
2	На эллиптической кривой	$O(n' \times n)$	$O(n'^2)$
3	Блэкли	$O(n' \times n)$	$O(n'^3)$
4	Карнин-Грин-Хеллмана	$O(n)$	$O(n'^3)$
5	Асмута-Блума	$O(n)$	$O(n'^2)$

Пример реализации пороговой схемы разделения секрета Шамира в беспроводных сетях представлен в работах [44, 55, 131, 132, 150, 163, 174].

Сообщение M делится на n частей, количество которых равно количеству независимых маршрутов между узлом-источником (УИ) и узлом-получателем (УП) сообщения. Выбирается некоторое простое число $p > M$. Формируется многочлен степени $(n'-1)$:

$$F(x) = \left(a_{n'-1} \cdot x^{n'-1} + a_{n'-2} \cdot x^{n'-2} + \ldots + a_1 \cdot x + M\right) \bmod p, \qquad (1.2)$$

где $n' \le n$ – ожидаемое минимальное количество частей секретного сообщения M, которые будут приняты по независимым маршрутам в УП. В этом многочлене:

M – разделяемое сообщение;

$a_{n'-1}, a_{n'-2}, \ldots, a_1$ – некоторые случайные числа.

Вычисляются n секретных сообщений:

$$y_1 = F(1) = \left(a_{n'-1} \cdot 1^{n'-1} + a_{n'-2} \cdot 1^{n'-2} + \ldots + a_1 \cdot 1 + M\right) \bmod p;$$
$$y_2 = F(2) = \left(a_{n'-1} \cdot 2^{n'-1} + a_{n'-2} \cdot 2^{n'-2} + \ldots + a_1 2 + M\right) \bmod p;$$
$$\vdots$$
$$y_i = F(i) = \left(a_{n'-1} \cdot i^{n'-1} + a_{n'-2} \cdot i^{n'-2} + \ldots + a_1 \cdot i + M\right) \bmod p;$$
$$\vdots$$
$$y_n = F(n) = \left(a_{n'-1} \cdot n^{n'-1} + a_{n'-2} \cdot n^{n'-2} + \ldots + a_1 \cdot n + M\right) \bmod p,$$

которые вместе с p будут переданы по n независимым маршрутам.

В УП принятые части секретного сообщения $y_i; i = \overline{1, n'}$, и p позволяют полностью восстановить исходный многочлен (1.2) (в том числе и исходное сообщение M) путем решения системы из $n' \le n$ уравнений.

В результате обеспечивается конфиденциальность информации. Использование многопутевой маршрутизации позволяет увеличить пропускную способность сети, уменьшить риск перегрузок сети, что положительно влияет на QoS приложений МСС [43, 44, 54, 55].

Кроме того, пользователи не должны иметь дополнительное специальное криптографическое программно-аппаратное обеспечение и обладать определенными знаниями в области защиты информации.

Однако данный подход чувствителен к модификации частей секретного сообщения. Действительно, если количество неискаженных частей секретного сообщения будет меньше n', то сообщение M не будет восстановлено в УП.

Кроме того, для реализации данного подхода на сети необходимо организовать как минимум три независимых маршрута между УИ и УП. Причем желательно, чтобы эти маршруты были максимально разнесены территориально и обладали одинаковыми вероятностно-временными характеристиками (ВВХ) (скорость передачи информации, время задержки, временной джиттер, вероятность ошибочного приема на пакет, символ и так далее). В противном случае передаваемое сообщение в точке приема не будет восстановлено, либо восстановлено с задержкой во времени, что может оказаться критичным для высокоскоростных приложений, функционирующих в реальном масштабе времени.

Достоинства и недостатки основных подходов, обеспечивающих конфиденциальность информации, приведены в таблице 1.2.

В результате можно сделать следующие выводы [67, 77, 78].

1. «Гибридная» система шифрования (асимметричные алгоритмы используются для организации закрытого канала связи, а симметричные непосредственно для шифрования информации) является вполне приемлемой в мультисервисных сетях связи. Так как для пользователей имеется возможность воспользоваться высокоскоростными приложениями, функционирующими в реальном масштабе времени, с обеспечением конфиденциальности.

2. Недостатки «гибридной» системы шифрования:

– пользователи должны обладать знаниями в области защиты информации;

– иметь в своем распоряжении специальное криптографическое программно-аппаратное обеспечение.

Таблица 1.2 – Результаты анализа основных подходов, обеспечивающих конфиденциальность информации

<table>
<tr><th>№ п/п</th><th>Способ обеспечения конфиденциальности</th><th>Достоинства</th><th colspan="2">Недостатки</th></tr>
<tr><td>1</td><td>Симметричная система шифрования</td><td>Высокая скорость шифрования
$t_{ш} = A \cdot L_k + B$</td><td>Наличие закрытого канала связи</td><td rowspan="3">Пользователи должны иметь дополнительное специальное криптографическое программно-аппаратное обеспечение</td></tr>
<tr><td>2</td><td>Асимметричная система шифрования</td><td>Отсутствие закрытого канала связи</td><td>Низкая скорость шифрования
$t_{ш} = A \cdot L_k^c + B$</td></tr>
<tr><td>3</td><td>«Гибридная» система шифрования</td><td>1. Отсутствие закрытого канала связи.
2. Высокая скорость шифрования:
$t_{ш} = A \cdot L_k + B$
3. Обеспечивается QoS приложений пользователя.</td><td></td></tr>
<tr><td>4</td><td>Многопутевая маршрутизация с пороговой схемой разделения сообщения</td><td>1. Пользователи не должны иметь дополнительное специальное криптографическое программно-аппаратное обеспечение.
2. Обеспечивается QoS приложений МСС.</td><td colspan="2">1. Чувствительность к модификации частей секретного сообщения.
2. Необходимость реализации независимых маршрутов с одинаковыми вероятностно-временными характеристиками.</td></tr>
</table>

3. Метод многопутевой маршрутизации с пороговой схемой разделения сообщения позволяет обеспечить конфиденциальность информации, увеличить пропускную способность сети, уменьшить риск перегрузок сети, что положительно влияет на QoS приложений мультисервисных сетей связи.

4. Недостатком использования метода многопутевой маршрутизации с пороговой схемой разделения сообщения является чувствительность к модификации частей секретного сообщения и необходимость организации

независимых маршрутов, обладающих одинаковыми вероятностно-временными характеристиками (скорость передачи информации, время задержки, временной джиттер, вероятность ошибочного приема на пакет, символ и так далее).

1.3 Анализ основных подходов по обеспечению целостности и доступности информации

На рисунке 1.2 приведены основные подходы, обеспечивающие целостность информации – криптографические методы с дублированием информации и методы, использующие резервирование информации.

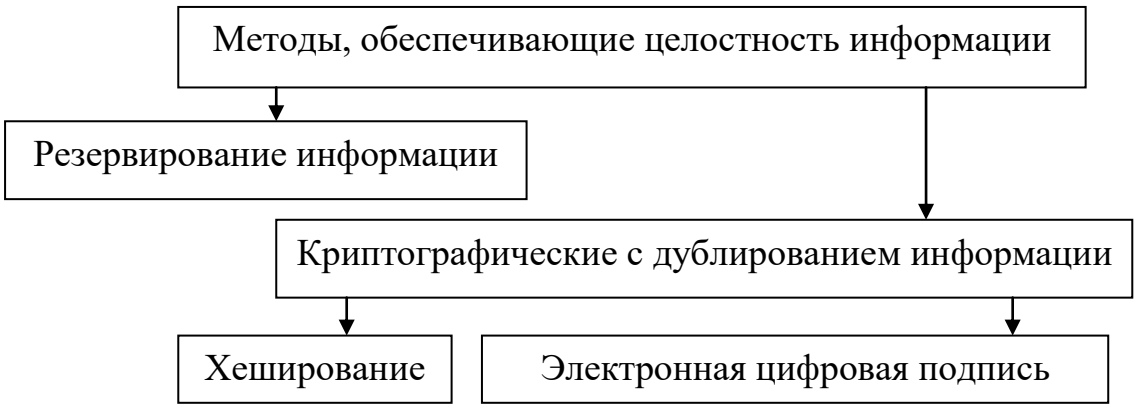


Рисунок 1.2 – Основные методы, обеспечивающие целостность информации в ТКС

Криптографический метод (хеширование, электронная цифровая подпись) [53, 66, 110, 114, 123] подразумевает введение в передаваемое сообщение избыточности – проверочной комбинации, которая вычисляется по определенным алгоритмам и является «индикатором» нарушения целостности информации.

В результате можно сделать вывод, что криптографический метод только контролирует целостность информации. В случае ее модификации источнику необходимо сделать повторную передачу сообщения. Данная процедура будет повторяться до тех пор, пока целостность информации не будет обеспечена. В этом случае между удаленными пользователями необходимо организовать канал обратной связи [60, 127, 129] и канал для повторной передачи сообщения, то есть

выполнить многократное дублирование информации, что значительно влияет на время задержки.

Таким образом, применение в МСС криптографического метода с дублированием информации с целью обеспечения целостности ограниченно для высокоскоростных приложений, функционирующих в реальном масштабе времени.

Метод резервирования информации для обеспечения целостности подразумевает одновременную параллельную передачу информации по нескольким маршрутам и принятия решения о целостности информации на приемной стороне [83]. Тем самым уменьшается время задержки передачи информации и обеспечивается QoS высокоскоростных приложений, функционирующих в реальном масштабе времени.

Основными методами обеспечения доступности информации являются:

– дублирование информации, к которой осуществляется доступ;
– резервирование каналов связи (КС).

Таким образом, обеспечение доступности информации сводятся к задачам обеспечения живучести и надежности сетей связи [11, 15, 37, 95, 126].

1.4 Выводы

Анализ основных подходов по обеспечению базовых параметров защиты информации (целостность, доступность и конфиденциальность) в мультисервисных сетях связи выявил следующие проблемы.

1. Для обеспечения конфиденциальности, доступности и целостности информации пользователи мультисервисной сети связи должны иметь в своем распоряжении специализированное актуальное (постоянно обновляемое) программно-аппаратное обеспечение и обладать знаниями в области защиты информации.

2. Применение основных подходов защиты информации в мультисервисных сетях связи ограничено. Это связано с увеличением времени

задержки передачи информации, что является критичным для приложений мультисервисной сети, функционирующих на больших скоростях и в реальном масштабе времени.

Перечисленные проблемы решаются за счет привлечения ресурсов мультисервисной сети связи (криптографических, канальных и других) под каждую заявку пользователей для передачи защищенной информации.

В этой связи возникает необходимость в разработке, исследовании новых методик, методов, способов и алгоритмов (*методологии*), позволяющих решать задачи обеспечения базовых параметров защиты информации (целостность, доступность и конфиденциальность) с поддержкой QoS приложений мультисервисной сети связи.

2 Разработка методов защиты информации с использованием ресурсов мультисервисных сетей связи

2.1 Исследование возможности использования многократного асимметричного шифрования

В асимметричных криптосистемах с открытым ключом отсутствует закрытый канал связи, что значительно упрощает проблему разовых сеансовых секретных ключей. Однако такие алгоритмы имеют особенности. Во-первых, для достижения аналогичной криптостойкости с симметричными алгоритмами шифрования требуется более длинный ключ. В таблице 2.1 приведены значения длин «…симметричных и открытых ключей с аналогичной устойчивостью к вскрытию грубой силой» [123].

Таблица 2.1 – Соответствие криптостойкости алгоритмов шифрования

Алгоритмы	Длины ключей				
Симметричные	56	64	80	112	128
Асимметричные	384	512	768	1792	2304

Во-вторых, зависимость времени шифрования от длины ключа L_k имеет нелинейный характер (1.1).

Оба фактора значительно ограничивают применение асимметричных криптосистем в МСС. Это связано с тем, что увеличение длины ключа до критичного значения $L_{k\,\text{кр}}$ приведет к недопустимому увеличению времени задержки на шифрование ($t_{\text{ш}}$) информации (рисунок 2.1), что скажется на снижении QoS высокоскоростных приложений, функционирующих в реальном масштабе времени.

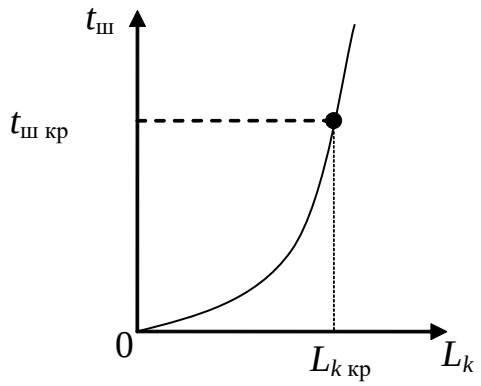


Рисунок 2.1 – Зависимость времени на шифрование от длины ключа

Вместе с тем многократное асимметричное шифрование с ключами меньшей длины позволяет решить перечисленные проблемы [4, 67, 72, 77, 78, 82]. Рисунок 2.2 демонстрирует данный подход.

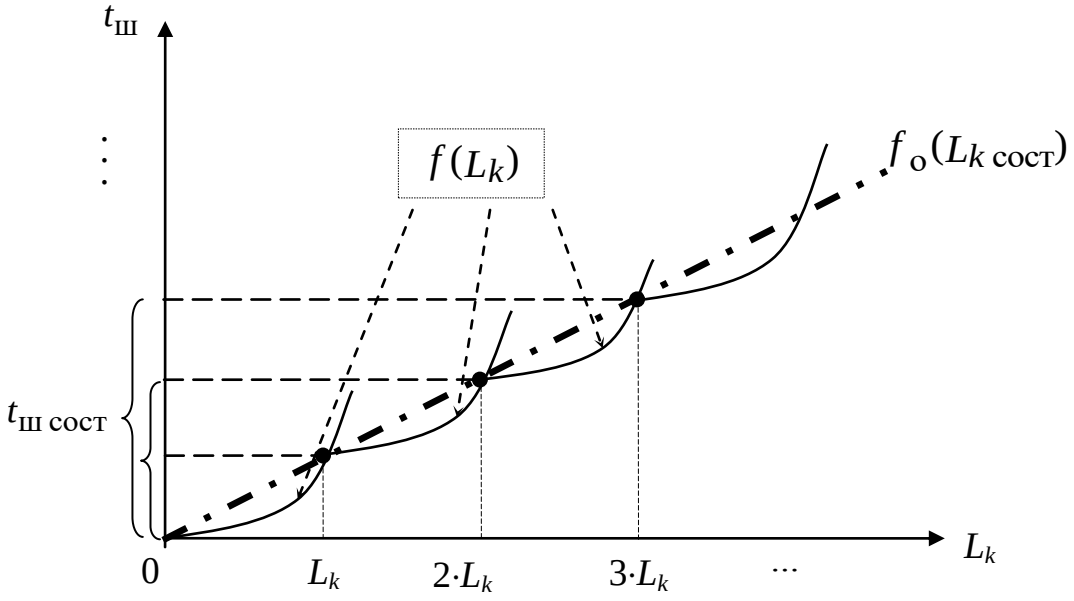


Рисунок 2.2 – Зависимости времени шифрования
от длины составного ключа

Отметим, что многократное шифрование широко используется в симметричных криптографических алгоритмах [53, 109, 114, 117, 119, 123, 124, 135, 184] с целью унификации зашифрования/расшифрования и увеличения длины секретного ключа.

Введем следующие обозначения:

$$y = E_{k^{(о)}}(M),\ M = D_{k^{(с)}}(y)$$

– соответственно функции зашифрования информации M с использованием открытого ключа $k^{(\text{о})}$ и расшифрования закрытой информации y с помощью секретного ключа $k^{(\text{с})}$.

В этом случае процедуры многократного зашифрования и расшифрования соответственно можно записать следующим образом:

$$y = E_{k_l^{(\text{о})}}\{..E_{k_i^{(\text{о})}}...[E_{k_1^{(\text{о})}}(M)]\};$$
$$M = D_{k_1^{(\text{с})}}\{..D_{k_i^{(\text{с})}}...[D_{k_l^{(\text{с})}}(y)]\}, \qquad (2.1)$$

где $k_l^{(\text{о})}$, $k_l^{(\text{с})}; i = \overline{1,l}$ – независимые ключи зашифрования и расшифрования соответственно.

Допустим, что длины всех открытых и секретных ключей одинаковы и равны между собой, т.е.:

$$L_{k_i^{(\text{о})}} = L_{k_i^{(\text{с})}} = L_k; i = \overline{1,l},$$

тогда общая длина составного ключа многократного шифрования определяется выражением:

$$L_{k\,\text{сост}} = \sum_{i=1}^{l} L_{k_i}; \; L_{k_i} = \text{const}.$$

В данном случае время шифрования с учетом (1.1) (рисунок 2.2) составит:

$$t_{\text{ш сост}} = l \cdot (A \cdot \frac{L_{k\,\text{сост}}}{l})^c + B = \frac{A^c \cdot L_{k\,\text{сост}}^c}{l^{c-1}} + B. \qquad (2.2)$$

Функция $t_{\text{ш}} = f(L_{k\,\text{сост}})$ (рисунок 2.2) представляет собой сложную кривую, состоящую из участков функциональных зависимостей:

$$t_{\text{ш}} = f(L_{k\,\text{сост}}) = f\{f(L_k);...;\, f(L_k);...\}.$$

Заменим функцию $t_{\text{ш}} = f(L_{k\,\text{сост}})$ на линейную ($f_{\text{о}}(L_{k\,\text{сост}})$), так как соответствующие первые производные равны.

Учитывая (2.2), характер $f_{\text{о}}(L_{k\,\text{сост}})$ и взяв отношение $t_{\text{ш}}$ к $t_{\text{ш сост}}$, получим относительный временной выигрыш от применения «составного» ключа по отношению к шифрованию одним «длинным» ключом (при $B = 0$):

$$\frac{t_{\text{ш}}}{t_{\text{ш сост}}} = \frac{A \cdot L_{k\,\text{сост}}^{c} + B}{l \cdot \left(A \cdot \left(\frac{L_{k\,\text{сост}}}{l} \right)^{c} + B \right)} = \frac{A \cdot L_{k\,\text{сост}}^{c}}{l \cdot A \cdot \left(\frac{L_{k\,\text{сост}}}{l} \right)^{c}} = l^{c-1}. \qquad (2.3)$$

На рисунке 2.3 представлены результаты натурного эксперимента [77] шифрования алгоритмом *RSA* блока данных объемом 1 кБ при изменении длины ключа от 256 бит до 2048 бит и использовании составного 256-битного ключа (многократное асимметричное шифрование).

Результаты натурного эксперимента подтвердили теоретическое предположение (2.3).

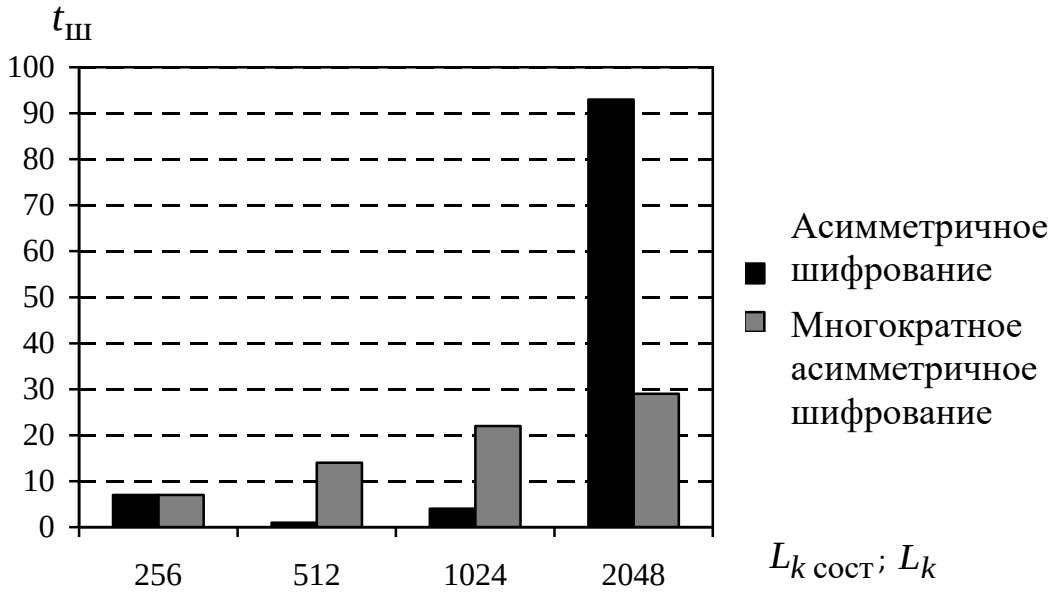


Рисунок 2.3 – Сравнение времени при асимметричном шифровании и при многократном асимметричном шифровании

2.2 Разработка метода обеспечения целостности информации на сетевом уровне мультисервисных сетей связи

Реализация параллельной передачи и обработки информации в точке приема является одним из эффективных методов, обеспечивающих надежность вычислительных и телекоммуникационных систем [8, 11, 91, 104, 116, 120]. Применим данный подход для обеспечения целостности информации с поддержанием показателей QoS высокоскоростных приложений МСС, функционирующих в реальном масштабе времени.

Пусть в МСС между УИ и УП передается сообщение, представляющее собой битовый поток $M = \{M_1, M_2\}$ с соответствующими априорными вероятностями $P(M_1)$ и $P(M_2)$.

Сообщение передается от УИ к УП по *n* параллельным соединениям через *m* транзитных узлов (ТУ) в каждом соединении (рисунок 2.4).

Пусть $P_{\text{м}}^{(i)}$ – вероятность модификации сообщения $M=\{M_1, M_2\}$ вследствие атаки нарушителя в соответствующем *i*-ом соединении ($i=\overline{1,n}$).

В данном случае целостность информации достигается за счет принятия решения в УП по *n* принятым символам $x=(x_1,...,x_i,...,x_n)$. В результате, значение *M** на выходе решающего устройства (РУ) будет соответствовать переданному значению M_1 или M_2.

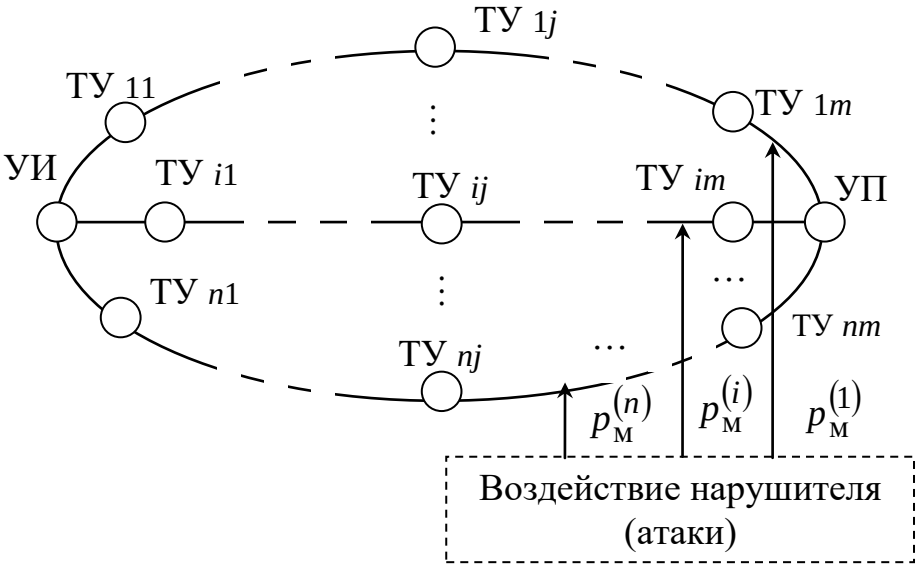


Рисунок 2.4 – Организация параллельных соединений

Условные вероятности принятия решения в пользу M_1 или M_2, соответственно, определяются как:

$$P\left(M_1/\left(x_i; i=\overline{1,n}\right)\right)=\frac{P(M_1)\cdot\left\{\prod\limits_{i:x_i=M_1}\left(1-P_{\text{м}}^{(i)}\right)\cdot\prod\limits_{i:x_i=M_2}P_{\text{м}}^{(i)}\right\}}{P\left(x_i; i=\overline{1,n}\right)};$$

$$P\left(M_2/\left(x_i; i=\overline{1,n}\right)\right)=\frac{P(M_2)\cdot\left\{\prod\limits_{i:x_i=M_1}P_{\text{м}}^{(i)}\cdot\prod\limits_{i:x_i=M_2}\left(1-P_{\text{м}}^{(i)}\right)\right\}}{P\left(x_i; i=\overline{1,n}\right)}.$$

Возьмем отношение этих выражений. Если результат окажется больше 1, то принимаем решение в пользу M_1, в противном случае M_2:

$$\frac{P\left\{M_1/\left(x_i;i=\overline{1,n}\right)\right\}}{P\left\{M_2/\left(x_i;i=\overline{1,n}\right)\right\}}=\frac{P(M_1)}{P(M_2)}\times\frac{\prod_{i:x_i=M_1}\left(1-P_{\text{м}}^{(i)}\right)}{\prod_{i:x_i=M_1}P_{\text{м}}^{(i)}}\times\frac{\prod_{i:x_i=M_2}P_{\text{м}}^{(i)}}{\prod_{i:x_i=M_2}\left(1-P_{\text{м}}^{(i)}\right)}. \quad (2.4)$$

Прологарифмируем выражение (2.4):

$$\ln\frac{P\left\{M_1/\left(x_i;i=\overline{1,n}\right)\right\}}{P\left\{M_2/\left(x_i;i=\overline{1,n}\right)\right\}}=\ln\frac{P(M_1)}{P(M_2)}+\sum_{i:x_i=M_1}\ln\frac{\left(1-P_{\text{м}}^{(i)}\right)}{P_{\text{м}}^{(i)}}+\sum_{i:x_i=M_2}\ln\frac{P_{\text{м}}^{(i)}}{\left(1-P_{\text{м}}^{(i)}\right)}. \quad (2.5)$$

Обозначим:

$$a_0=\ln\frac{P(M_1)}{P(M_2)};\ a_i=\ln\frac{\left(1-P_{\text{м}}^{(i)}\right)}{P_{\text{м}}^{(i)}}. \quad (2.6)$$

В результате получим:

$$\ln\frac{P\left\{M_1/\left(x_i;i=\overline{1,n}\right)\right\}}{P\left\{M_2/\left(x_i;i=\overline{1,n}\right)\right\}}=a_0+\sum_{i=1}^{n}x_i\cdot a_i. \quad (2.7)$$

Таким образом, имеет место следующее правило принятия решения [2, 83, 108]:

$$a_0+\sum_{i=1}^{n}x_i\cdot a_i\begin{cases}\text{если}>0\Rightarrow M^*=M_1;\\ \text{если}<0\Rightarrow M^*=M_2.\end{cases} \quad (2.8)$$

Функциональная схема РУ приведена на рисунке 2.5.

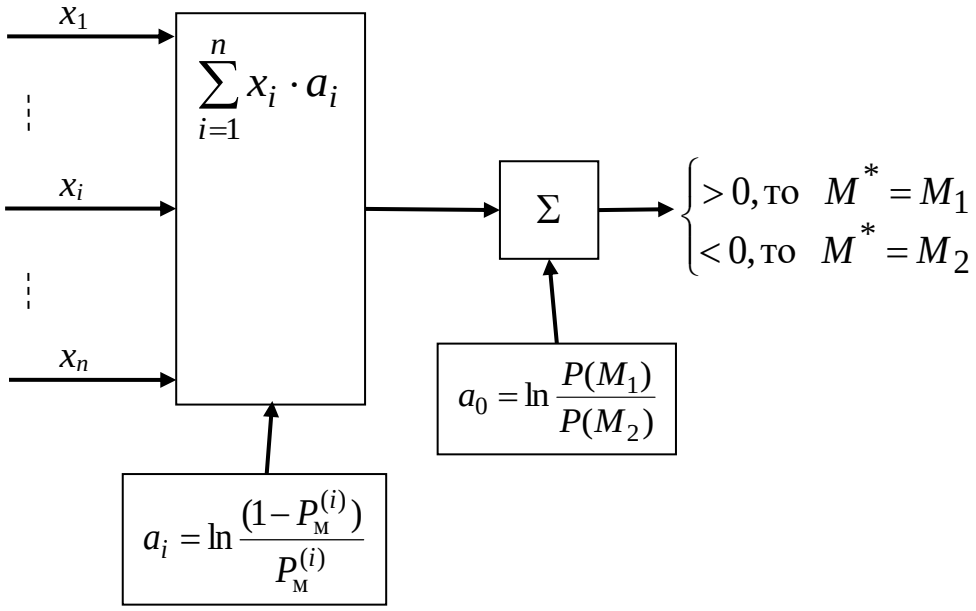


Рисунок 2.5 – Функциональная схема РУ

2.2.1 Оценка вероятности целостности информации

Введем следующие ограничения:

– вероятности модификации $M = \{M_1, M_2\}$ по всем соединениям между УИ и УП равны, т.е. $P_{\text{м}} = P_{\text{м}}^{(i)}; i = \overline{1,n}$ (рисунок 2.4) и независимы;

– количество параллельных соединений n между УИ и УП нечетно и $n \geq 3$.

Тогда вероятность целостности информации (рисунок 2.5) определяется выражением [2, 67, 107]:

$$P_{\text{ц РУ}} = 1 - \sum_{i=0}^{(n-1)/2} C_n^{(n+1+2\cdot i)/2} \cdot (1 - P_{\text{м}})^{(n-1-2\cdot i)/2} \cdot P_{\text{м}}^{(n+1+2\cdot i)/2}, \qquad (2.9)$$

где $C_n^{(n+1+2\cdot i)/2}$ – число сочетаний $(n+1+2\cdot i)/2$ из n.

На рисунке 2.6. приведены результаты оценки целостности информации, рассчитанные по формуле (2.9).

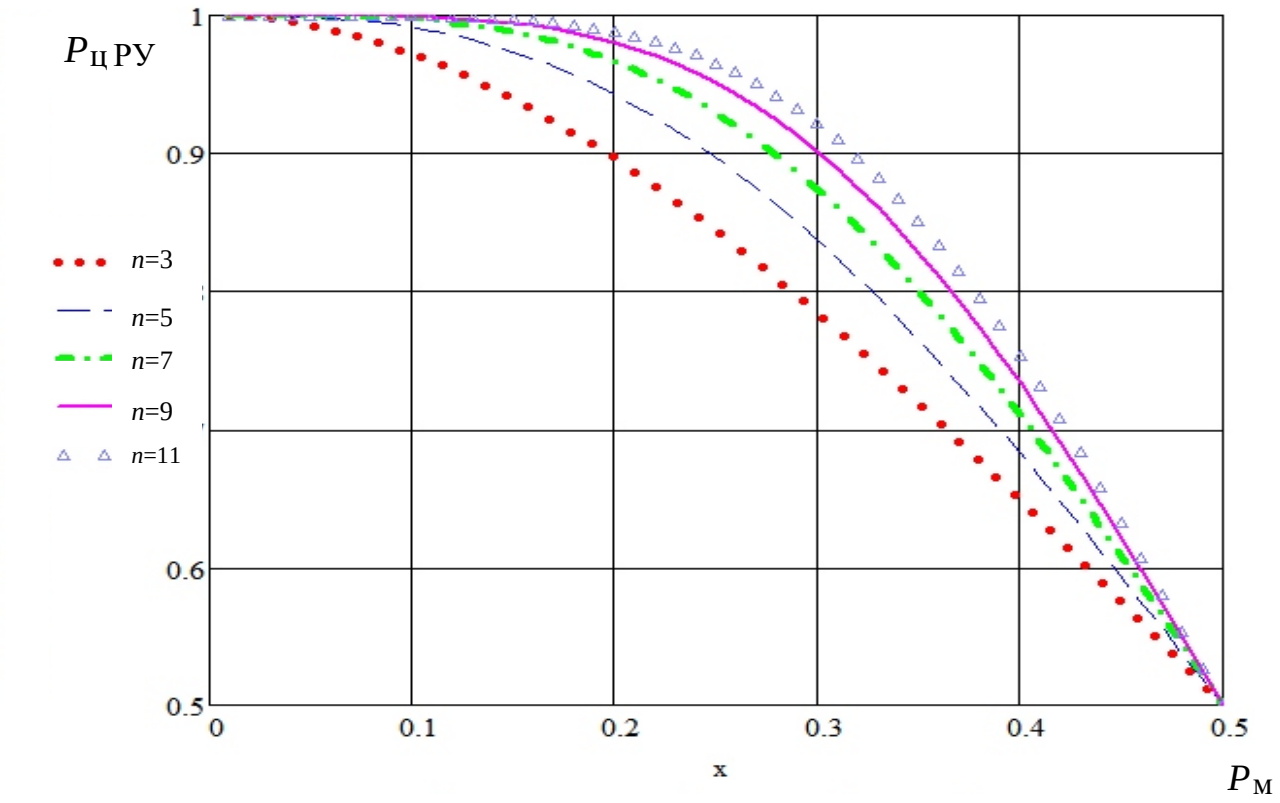


Рисунок 2.6 – Результаты теоретического расчета $P_{\text{Ц РУ}} = f(P_{\text{М}})$ для различных значений n

2.2.2 Имитационное моделирование обеспечения целостности информации на сетевом уровне мультисервисных сетей связи

Апробация функционирования РУ (рисунок 2.5), реализующего алгоритм (2.8), на действующей сети связи сопряжена с финансовыми, организационными и временными затратами. В этой связи для подтверждения теоретических результатов оценки вероятности целостности информации на выходе РУ воспользуемся методом статистического моделирования [13], суть которого сводится к следующему (рисунок 2.7) [107].

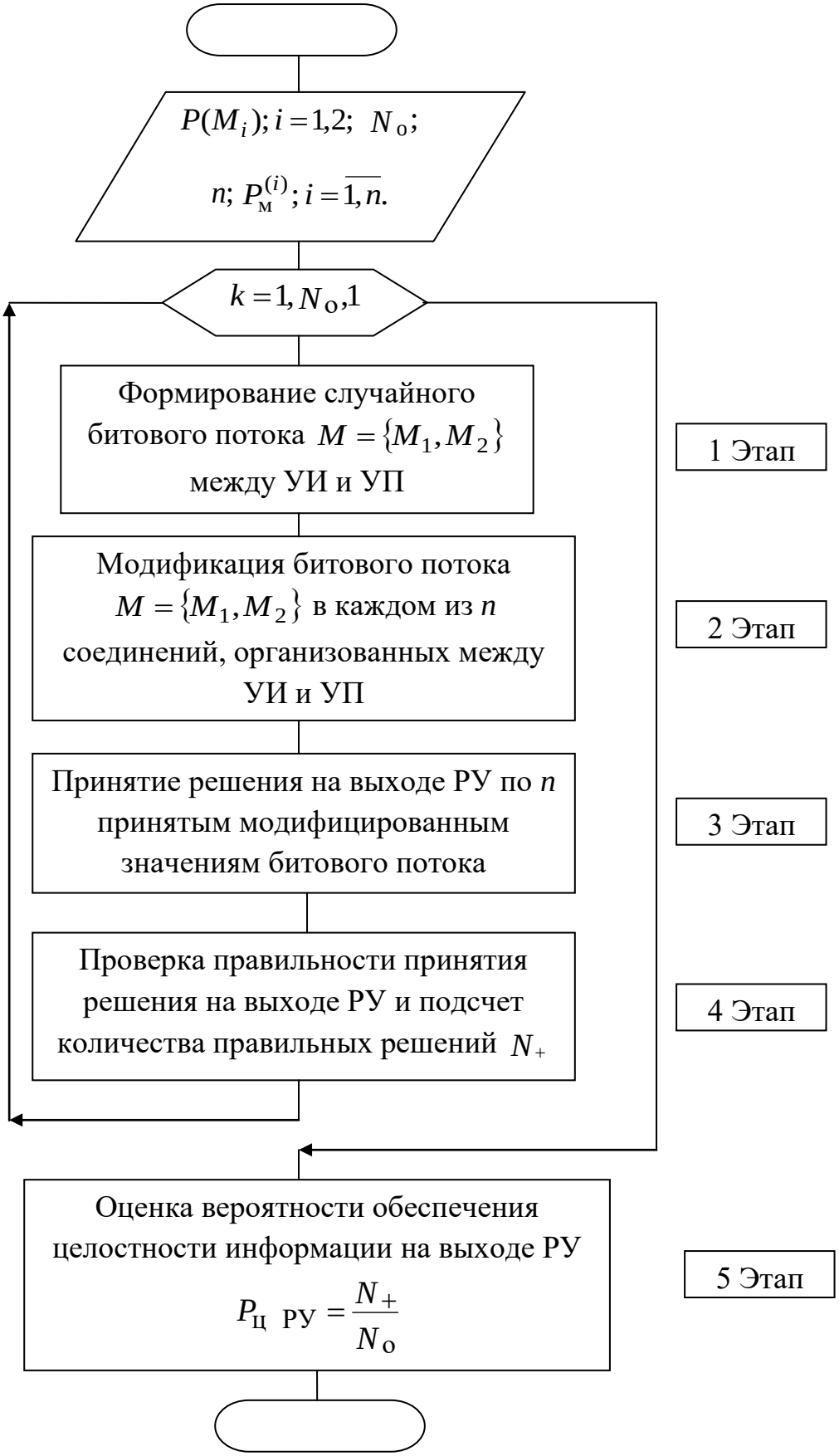


Рисунок 2.7 – Основные этапы оценки целостности информации на выходе РУ методом статистического моделирования

Исходными данными алгоритма моделирования являются:

$P(M_1); P(M_2)$ – априорные вероятности появления $M = \{M_1, M_2\}$ на выходе УИ, при условии $P(M_1) + P(M_2) = 1$;

n – количество соединений между УИ и УП;

$P_{\text{м}}^{(i)}; i = \overline{1,n}$ – вероятности модификации битового потока $M = \{M_1, M_2\}$ в каждом из n соединений между УИ и УП;

$N_{\text{о}}$ – количество переданных значений $M = \{M_1, M_2\}$ между УИ и УП (количество независимых испытаний при статистическом моделировании).

Осуществляют $N_{\text{о}}$ независимых испытаний, каждое из которых состоит из четырех этапов. На первом этапе формируется случайный битовый поток $M = \{M_1, M_2\}$ по правилу:

$$M = \begin{cases} +1, & \text{если } z_k \le P(M_1); \\ -1, & \text{если } z_k > P(M_1), \end{cases}$$

где z_k – случайное число, генерируемое датчиком случайных чисел с равномерным законом распределения ($0 \le z_k \le 1$; $k = \overline{1, N_{\text{о}}}$).

Второй этап посвящен модификации значений $M = \{M_1, M_2\}$ в каждом из n установленных параллельных соединений между УИ и УП:

$$x_i = \begin{cases} \text{если } z_k \le P_{\text{м}}, \text{ то модификация есть, } x_i = M \times (-1) \\ \text{если } z_k > P_{\text{м}}, \text{ то модификации нет, } x_i = M. \end{cases}$$

Третий этап – расчет коэффициентов по формулам (2.6) и принятие решения по правилу (2.8).

На четвертом этапе проверяется правильность принятия решения по правилу (2.8) и подсчет N_+ – количества правильно принятых значений $M = \{M_1, M_2\}$ из $N_{\text{о}}$ переданных.

На пятом этапе определяется оценка вероятности целостности информации на выходе РУ:

$$P_{\text{Ц РУ}} = \frac{N_+}{N_\text{о}}.$$

Метод статистического моделирования является приближенным. Погрешность результата вычисления имеет статистическую природу. Количественная взаимосвязь между абсолютной погрешностью и числом испытаний $N_\text{о}$ определяется следующей формулой [13, стр. 95]:

$$\Delta_\text{а} = N_\text{о}^{-0,5} \cdot \sigma \cdot t_\beta, \qquad (2.10)$$

где

$\Delta_\text{а}$ – абсолютное значение ошибки (половина доверительного интервала);

$P_{\text{Ц РУ}}, \sigma$ – значение искомой величины и среднеквадратичное отклонение от $P_{\text{Ц РУ}}$;

дисперсия искомой величины определяется выражением:

$$\sigma^2 = P_{\text{Ц РУ}} \cdot (1 - P_{\text{Ц РУ}});$$

β – достоверность полученной оценки;

t_β – функция, обратная нормальной при аргументе $(1+\beta)^{-1}$, находится по таблице (например, [13]).

В практике статистического моделирования задача формулируется иначе, а именно: сколько необходимо провести испытаний, чтобы обеспечить заданную абсолютную или относительную погрешность вычисления. Тогда из (2.10) легко получить искомую величину:

$$N_{\text{о}} = t_{\beta}^{2} \cdot \sigma^{2} \cdot \Delta_{\text{а}}^{-2}. \qquad (2.11)$$

В формулу входят значения $P_{\text{ц РУ}}$ и σ в качестве точных значений. Но поскольку само $P_{\text{ц РУ}}$ является предметом измерения и может быть получено лишь приближенно, то погрешность $\Delta_{\text{а}}$ по результатам опыта не может быть получена точно.

Оценку получают экспериментально путем проведения небольшого количества предварительных испытаний ($N_{\text{о предв.}} \approx 5 \div 20$).

В качестве $P_{\text{ц РУ}}$ и σ берут величины:

$$\hat{P}_{\text{ц РУ}} = N_{\text{о предв.}}^{-1} \cdot \sum_{i=1}^{N_{\text{о предв.}}} y_i; \;\; \hat{\sigma} = N_{\text{о предв.}}^{-1} \cdot \sum_{i=1}^{N_{\text{о предв.}}} (y_i - \hat{P}_{\text{ц РУ}}),$$

где y_i – значения, которые принимает измеряемая случайная величина. Затем эти оценки учитываются в формуле (2.11) для расчета требуемого количества испытаний $N_{\text{о}}$.

Результаты оценки целостности информации на выходе РУ (рисунок 2.5) методом статистического моделирования (рисунок 2.7) (программная реализация выполнена в среде MatLab) представлены на рисунке 2.8 [107]. Данные результаты получены при условиях $N_{\text{о}} = 30000$, $\beta = 0{,}999$ и $t_{\beta} = 3{,}29$, что при $P_{\text{ц РУ}} = 0{,}5$ обеспечивает абсолютную погрешность $\Delta_{\text{а}} \le 0{,}01$.

Результаты имитационного моделирования подтверждают теоретические расчеты по формуле (2.9).

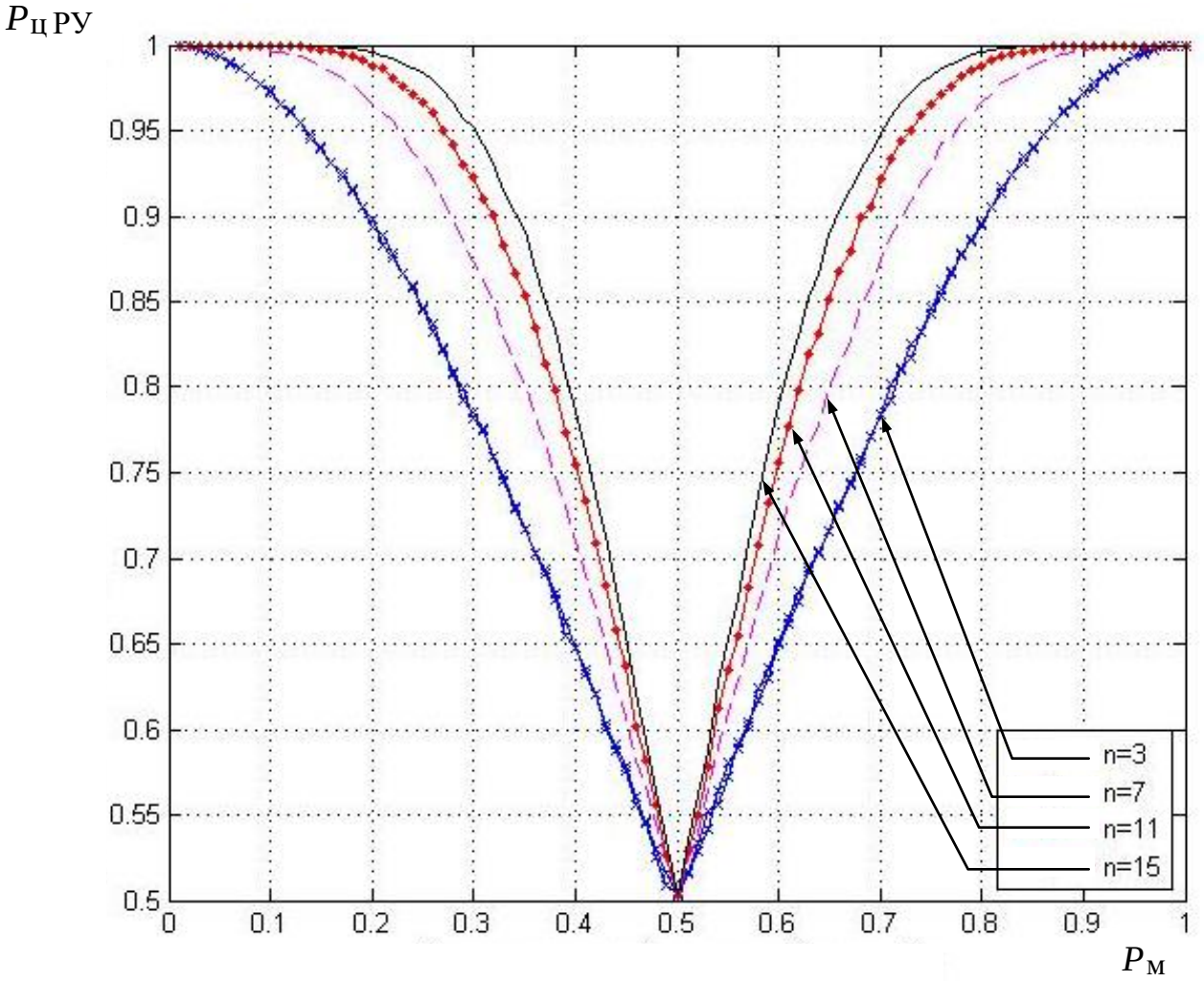


Рисунок 2.8 – Результаты имитационного моделирования работы РУ $P_{\text{ц РУ}} = f(P_{\text{м}})$ для различных значений n

2.3 Разработка критерия выбора ресурсов мультисервисных сетей связи для обеспечения целостности и доступности информации

Резервирование каналов связи и дублирование самой информации являются базовыми методами обеспечения доступности информации ТКС [8, 11, 91, 104, 116, 120]. Применительно к МСС данный подход реализуется за счет организации параллельных соединений между УИ и УП (рисунок 2.4). В данном случае необходимо определить критерий выбора соединений между УИ и УП, обеспечивающий требуемый уровень доступности либо целостности пользовательской информации [3, 67].

Введем следующие обозначения. Пусть: c_i – стоимость *i*-ого соединения между УИ и УП (рисунок 2.4), участвующего в обеспечении доступности либо целостности информации; p_i – вероятность обеспечения доступности либо целостности *i*-ого соединения ($i = \overline{1,n}$).

Тогда общая стоимость организации *n* параллельных соединений составит:

$$C_{\text{о}} = \sum_{i=1}^{n} c_i \,. \tag{2.12}$$

Пусть воздействия нарушителей на каждое соединение являются независимыми событиями. В этом случае результирующую (общую) вероятность обеспечения доступности либо целостности информации можно определить:

$$P_{\text{рез}} = 1 - \prod_{i=1}^{n} (1 - p_i). \tag{2.13}$$

Введем обозначения:

$$Q_{\text{рез}} = 1 - P_{\text{рез}}; q_i = 1 - p_i; i = \overline{1,n}.$$

Предположем, что все *n* соединений (рисунок 2.4) одинаковы по стоимости и вероятности обеспечения доступности либо целостности информации.

Тогда:

$$C_{\text{о}} = n \cdot c_i; i = \overline{1,n}; \tag{2.14}$$

$$Q_{\text{рез}} = q_i^n; i = \overline{1,n}. \tag{2.15}$$

Прологарифмируем выражение (2.15):

$$\ln Q_{\text{рез}} = n \cdot \ln q_i ; i = \overline{1,n}$$

и разделим на (2.14). В результате получим:

$$\frac{\ln Q_{\text{рез}}}{C_{\text{о}}} = \frac{\ln q_i}{c_i} ; i = \overline{1,n}.$$

Учитывая, что

$$\frac{\ln Q_{\text{рез}}}{C_{\text{о}}} = \frac{\ln q_i}{c_i} \le 0; i = \overline{1,n},$$

то примем:

$$\left| \frac{\ln Q_{\text{рез}}}{C_{\text{о}}} \right| = \left| \frac{\ln q_i}{c_i} \right| ; i = \overline{1,n}. \qquad (2.16)$$

Из (2.16) следует вывод. Для обеспечения доступности либо целостности информации за счет организации n параллельных независимых соединений между УИ и УП необходимо выбирать те соединения, у которых отношение

При организации n параллельных соединений между УИ и УП необходимо выбирать те маршруты, у которых:

$$\max \left\{ \alpha_i = \left| \frac{\ln(1 - p_i)}{c_i} \right| ; i = \overline{1,n} \right\}. \qquad (2.17)$$

2.4 Выводы

1. Многократное асимметричное шифрование ключами меньшей длины обеспечивает конфиденциальность информации при меньшем времени ее шифрования.

2. Параллельные соединения между узлом-источником и узлом-получателем, учитывающие вероятностно-стоимостные параметры, позволяют по совокупности параллельно принятых символов восстановить переданную информацию, тем самым обеспечить ее целостность и уменьшить время задержки передачи информации (по сравнению с известными методами, использующих контроль модификации переданной информации и запрос на ее повторную передачу).

3. Формирование параллельных независимых соединений в соответствии с критерием выбора сетевых ресурсов (2.17), учитывающим вероятностно-стоимостные параметры соединений, обеспечивает доступность и целостность информации в мультисервисных сетях связи.

4. Применение метода информационного резервирования и резервирования элементов инфраструктуры позволяет обеспечить защиту информации с QoS.

5. Процедуры, участвующие в мониторинге инфраструктуры мультисервисной сети связи, выборе оптимального маршрута и установлении соединений, позволяют обеспечить не только QoS приложений, но и требуемый уровень информационной безопасности.

В этой связи возникает необходимость в разработке, исследовании новых методов маршрутизации, способных решать задачи защиты информации с поддержкой QoS приложений мультисервисной сети связи.

3 Разработка методов маршрутизации в мультисервисных сетях связи

3.1 Термины и определения предметной области «Маршрутизация в сетях связи»

Дадим основные определения, необходимые для дальнейшего изложения материала [10, 47, 80, 121, 128].

Маршрут – список элементов сети связи (линий связи (ЛС), узлов коммутации (УК), каналов связи (КС), трактов передачи сообщений (ТПС)), начинающийся с УИ передаваемой информации и заканчивающийся в УП.

Маршрутизация – набор процедур, позволяющих определить и установить оптимальный по заданным параметрам маршрут на сети связи между УИ и УП.

В МВОС функции маршрутизации возложены на третий – сетевой уровень [179]. Данный уровень удобно представить в виде подуровней (рисунок 3.1) [47]. На втором, верхнем подуровне производится мониторинг состояния сети связи и формирование таблиц маршрутизации (ТМ).

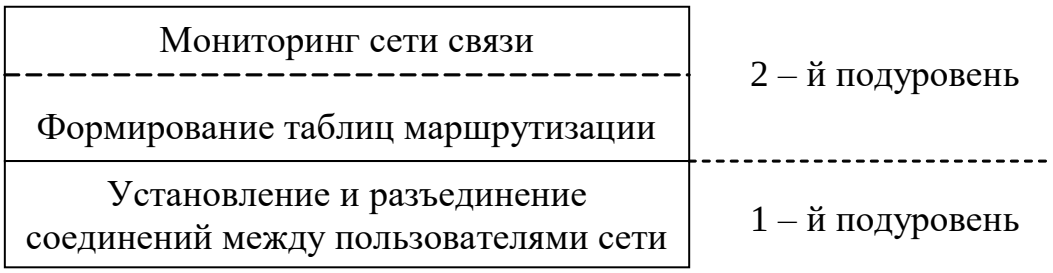


Рисунок 3.1 – Подуровни сетевого уровня модели ВОС

Основная задача мониторинга состоит в определении вероятностно-временных характеристик (ВВХ) элементов сети связи: скорость передачи информации; время задержки передачи информации; надежность и другие. Данная информация является основанием для определения маршрутов с требуемыми ВВХ между всеми УК анализируемой сети связи. Сформированные

маршруты прописываются в ТМ в ранжированном порядке по предпочтительности выбора.

В процессе функционирования сети связи, сформированные ТМ, используются процедурами первого подуровня для установления соединений между пользователями.

Протоколы, участвующие во 2-ом подуровне (формирующие ТМ), принято называть протоколами маршрутизации [47].

Протоколы, выполняющие функции установления и разъединения соединений, обычно называют протоколами сигнализации [47].

В совокупности протоколы 2-го и 1-го подуровней являются служебными протоколами, которые обеспечивают возможность передачи пользовательской информации с требуемым качеством обслуживания.

Заметим, что в системах телекоммуникаций сетевой уровень МВОС может быть реализован в двух вариантах:

– наличие только протоколов маршрутизации (только второй подуровень сетевого уровня МВОС);

– наличие протоколов маршрутизации и сигнализации (второй и первый подуровни сетевого уровня МВОС).

Говорят, что в первом случае в сети связи реализуется технология коммутации пакетов в режиме дейтаграмм. Известно, что данная технология не поддерживает QoS приложений, функционирующих в сетях связи [10, 47, 121].

Во втором случае в сети реализуется технология коммутация пакетов с предварительным установлением соединений, гарантирующая QoS, что является необходимым условием для мультисервисных сетей связи. Поэтому в дальнейшем мы будем анализировать только второй вариант.

Вызывающий пользователь сети через оконечное оборудование инициирует пакет вызова на установление соединения с вызываемым пользователем. Пакет вызова содержит следующую информацию:

– адрес УИ;

– адрес УП;

– приложение МСС (телефония, телевидение, видеоконференция и другие), которое будет участвовать при передаче пользовательской информации (фактически определяются требования к ВВХ передаваемой информации – время задержки, скорость передачи информации, вероятность ошибочного приема на символ и так далее).

Система сигнализации:

– принимает данный пакет вызова;

– обращается к ТМ, которые сформированы на втором подуровне (протоколами маршрутизации) для указанного в пакете вызова приложения;

– выбирает первый в ранжированном списке маршрут – определяет исходящие ТПС и наличие в них свободных каналов с требуемыми ВВХ;

– устанавливает по выбранному маршруту соединение между заданными пользователями (при наличии свободных каналов с требуемыми ВВХ).

В результате информация установленного соединения фиксируется в таблицах коммутации (ТК) соответствующих УК.

Фактически это означает, что МСС выделила требуемые ресурсы (КС, ТПС) для данного вызова и готова для передачи пользовательской информации с требуемым качеством обслуживания выбранного приложения.

Если по каким либо причинам первый в ранжированном списке маршрут не доступен, то выбирается следующий по предпочтительности маршрут. И так до тех пор, пока маршрут не будет реализован в виде соединения между парой пользователей. В противном случае пользователю будет дан отказ в обслуживании.

По завершению передачи сообщения информация в ТК стирается. Это означает, что выделенные ресурсы (КС, ТПС) для передачи пользовательской информации освободились и могут быть использованы сетью связи для передачи другой информации.

Для того, чтобы была возможность определять маршруты между любой парой УК, необходимо построить ТМ в каждом узле сети.

Совокупность ТМ во всех УК сети называется планом распределения информации (ПРИ) на сети связи. Считается, что ПРИ на сети задан, если определены ТМ для каждого УК.

На практике таблицы маршрутизации могут быть реализованы в двух вариантах: пошаговые ТМ; ТМ от источника.

Пошаговая таблица маршрутизации представляет собой матрицу:

$$M^{(j)} = \left\| m_{i,\nu}^{(j)} \right\|_{(S-1),\chi_j} = \left(\overline{m_1^{(j)}}, \ldots, \overline{m_i^{(j)}}, \ldots, \overline{m_{j-1}^{(j)}}, \overline{m_{j+1}^{(j)}}, \ldots, \overline{m_S^{(j)}} \right), \quad (3.1)$$

$$\overline{m_i^{(j)}} = \left(m_{i1}^{(j)}, \ldots, m_{i\nu}^{(j)}, \ldots m_{i\chi_j}^{(j)} \right); \nu = \overline{1, \chi_j}; i, j = \overline{1, S}; i \neq j, \quad (3.2)$$

где S – количество УК в сети; χ_j – количество исходящих ТПС из j-го УК.

Матрица $M^{(j)}$ содержит информацию о предпочтительности выбора исходящего ТПС из j-го УК при поиске маршрута к i-му узлу (УП).

Первый элемент $m_{i1}^{(j)}$ вектор-строки (3.2) указывает номер исходящего ТПС из j-го УК к смежному УК, который предпочтительнее выбрать для организации маршрута к i-му УК (УП).

Второй элемент $m_{i2}^{(j)}$ вектор-строки (3.2) указывает номер следующего исходящего ТПС из j-го УК к другому смежному УК, который менее предпочтительный для организации искомого маршрута к i-му УК. И так до χ_j-го элемента вектор-строки (3.2).

При этом говорят, что $m_{i1}^{(j)}$ является исходящим ТПС первого выбора, $m_{i2}^{(j)}$ – исходящим ТПС второго выбора и, соответственно, $m_{i\chi_j}^{(j)}$ исходящим ТПС χ_j-го выбора.

Таблица маршрутизации от источника представляет собой матрицу:

$$M^{(j)}=\left(\overline{\mu_1^{(j)}},\ldots,\overline{\mu_i^{(j)}},\ldots,\overline{\mu_{j-1}^{(j)}},\overline{\mu_{j+1}^{(j)}},\ldots,\overline{\mu_S^{(j)}}\right); \quad (3.3)$$

$$\overline{\mu_i^{(j)}}=\left(\langle\mu_{i1}^{(j)}\rangle,\ldots,\langle\mu_{i\nu}^{(j)}\rangle,\ldots\langle\mu_{im_j}^{(j)}\rangle\right), i,\ j=\overline{1,S}; i\neq j, \quad (3.4)$$

где S – количество УК в сети;

$\overline{\mu_i^{(j)}}$ – ранжированный по предпочтительности список маршрутов из j-го УИ к i-му УП;

$\left\langle \mu_{i\nu}^{(j)} \right\rangle$ – маршрут (список элементов сети) ν-го по предпочтительности выбора из j–го УИ к i-му УП;

m_j – количество маршрутов в ранжированном списке из j-го УИ к i-му УП.

Первоначально (при проектировании или модификации сети связи) ПРИ формируется администрацией. Однако ВВХ элементов сети (надежность; время задержки передачи информации; скорость передачи информации и другие) являются случайными функциями от времени t и зависят от многих причин:

- вида и интенсивности пользовательского трафика в сети;
- условий окружающей среды при эксплуатации оборудования сети;
- технического состояния оборудования сети;
- вмешательства третьих лиц (нарушителей) в процесс функционирования телекоммуникационной системы

и других причин. Поэтому в процессе эксплуатации сетей связи могут возникнуть ситуации, при которых необходимо скорректировать ТМ и тем самым переформировать ПРИ. Как правило, формирование и коррекция ТМ (действие протоколов маршрутизации) происходит в фиксированные моменты времени t_i с интервалом Δt (рисунок 3.2). Причем Δt может быть как постоянной [134], так и переменной величиной [168]. Однако заявки на установление соединений поступают в сеть связи в произвольные моменты времени. Следовательно, информация в ТМ принципиально не может отражать реальную ситуацию,

сложившуюся на сети в момент установления соединений. Поэтому процедура первого подуровня (действие протоколов сигнализации) предназначена для уточнения выбора маршрута с соответствующими ВВХ и его реализации в виде соединения.

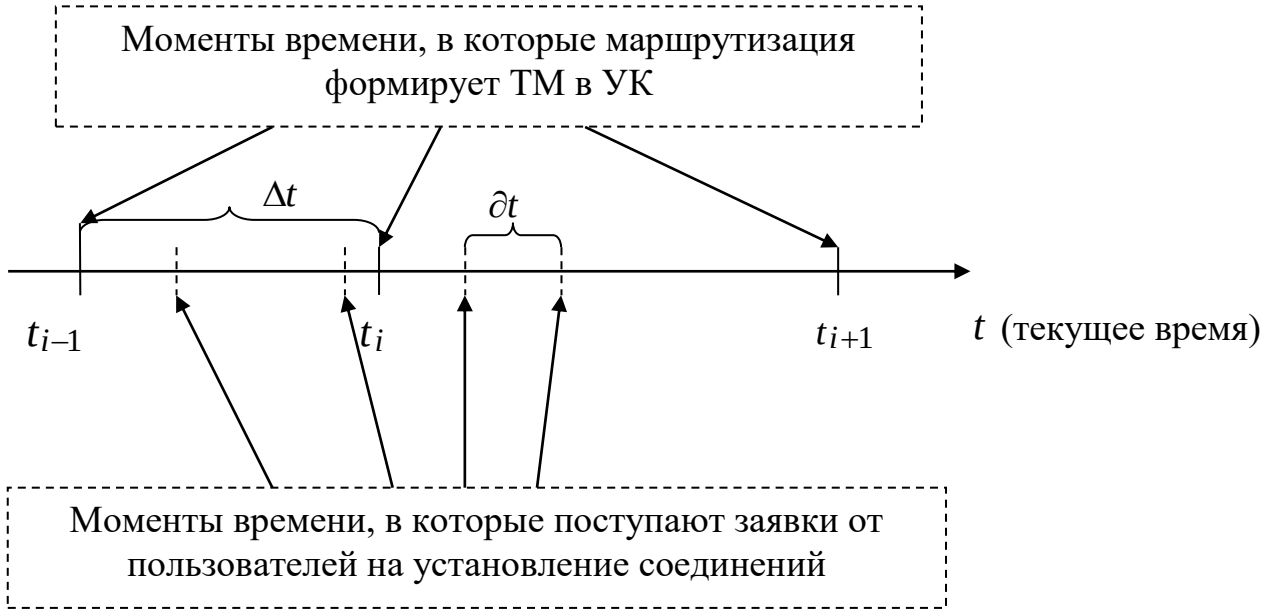


Рисунок 3.2 – Причины несоответствия информации, хранящейся в ТМ, реальной ситуации в сети на момент установления соединения

Если в процессе эксплуатации сетей связи происходит автоматическое переформирование ПРИ (без участия администрации сети), то такой метод формирования ПРИ называют динамическим. В противном случае метод формирования ПРИ будет статическим.

Частота коррекции ПРИ Δt зависит от многих факторов:

– использование статических или динамических методов маршрутизации;

– набора статистики (за определенный период времени T) о состоянии элементов сети связи (ВВХ);

– степени централизации устройств управления сетью связи (централизованные, децентрализованные или комбинированные методы управления);

– возможности администрации сети связи влиять на процесс управления сетью связи;

– наличие постоянных (не коммутируемых) соединений между пользователями сети связи

и других факторов.

3.2 Разработка обобщенной функциональной модели маршрутизации в мультисервисных сетях связи

Анализ вышеизложенного материала позволяет выработать обобщенную функциональную модель маршрутизации в МСС [78, 80, 128], которая изображена на рисунке 3.3.

Обобщенная модель маршрутизации в МСС содержит два уровня:

– уровень формирования ПРИ выполняет функции формирования и коррекции баз данных (БД) о состоянии элементов сети;

– уровень сигнализации выполняет функции выделения и резервирования ресурсов сети для каждой заявки вызовов.

Основным продуктом уровня формирования ПРИ являются ТМ для каждого приложения МСС $\left(\varepsilon = \overline{1,\mathrm{E}}\right)$. При этом применяются соответствующие методы формирования и коррекции баз данных (БД), которые по степени централизации можно классифицировать на централизованные, распределенные и комбинированные.

Уровень сигнализации, используя методы выбора исходящих ТПС, по сформированным ТМ формирует во всех транзитных УК, начиная с УИ:

– таблицы коммутации для каждой заявки на установление соединения с требуемыми ВВХ;

– структуру соединений защиты с целью выполнения требований пользователей к степени защищенности передаваемой информации.

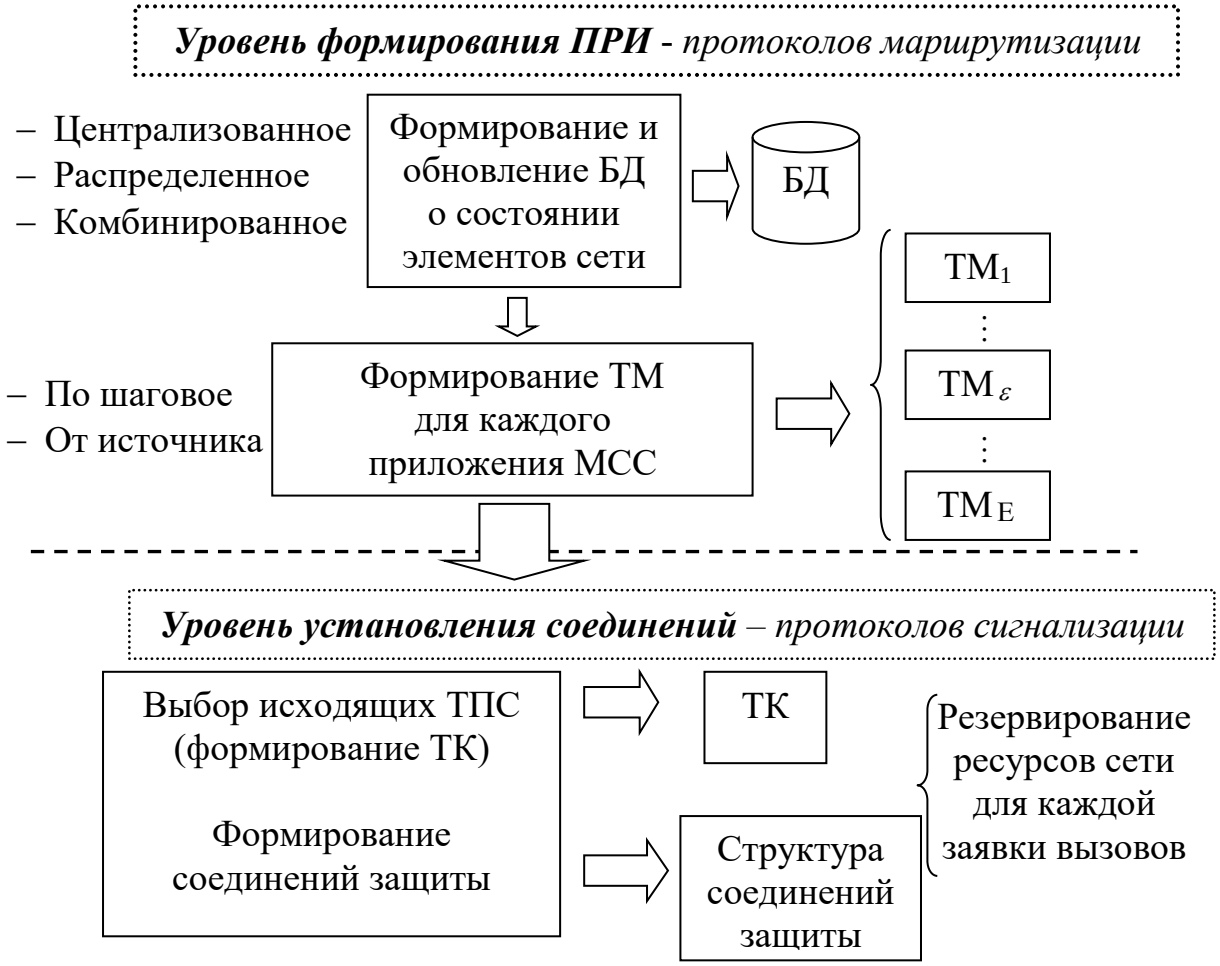


Рисунок 3.3 – Обобщенная функциональная модель маршрутизации в МСС

Передача сообщений пользователей осуществляется по установленным соединениям, в соответствии с таблицами коммутации.

Введем следующие обозначения.

$r_{\text{о}}(t)$ – общий сетевой ресурс МСС – совокупность программно-аппаратных средств и каналов связи МСС, обеспечивающих передачу всех видов информации. Тогда общий средний сетевой ресурс МСС за период наблюдения T составит:

$$R_{\text{о}} = \lim_{T\to\infty} \frac{1}{T} \int_0^T r_{\text{о}}(t)dt. \qquad (3.5)$$

Соответственно, $r_{\text{П}}(t)$ – сетевой ресурс, выделяемый МСС для передачи пользовательской информации;

$$R_{\text{П}} = \lim_{T\to\infty} \frac{1}{T} \int_0^T r_{\text{П}}(t)dt \tag{3.6}$$

– средний ресурс, выделяемый МСС для передачи пользовательской информации за период наблюдения T;

$r_{\text{с}}(t)$ – сетевой ресурс, выделяемый МСС для передачи служебной информации;

$$R_{\text{с}} = \lim_{T\to\infty} \frac{1}{T} \int_0^T r_{\text{с}}(t)dt \tag{3.7}$$

– средний ресурс, выделяемый МСС для передачи служебной информации за период наблюдения T;

$r_{\text{тм}}(t)$ – сетевой ресурс, выделяемый МСС для передачи служебной информации, участвующей в формировании ПРИ;

$$R_{\text{тм}} = \lim_{T\to\infty} \frac{1}{T} \int_0^T r_{\text{тм}}(t)dt \tag{3.8}$$

– средний ресурс, выделяемый МСС для передачи служебной информации, участвующей в формировании ПРИ, за период наблюдения T;

$r_{\text{сс}}(t)$ – сетевой ресурс, выделяемый МС для передачи служебной информации, участвующей в формировании ТК;

$$R_{\text{сс}} = \lim_{T\to\infty} \frac{1}{T} \int_0^T r_{\text{сс}}(t)dt \tag{3.9}$$

– средний ресурс, выделяемый МСС для передачи служебной информации, участвующей в формировании ТК, за период наблюдения T;

$r_з(t)$ – сетевой ресурс, выделяемый МС для передачи служебной информации, участвующей в формировании соединений защиты пользовательской информации;

$$R_з = \lim_{T\to\infty} \frac{1}{T} \int_0^T r_з(t)dt \tag{3.10}$$

– средний ресурс, выделяемый МСС для передачи служебной информации, участвующей в формировании соединений защиты пользовательской информации, за период наблюдения T.

В данном случае справедливы следующие соотношения (рисунок 3.4):

$$r_с(t) = r_{тм}(t) + r_{сс}(t) + r_з(t);$$

$$r_о(t) = r_п(t) + r_с(t) = r_п(t) + r_{тм}(t) + r_{сс}(t) + r_з(t);$$

$$R_с = R_{тм} + R_{сс} + R_з; \tag{3.11}$$

$$R_о = R_п + R_с = R_п + R_{тм} + R_{сс} + R_з. \tag{3.12}$$

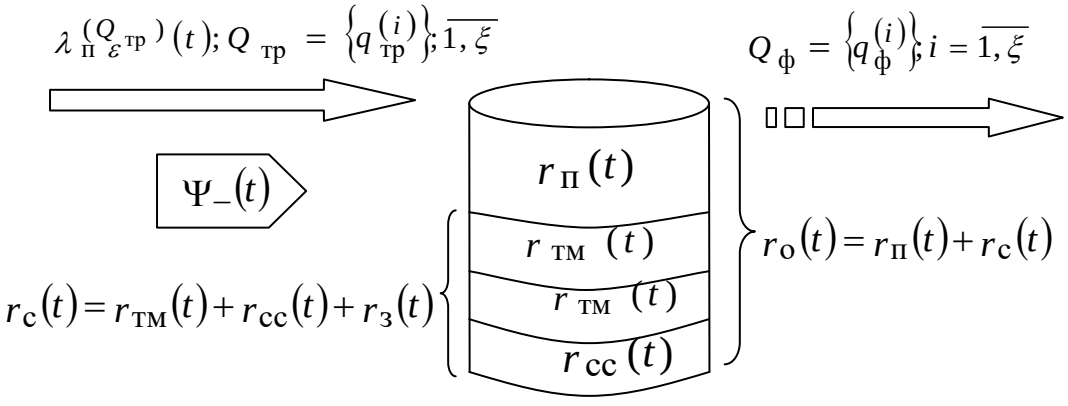


Рисунок 3.4 – Распределение сетевых ресурсов МСС

Пусть:

$\lambda_{\text{п}\,\varepsilon}^{(Q_{\text{тр}})}(t)$ – интенсивность поступления заявок от санкционированных пользователей в МСС с требуемым качеством обслуживания ε-го приложения $\left(\varepsilon = \overline{1,\text{E}}\right)$

$$Q_{\text{тр}} = \left\{q_{\text{тр}}^{(i)}\right\}, i = \overline{1,\xi}, \tag{3.13}$$

где $q_{\text{тр}}^{(i)}$ – i-й параметр качества обслуживания (время задержки, скорость передачи информации, надежность, помехозащищенность, защищенность информации и так далее) требуемый ε-м приложением $\left(\varepsilon = \overline{1,\text{E}}\right)$ для передачи пользовательской информации;

$\Psi_{-}(t)$ – внешнее деструктивное воздействие на МСС с целью несанкционированного использования сетевых ресурсов МСС $r_{\text{о}}(t)$;

$$Q_{\text{ф}} = \left\{q_{\text{ф}}^{(i)}\right\}, i = \overline{1,\xi}$$

параметры качества обслуживания приложений пользователей, которые фактически обеспечивает МСС, где $q_{\text{ф}}^{(i)}$ – i-й параметр качества обслуживания (время задержки, скорость передачи информации, надежность, помехозащищенность, защищенность информации и так далее), который фактически обеспечивает МСС.

Тогда можно утверждать следующее. При заданных параметрах МСС

$$\{r_{\text{о}}(t), \lambda_{\text{п}\,\varepsilon}^{(Q_{\text{тр}})}(t), \Psi_{-}(t)\}$$

маршрутизация

$$ROUT = \{ROUT_{\text{тм}} \uparrow ROUT_{\text{сс}}\} \tag{3.14}$$

(здесь знак $\uparrow$ означает последовательное выполнение двух процедур), содержащая процедуры формирования множества таблиц маршрутизации ($ROUT_{\text{тм}}$) и процедуры выбора исходящего ТПС ($ROUT_{\text{сс}}$) в каждом УК при поиске маршрута $\mu_{\text{уи,уп}}$ между УИ и УП, будет:

– оптимальной, если при минимальном использовании $r_{\text{с}}(t)$, то есть $r_{\text{с}}(t) = \min r_{\text{с}}(t)$, выполняется условие $Q_{\text{ф}} = Q_{\text{тр}}$;

– субоптимальной, если при условии $\lim\limits_{r_c(t)\to\min r_c(t)}$ выполняется требование $Q_{\text{ф}} \geq Q_{\text{тр}}$.

3.3 Обзор современных методов маршрутизации в мультисервисных сетях связи

3.3.1 Современные методы формирования плана распределения информации в мультисервисных сетях связи

«Лавинный» метод [45] формирования ПРИ на сети состоит в следующем. В каждом УК через определенное время $\Delta t = \text{constant}$ генерируются зонд-сигналы, которые пересылаются ко всем смежным узлам. В смежных УК эта процедура повторяется. Таким образом, зонд-сигналы попадают во все узлы сети. По мере продвижения по сети зонд-сигналы анализируют ВВХ всех элементов сети (УК, ЛС, ТПС, КС и так далее). По окончании зондирования сети сигналы возвращаются в исходные УК. Собранная информация о ВВХ элементов сети записывается в базы данных УК, анализируется и используется для расчета ТМ.

Основным недостатком «Лавинного» метода формирования ПРИ является необходимость выделения определенного ресурса сети (КС, ТПС) для передачи зонд-сигналов.

«Лавинный» метод реализован в технологии ATM и IP всех версий [167], а именно: PNNI (Private Network – to – Network Interface) [134], RIP (Routing Information Protocol) [166], IGRP (Interior Gateway Routing Protocol), EIGRP (Extended IGRP), IS-IS (Intermediate System – to – Intermediate System) [147], OSPF (Open Shortest Path First) [165].

«Статистический», или «Игровой» метод [46] предусматривает формирование ПРИ по накопленной статистике установления соединения между заданной парой УК.

Перед началом функционирования на сети устанавливается начальный ПРИ в виде набора ТМ (3.1) (для пошаговой ТМ). Каждому значению матрицы (3.1)

$$m_{i\nu}^{(j)}; \nu = \overline{1, \chi_j}; i, j = \overline{1, S}; i \neq j$$

присваивается некоторый весовой коэффициент

$$0 \leq p_{i\nu}^{(j)} \leq 1; \nu = \overline{1, \chi_j}; i, j = \overline{1, S}; i \neq j.$$

Причем

$$\overline{p_i^{(j)}} = \left(p_{i1}^{(j)}, ..., p_{i\nu}^{(j)}, ... p_{i\chi_j}^{(j)} \right); \nu = \overline{1, \chi_j}; i, j = \overline{1, S}; i \neq j,$$

нормируется, то есть

$$\sum_{\nu=1}^{\chi_j} p_{i\nu}^{(j)} = 1.$$

В результате формируется матрица весовых коэффициентов:

$$P^{(j)} = \left\| p_{i,\nu}^{(j)} \right\|_{(S-1),\chi_j} = \left(\overline{p_1^{(j)}},\ldots,\overline{p_i^{(j)}},\ldots,\overline{p_{j-1}^{(j)}},\overline{p_{j+1}^{(j)}},\ldots,\overline{p_S^{(j)}} \right), \quad (3.15)$$

где

$$\overline{p_i^{(j)}} = \left(p_{i1}^{(j)},\ldots,p_{i\nu}^{(j)},\ldots p_{i\chi_j}^{(j)} \right); \nu = \overline{1,\chi_j}; i, j = \overline{1,S}; i \neq j. \quad (3.16)$$

Формирование (коррекция) ПРИ и определение маршрута осуществляется следующим образом. Во всех транзитных УК, начиная с УИ, при поиске маршрута к *i*-му УП происходит обращение к *i*-м строкам матриц маршрутизации (3.15). В *i*-х строках (3.16) определяется максимальный весовой коэффициент $p_{i\nu}^{(j)}$. Тем самым выбирается *ν*-й исходящий ТПС из *j*-го УК при организации маршрута к *i*-му УК. В результате данных действий маршрут между заданной парой УК будет либо определен, либо данной заявке на определение маршрута будет дан отказ (в случае, если в одном из УК все исходящие ТПС оказались недоступными либо число транзитных узлов превысило допустимое значение, которое заранее было определено).

В первом случае, когда маршрут между заданной парой УК определен, все ТПС, входящие в данный маршрут, поощряются. Весовые коэффициенты $p_{i\nu}^{(j)}$ данных исходящих ТПС $m_{i\nu}^{(j)}$ увеличиваются. Во втором случае, когда маршрут не определен, исходящие ТПС, участвующие в данном поиске, штрафуются. Весовые коэффициенты $p_{i\nu}^{(j)}$ данных исходящих ТПС $m_{i\nu}^{(j)}$ уменьшаются. В обоих случаях строки

$$\overline{p_i^{(j)}} = \left(p_{i1}^{(j)},\ldots,p_{i\nu}^{(j)},\ldots p_{i\chi_j}^{(j)} \right); \nu = \overline{1,\chi_j}; i, j = \overline{1,S}; i \neq j,$$

элементы которых были изменены (поощрены или оштрафованы), нормируются.

Таким образом, в процессе эксплуатации сети формируется (корректируется) оптимальный ПРИ с переменным интервалом $\Delta t = \partial t$ (рисунок 3.2). Критерием оптимальности в данном случае является результат организации маршрутов в предыдущие моменты времени.

Если рассматривать весовые коэффициенты $p_{iv}^{(j)}$ как вероятности выбора соответствующих исходящих ТПС $m_{iv}^{(j)}$, то можно предположить, что «Статистический» метод формирования ПРИ имеет итеративный характер и решает задачу глобальной оптимизации ПРИ на сети связи по критерию – вероятность установления соединения между парами УИ и УП.

Необходимость передачи минимального количества служебной информации для формирования ПРИ на сети является несомненным достоинством «Статистического» метода. Однако данный метод обладает инерционностью. Действительно, при выходе элементов сети связи из строя потребуется некоторый период времени для переформирования ПРИ на сети.

Другим недостатком «Статистического» метода является неопределенность выбора начального ПРИ в случае ввода новых УК в эксплуатацию.

Отметим, что данный метод был реализован в технологии MPLS [168].

«Логический» метод [22, 23] формирования ПРИ на сети связи состоит в процедуре, выполняемой в каждом транзитном УК, начиная с УИ, и позволяющей определить исходящий ТПС, максимально близкий к геометрическому направлению на УП. Для этого сеть связи вкладывается в систему координат (например, в прямоугольную). Каждому узлу сети согласно системы координат (*X, Y*) присваивается собственный адрес (рисунок 3.5).

В каждом транзитном УК (X_i, Y_j), начиная с УИ (X_R, Y_L), производится анализ адреса УП сопоставлением его с собственным. В результате вычисляется геометрическое направление из данного узла на УП. Затем определяется тот исходящий ТПС, который имеет наибольшее совпадение с ранее рассчитанным геометрическим направлением на УП. Если ближайший по направлению ТПС недоступен, то подбирается очередной по предпочтительности исходящий ТПС.

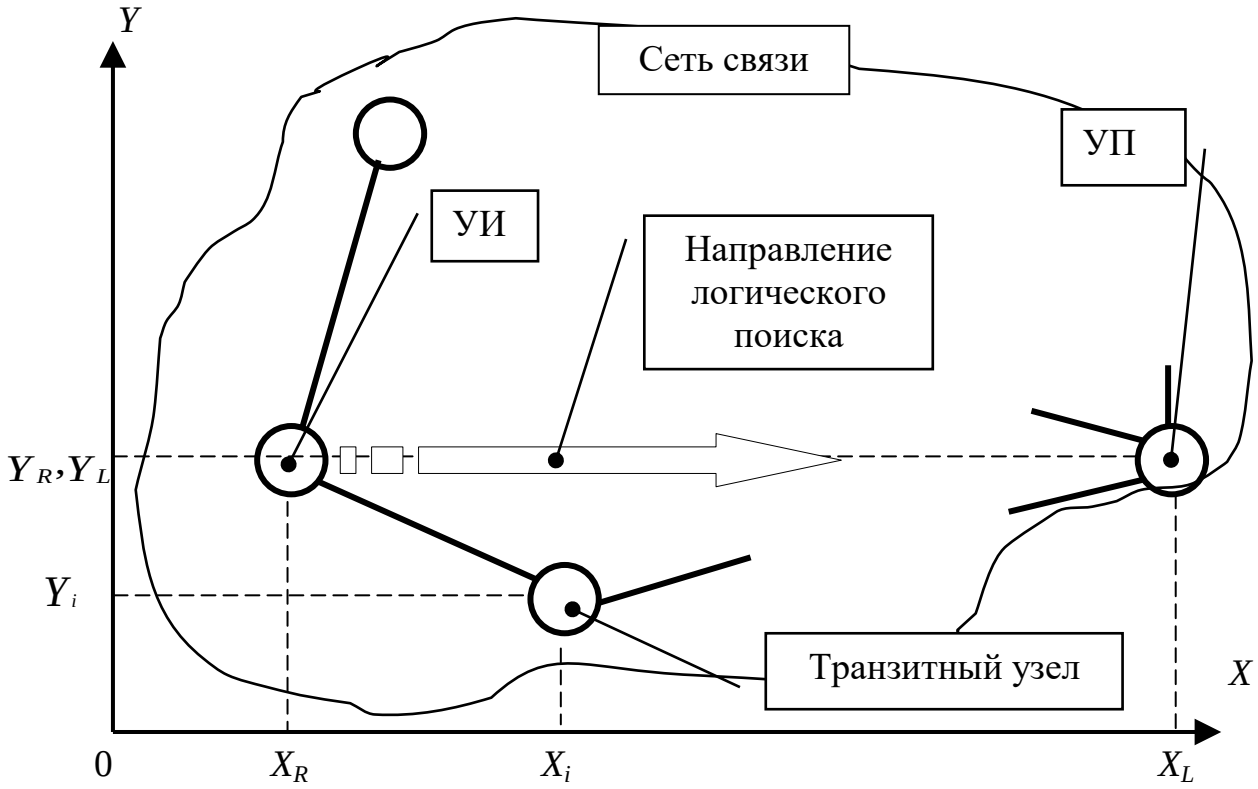


Рисунок 3.5 – Поиск маршрута «Логическим» методом

Несомненным достоинством данного метода является простота и отсутствие необходимости передачи служебной информации по сети. Применение простого алгоритма вычисления исходящего ТПС в каждом УК позволяет отказаться от ТМ, что значительно сокращает объем оперативной памяти УК, упрощает процедуру маршрутизации и ввод в эксплуатацию новых узлов. В то же время данный метод не является динамическим и не решает задачу глобальной оптимизации ПРИ.

3.3.2 Методы выбора исходящих трактов в узлах коммутации мультисервисных сетей связи

В зависимости от количества одновременно устанавливаемых маршрутов между УИ и УП различают последовательный либо параллельный (многопутевой) выбор исходящих ТПС [41, 80, 125, 128, 153].

Последовательный выбор исходящих ТПС состоит в том, что в каждом УК, начиная с УИ, осуществляется выбор только одного исходящего ТПС. В

результате на сети будет формироваться один маршрут, состоящий из последовательного наращивания коммутационных участков из УИ к УП.

Отличительная особенность алгоритмов с параллельным выбором исходящих ТПС состоит в том, что поиск маршрута между УИ и УП осуществляется одновременно по всем исходящим ТПС в определенной зоне сети связи.

В зависимости от характера распространения на сети процесса поиска маршрута выделим три основных класса последовательных алгоритмов выбора исходящих ТПС: градиентный, диффузный и градиентно-диффузный.

Градиентный состоит в том, что в каждом транзитном узле, начиная с УИ, в процессе выбора исходящего ТПС участвуют не все исходящие ТПС, а лишь часть (наиболее предпочтительные). Если в одном из УК исходящие ТПС, участвующие в выборе, не доступны, то данной заявке на формирование маршрута дается отказ.

В результате градиентного выбора маршрут будет формироваться вдоль геометрического направления с УИ на УП (рисунок 3.6).

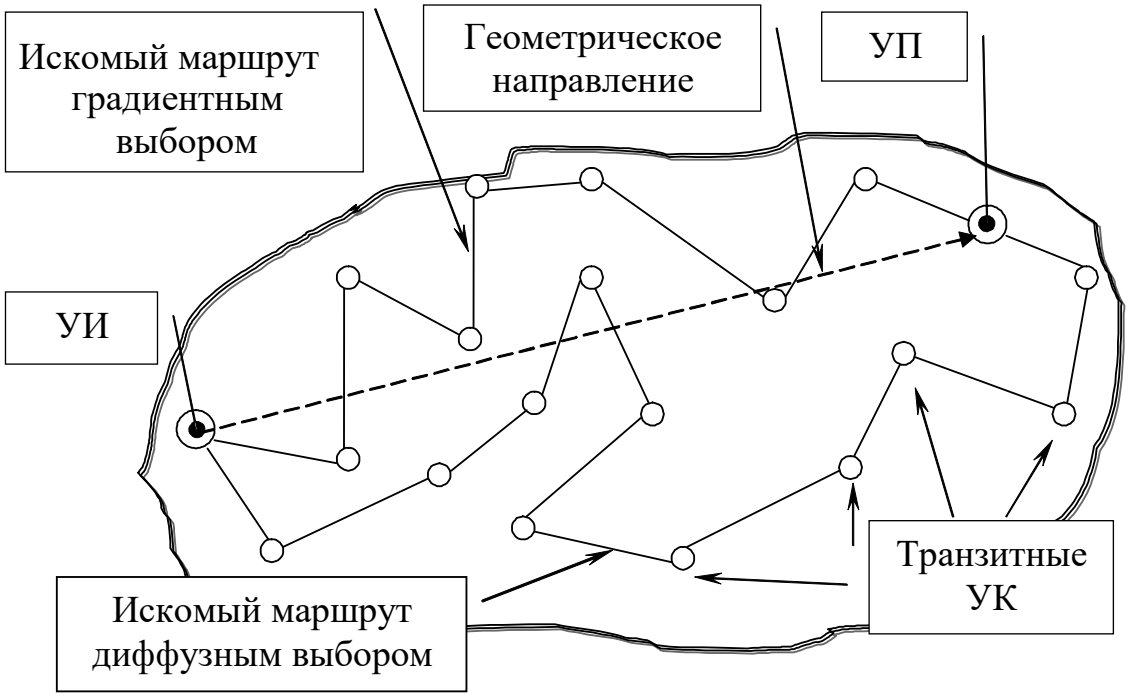


Рисунок 3.6 – Градиентный и диффузный выбор исходящих ТПС

Увеличение количества исходящих ТПС, участвующих в выборе, приведет к возможному отклонению маршрута от геометрического направления с УИ на УП, в том числе и в сторону противоположную от УП.

Выбор ТПС, при котором искомый маршрут формируется и в противоположную сторону от УП, будем называть диффузным.

Таким образом, диффузный выбор исходящих ТПС допускает возможность выбора любого доступного исходящего ТПС.

Градиентно-диффузный метод являются комбинацией первых двух.

Реализация градиентных алгоритмов выбора исходящих ТПС позволяет организовать кратчайшие маршруты (по числу транзитных УК).

Диффузные обладают большой гибкостью при обходах поврежденных участков сети, однако средняя длина маршрута в равных с градиентным условиях будет большей.

В свою очередь процедура выбора исходящего ТПС в каждом УК может быть детерминированной и стохастический. В первом случае выбор исходящего ТПС осуществляется однозначно по максимальному значению одного из элементов вектора (3.2). Во втором случае выбор исходящего ТПС производится в результате случайного розыгрыша. При этом исходящие ТПС, имеющие большие значения $m_{iv}^{(j)}$, получают большую вероятность выбора.

Возможен и комбинированный способ выбора исходящих ТПС, который содержит как вероятностную, так детерминированную компоненты.

Учитывая перечисленные градации, можно указать множество вариантов последовательных алгоритмов выбора исходящих ТПС в УК (например, "Диффузный вероятностный" или "Градиентно-диффузный детерминированный").

На сегодняшний день из последовательных методов широкое применение нашел «Диффузный детерминированный" [134, 164, 169, 170].

3.4 Разработка классификации методов маршрутизации в сетях связи

Анализ вышеизложенного материала позволяет разработать новую классификацию методов маршрутизации для сетей связи. Отличительная особенность данной классификации состоит в том, что она учитывает независимые процедуры: формирование плана распределения информации на сети; выбор исходящих линий, трактов, каналов связи в узлах коммутации (рисунок 3.7) [74].

Данная классификация позволяет:

– выявить множество вариантов реализации как последовательных, так и параллельных (многопутевых) методов маршрутизации (например: "Вероятностный диффузный с использованием лавинного метода формирования ПРИ);

– провести целенаправленный анализ и синтез тех методов маршрутизации, которые будут наиболее эффективно функционировать в предполагаемых сетях связи и в заданных условиях.

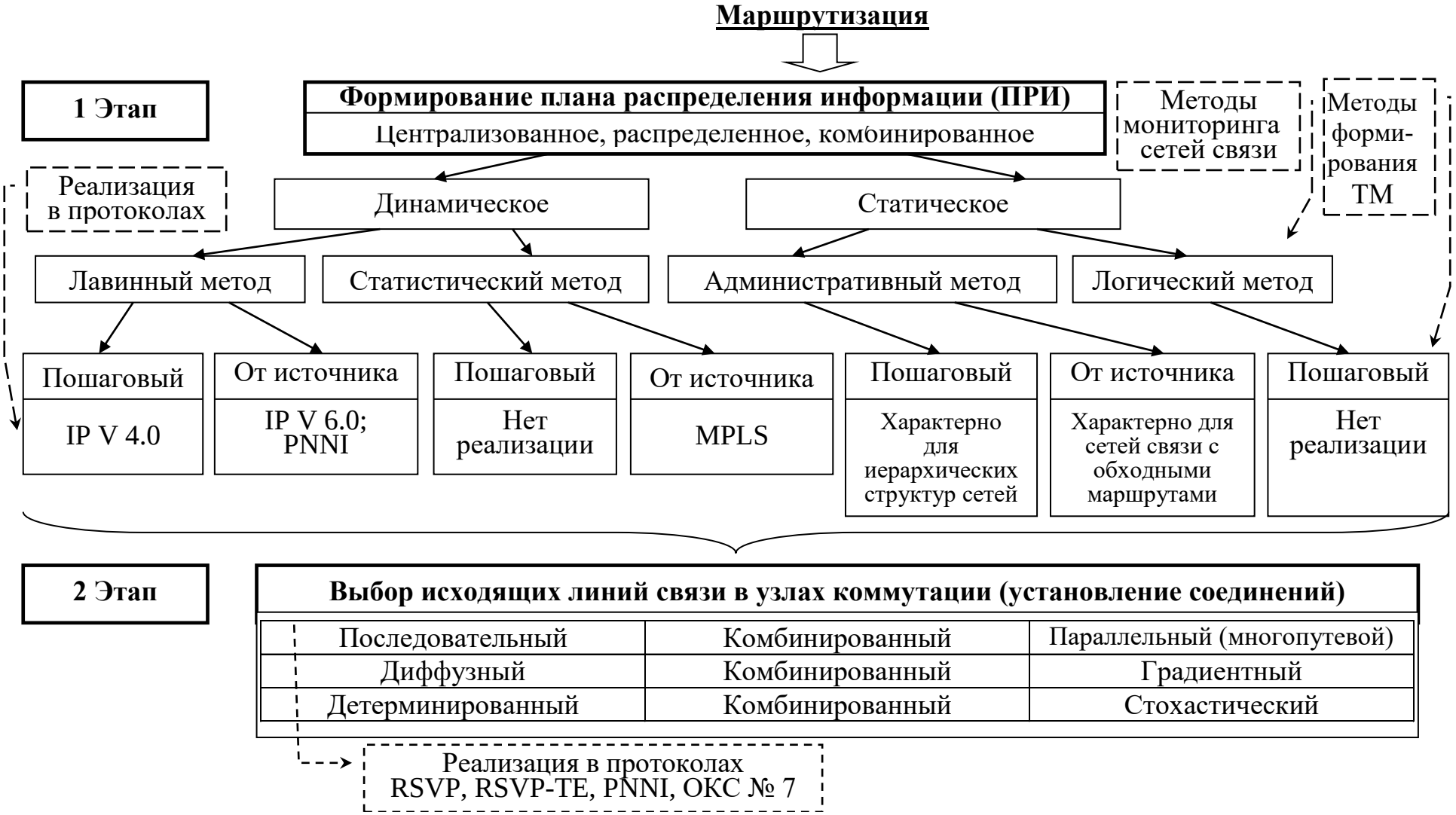


Рисунок 3.7 – Классификация методов маршрутизации в сетях связи

3.5 Разработка перспективных методов маршрутизации в сетях связи

3.5.1 «Логико-статистический» метод формирования плана распределения информации

«Логико-статистический» метод формирования ПРИ [74, 78] является обобщением «Логического» и «Статистического». Данный метод вобрал в себя положительные свойства обоих методов:

– отсутствие необходимости передачи служебной информации на сети при формировании (во время ввода УК в эксплуатацию) и переформировании (в процессе эксплуатации УК) ТМ;

– решение задачи глобальной оптимизации ПРИ на сети связи по накопленной статистике установления соединения между заданной парой УК.

Суть «Логико-статистического» метода формирования ПРИ сводится к следующему. По аналогии с «Логическим» методом сеть связи вкладывается в прямоугольную систему координат, в соответствии с которой каждому узлу сети присваивается собственный адрес (*X*, *Y*). В каждом *j*-м УК имеется расширенная матрица (3.15):

$$P'^{(j)} = \left\| p'^{(j)}_{i,v} \right\|_{(S^{(j)}-1),(\chi_j+3)}; v = \overline{1, \chi_j}; i, j = \overline{1, S}; i \neq j, \qquad (3.17)$$

которая содержит $(S-1)$ строк и (χ_j+3) столбца. Один столбец отводится для номеров УП, представленных в общепризнанной нумерации (№ УП), и два столбца для номеров в прямоугольной системе координат (*X*, *Y*).

На момент ввода узла в эксплуатацию матрица содержит только информацию о смежных номерах УК с данным, выраженную в прямоугольной системе координат.

По мере функционирования сети связи матрица $P'^{(j)}$ заполняется и корректируется.

Определение исходящих ТПС осуществляется «Логическим» методом, а заполнение и корректировка матрицы $P'^{(j)}$ осуществляется «Статистическим» методом.

Тем самым при формировании (во время ввода УК в эксплуатацию) и переформировании (в процессе эксплуатации УК) ТМ отпадает необходимость передачи служебной информации по сети. Накапливание информации в ТМ о формировании маршрутов позволяет решить задачу глобальной оптимизации ПРИ на сети связи.

3.5.2 «Локально-волновой» метод маршрутизации

Рассмотрим «Локально-волновой» метод [23, 41, 56, 78, 80], который является обобщением «Лавинного» и «Логического» методов формирования плана распределения информации на сети связи. «Локально-волновой» метод маршрутизации в зависимости от организации выбора исходящего ТПС может быть отнесен к параллельным (многопутевым) и к параллельно-последовательным (комбинированным) методам. В то же время способ выбора зоны, в которой осуществляется поиск маршрута, в «Локально-волновом» методе может быть вероятностным, детерминированным и комбинированным.

«Локально-волновой» метод маршрутизации состоит в том, что для нахождения оптимального маршрута в сети между парой узлов из узла-источника организуется «Лавинный» поиск, но не во всех направлениях, а лишь в сторону узла-получателя. Волна поиска распространяется в некоторой зоне в виде полосы, охватывающей пару соединяемых узлов (рисунок 3.8). Ширина и форма полосы в зависимости от приоритета пользователя, состояния элементов сети (УК, ТПС) и требований приложений МСС к качеству обслуживания может устанавливаться в различных пределах. На рисунке 3.8 показан «Локально-волновой» поиск на сети от УИ к УП в некоторый момент времени, соответствующий примерно половине

пути между парой узлов. Из рисунка видно, что поисковая волна – это подвижная узкая зона, все узлы в пределах которой охвачены процессом «Лавинного» поиска.

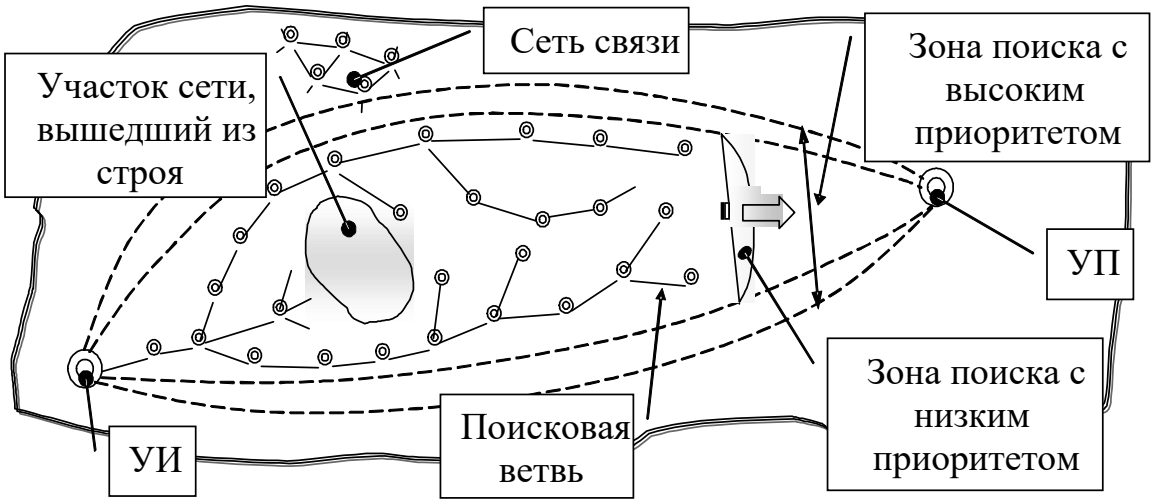


Рисунок 3.8 – Поиск маршрута «Локально-волновым» методом

Чем выше приоритет пользователя или требования приложений МСС к качеству обслуживания (QoS), тем больше возможностей имеется для установления соединения. Таким образом, при «Локально-волновом» методе в каждом узле определяются исходящие из данного узла ТПС к смежным УК, наиболее близко совпадающие с геометрическим направлением на искомый узел. Выбранные исходящие ТПС располагаются в ряд по степени предпочтительности. При этом в понятие предпочтительности может вкладываться не только степень близости к указанному направлению на УП, а также ВВХ элементов сети связи.

Количество подсоединенных ТПС, а следовательно, и ширина поисковой волны определяются приоритетом вызывающего пользователя, либо требованиями приложений МСС к качеству обслуживания (QoS). Для пользователей низшей категории количество выбранных трактов передачи сообщений может не превышать одного, тогда поиск превращается в последовательный. Для пользователей высших приоритетов поиски могут отличаться не только шириной волны поиска, но и комбинированием последовательного поиска с расщеплением на «Локально-волновой» в тех узлах, где последовательный поиск встречает препятствие.

Для организации в сети «Локально-волнового» метода маршрутизации необходимо обеспечить выполнение следующих требований.

В волне поиска должны быть исключены замкнутые петли, то есть один и тот же узел коммутации не должен подключаться к процессу поиска более одного раза.

В области поиска не должно быть неохваченных волной узлов, кроме тех, которые полностью загружены или вышли из строя.

В случае занятости УП, невозможности доступа к нему или его повреждения распространение волны поиска должно быть приостановлено, а все выбранные волной ТПС должны самораспадаться.

Доступ к УП должен быть обеспечен со всех входящих в него ТПС.

Внутри области, охваченной поисковой волной, отдельные тупиковые маршруты должны самораспадаться еще до завершения процесса поиска.

Набранные таким образом маршруты (маршрут) фиксируются на все время сеанса передачи пользовательской информации между заданной парой узлов коммутации. По окончании сеанса передачи пользовательской информации маршруты (маршрут) распадаются.

Организация «Локально-волнового» метода маршрутизации может быть следующей.

Адресация узлов коммутации на сети допускается произвольной, обеспечивающая, однако, единственность номера каждого узла коммутации. В запоминающем устройстве блока управления каждого УК содержится ТМ, число строк которой равно $(S-1)$. Таблица запоминается к моменту запуска в работу данного узла. Таблица может заполняться и корректироваться по мере расширения сети и появления новых узлов коммутации, ТПС, изменения режима работы узла, изменения адресов и приоритетов.

Для данного УК в *T*-й строке таблицы содержится следующая информация.

1. Перечень исходящих из данного узла трактов передачи сообщений, начинающийся с наиболее близкого к геометрическому направлению на УП и далее в убывающем порядке.

2. Перечень тех исходящих ТПС, по которым должна распространяться волна поиска из данного узла к УП для каждого из принятых в сети приоритетов. Чем выше приоритет, тем больше число возможных исходящих ТПС одновременно участвует в распространении волны поиска.

3. Время существования данного поиска, что косвенно отражает расстояние между данным узлом и УП. Для высших приоритетов время поиска может быть увеличено.

Далее будет рассматриваться только процесс установления соединения между УИ и УП в сети. Процедура подключения вызывающего пользователя здесь не рассматривается. Предполагается, что вызывающий пользователь, получив доступ к сети, передал, а УИ принял и зафиксировал адрес УП и приоритет вызывающего пользователя.

Процесс организации в сети «Локально-волнового» поиска маршрута инициируется УИ. В УИ, при этом формируется поисковая посылка, в состав которой входят:

– номер узла получателя;

– номер узла источника и индекс, отличающий данный поиск от других, одновременно исходящих с одного и того УИ;

– приоритет поиска;

– абсолютное время, до которого разрешается существование данного поиска.

Поисковая посылка в УИ подвергается анализу – определяются с учетом приоритета те ТПС, по которым должна распространяться данная волна поиска. Если в этих ТПС есть свободные каналы, то они резервируются данным поиском. По этим же каналам (либо по специально выделенным служебным каналам) на смежные УК передается поисковая посылка. В смежных узлах данная посылка подвергается такому же анализу, и также резервируются свободные каналы в выбранных ТПС. На всех последующих УК процесс повторяется аналогично описанному.

3.5.3 «Гибридный» метод маршрутизации

«Гибридный» или «Логико-лавинно-статистический» метод маршрутизации [74, 78] является обобщением «Логического», «Лавинного» и «Статистического», суть которого сводится к следующему. По аналогии с «Логическим» методом сеть связи вкладывается в прямоугольную систему координат, в соответствии с которой каждому узлу коммутации сети присваивается собственный адрес (X, Y). В каждом j-м УК имеется матрица (3.17).

На момент ввода узла в эксплуатацию матрица содержит только информацию о смежных номерах УК с данным и выраженных в прямоугольной системе координат.

По мере функционирования сети связи матрица (3.17) заполняется и корректируется. Определение исходящих ТПС осуществляется «Логическим» методом, а заполнение и корректировка матрицы (3.17) осуществляется «Статистическим» методом. Тем самым при формировании (во время ввода УК в эксплуатацию) и переформировании (в процессе эксплуатации УК) ТМ отпадает необходимость передачи служебной информации по сети. Накапливание информации в ТМ о формировании маршрутов позволяет решить задачу глобальной оптимизации ПРИ на сети связи.

В случае внешних деструктивных воздействий на элементы МСС (УК, ЛС) формирование ПРИ осуществляется «Лавинным» методом. При этом выбор исходящих ЛС в УК, начиная от УИ до УП, может быть последовательным, параллельным (многопутевым) либо комбинированным. Данный подход позволяет сократить объем передаваемой служебной информации на сети во время: ввода узлов коммутации в эксплуатацию; штатной эксплуатации сети, за счет накопленной ранее статистики установления соединения между заданной парой УК; внешних деструктивных воздействий на элементы МСС.

Таким образом, данный метод вобрал в себя положительные свойства трех методов «Логического», «Лавинного» и «Статистического»:

– отсутствие необходимости передачи служебной информации на сети при формировании (во время ввода УК в эксплуатацию) и переформировании (в процессе эксплуатации УК) ТМ;

– определение оптимальных маршрутов и установление соединений, поддерживающих QoS приложений в условиях внешних деструктивных воздействий на элементы МСС;

– решение задачи глобальной оптимизации ПРИ на сети связи по накопленной ранее статистике установления соединения между заданной парой УК.

3.6 Выводы

1. Обобщенная функциональная модель маршрутизации учитывает резервирование сетевых ресурсов для обеспечения комплексной защиты пользовательской информации и поддержания качества обслуживания приложений мультисервисной сети связи.

2. Классификация методов маршрутизации для сетей связи учитывает независимые процедуры: формирование плана распределения информации на сети; выбор исходящих линий, трактов, каналов связи в узлах коммутации. Данная классификация позволяет:

– выявить множество вариантов реализации как последовательных, так и параллельных (многопутевых) методов маршрутизации;

– провести целенаправленный анализ и синтез тех методов маршрутизации, которые будут наиболее эффективно функционировать в предполагаемых сетях связи и в заданных условиях.

3. «Гибридный» метод маршрутизации в зависимости от степени и характера внешних деструктивных воздействий на элементы сети использует для формирования таблиц маршрутизации «Логический», «Статистический» или «Лавинный» методы формирования ПРИ. Это позволяет сократить объем передаваемой служебной информации на сети во время: ввода узлов коммутации

в эксплуатацию; штатной эксплуатации сети, за счет накопленной ранее статистики установления соединения между заданной парой УК; внешних деструктивных воздействий на элементы сети.

4. Для определения границы использования «Логического», «Статистического» и «Лавинного» методов формирования ПРИ необходимо провести исследование функционирования МСС в условиях внешних деструктивных воздействий на элементы сети.

4 Разработка моделей маршрутизации в мультисервисной сети связи в условиях внешних деструктивных воздействий

4.1 Постановка задачи

Спектр методов маршрутизации, которые можно применить на сетях связи, весьма широк – от простейших, фиксированных процедур, до весьма сложных (рисунок 3.7). Каждый из них имеет свои достоинства и недостатки.

Вопросам исследования методов маршрутизации на сетях связи посвящено много работ [10, 14, 16 ÷ 20, 26, 30, 38, 42, 44 ÷ 51, 54, 57, 59, 63, 87, 88, 103, 111, 115, 121, 132, 138, 149, 154, 183]. Это связано с тем, что выбор метода маршрутизации в значительной мере влияет на эффективность использования ресурсов сети и качество обслуживания приложений, доступных пользователям. Вместе с тем проведение натурных исследований на действующих сетях сопряжено с существенными техническими, организационными и финансовыми трудностями. Поэтому в качестве инструментария для анализа влияния маршрутизации на QoS приложений мультисервисной сети связи применяют имитационное и математическое моделирование.

К настоящему времени в качестве математического аппарата используют теорию графов [88, 95], массового обслуживания [16, 26, 38, 40, 42, 64, 103, 106], цепей Маркова [17 ÷ 20], нечетких множеств [14], нейронных сетей [30], игр [178], сетей Петри [31]. Применение столь широкого диапазона математических подходов обусловлено сложностью и спецификой предмета анализа. Задача исследования методов маршрутизации особенно усложняется в условиях внешних деструктивных воздействий на элементы мультисервисных сетей связи.

В данной главе представлены модели, позволяющие (при определенных ограничениях) проводить анализ влияния методов маршрутизации на QoS приложений мультисервисных сетей в условиях внешних деструктивных воздействий.

4.2 Математическая модель влияния методов формирования плана распределения информации на объем доступных сетевых ресурсов

Представим структуру мультисервисной сети связи в виде неориентированного графа $G[A_S, M_S]$ с множеством: вершин $A_S = \{a_i\}; i = \overline{1,S}$, соответствующих УК; ребер $M_S = \{m_{ij}\}; i, j = \overline{1,S}; i \neq j$, соответствующих ЛС.

Пусть каждая ЛС обладает средней пропускной способностью за время наблюдения T:

$$r_{ij} = \lim_{T \to \infty} \frac{1}{T} \int_0^T r_{ij}(t)dt; i, j = \overline{1,S}; i \neq j \text{ [бит/с]},$$

которую будем называть ресурсом ЛС.

Очевидно, что общий средний сетевой ресурс МСС (3.5) будет определяться выражением:

$$R_{\text{О}} = \sum_{i,j=1; i \neq j}^{S} r_{ij} \text{ [бит/с]}; \quad (4.1)$$

В мультисервисной сети связи отказ в установлении соединения возникает при недоступности пользовательских сетевых ресурсов, гарантирующих QoS выбранных приложений. В этой связи представляет интерес проведения исследований влияния методов маршрутизации $ROUT$ (3.14) на доступность пользовательских сетевых ресурсов $R_{\text{П}}$ (3.6) (рисунок 3.4) в условиях внешнего деструктивного воздействия $\Psi_-(t)$:

$$R_{\text{П}} = f(R_{\text{О}}, \Psi_-(t), ROUT). \quad (4.2)$$

Приведенная на рисунке 3.7 классификация методов маршрутизации показывает, что современные сетевые технологии ATM, IP, MPLS и ОКС №7 используют «Последовательный, диффузный, детерминированный» метод выбора исходящих ТПС (протоколы сигнализации). При этом в ATM, IP (всех версий) применяется «Лавинный» метод формирования плана распределения информации, а в MPLS – «Статистический» метод. Поэтому для анализа функционала (4.2) выберем:

– методы формирования плана распределения информации (протоколы маршрутизации): $ROUT_{\text{тм}}^{(\text{лав})}$ – «Лавинный» (от источника); $ROUT_{\text{тм}}^{(\text{стат})}$ – «Статистический» (от источника);

– $ROUT_{\text{сс}}$ − метод выбора исходящих ТПС (протоколы сигнализации) – «Последовательный, диффузный, детерминированный».

Нагрузка на сетевые элементы, создаваемая маршрутизацией $ROUT = \{ROUT_{\text{тм}} \uparrow ROUT_{\text{сс}}\}$, зависит от многих факторов:

– внешних деструктивных воздействий на элементы МСС;

– частоты попыток установления соединений между УИ и УП;

– методов выбора исходящих ТПС (протоколов сигнализации);

– методов формирования плана распределения информации (протоколов маршрутизации) и многих других.

Можно предположить, что процесс использования сетевых ресурсов, необходимых для реализации анализируемых методов маршрутизации в МСС, имеет нелинейную зависимость и в общем случае подчиняется полиномиальному закону [68, 75]:

$$R^{(ROUT)} = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0, \qquad (4.3)$$

где

$a_i; i = \overline{0,n}$ – коэффициенты, значение которых зависит от применения метода маршрутизации на сети связи;

$0 \le x \le 1$ – переменная, которая определяет степень недоступности общих сетевых ресурсов МСС и имеет следующий физический смысл.

1. Влияет на величину средних сетевых ресурсов, необходимых для организации маршрутизации. Действительно,

$$\text{если} \begin{cases} x = 0, \text{то используются минимальные сетевые ресурсы при процедуре } ROUT; \\ x = 1, \text{то используются максимальные сетевые ресурсы при процедуре } ROUT. \end{cases}$$

2. Определяет часть сетевых ресурсов, которые подвержены внешним деструктивным воздействиям $\Psi_-(t)$. В этом случае средние сетевые ресурсы, оставшиеся после воздействия $\Psi_-(t)$ на МСС, определяются выражением:

$$R'_{\text{о}} = (1-x) \cdot R_{\text{о}} = (1-x) \cdot \sum_{i,j=1; i \ne j}^{S} r_{ij} \text{ [бит/с]}. \quad (4.4)$$

Очевидно, что средние сетевые ресурсы, доступные для передачи пользовательской информации, определяются выражением:

$$R_{\text{П}} = R'_{\text{о}} - R^{(ROUT)} \text{ [бит/с]}. \quad (4.5)$$

Определим значения коэффициентов $a_i; i = \overline{1,n}$ для различных методов маршрутизации. Предположим, что для реализации каждого из анализируемых методов маршрутизации в МСС генерируется за единицу времени блок данных B битов.

При «Лавинном» методе формирования плана распределения информации $ROUT^{(\text{лав})}$ каждый УК генерирует через равные интервалы времени $\Delta t = \text{consnat}$

(рисунок 3.2) зонд-сигналы путем широковещательной рассылки *K* блоков данных размером *B*. Следовательно, средние сетевые ресурсы, необходимые для организации «Лавинного» метода формирования ПРИ, определяется выражением:

$$R^{(\text{лав})} = a_0 = \frac{K \cdot B \cdot S}{\Delta t}.$$

Тогда выражение (4.5) с учетом (4.4) для «Лавинного» метода формирования ПРИ примет вид:

$$R_{\text{П}}^{(\text{лав})} = (1 - x) \cdot R_{\text{О}} - \frac{K \cdot B \cdot S}{\Delta t} \tag{4.6}$$

или в относительном выражении:

$$R_{\text{П отн}}^{(\text{лав})} = (1 - x) - \frac{K \cdot B \cdot S}{\Delta t \cdot R_{\text{О}}} = 1 - x - a'_0, \tag{4.7}$$

где

$$a'_0 = \frac{K \cdot B \cdot S}{\Delta t \cdot R_{\text{О}}}.$$

При «Статистическом» методе $ROUT^{(\text{стат})}$ корректировка таблиц маршрутизации происходит при попытке установления соединений. Следовательно, по аналогии с выводом выражения (4.7) получим:

$$R_{\text{П}}^{(\text{стат})} = 1 - x - \sum_{i=0}^{n} a_i^{(\text{стат})} \cdot x^i; \tag{4.8}$$

$$R_{\text{П отн}}^{(\text{стат})} = (1 - x) - \frac{\left(a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0\right)}{R_{\text{О}}} = 1 - x - \sum_{i=0}^{n} a'^{(\text{стат})}_i \cdot x^i, \tag{4.9}$$

где

$$a'_i = \frac{a_i}{R_0}; i = \overline{0,n}.$$

Ограничимся только одним членом полученного ряда, то есть получим завышенную оценку для «Статистического» метода формирования ПРИ

$$R_{\text{п отн}}^{(\text{стат})} = 1 - x - a'_1 \cdot x. \tag{4.10}$$

Проведем анализ выражений (4.7), (4.10). На рисунках 4.1 и 4.2 приведены графики зависимостей (4.7), (4.10) при изменении коэффициентов a'_0 и a'_1. Здесь $R'^{(ROUT)}_{\text{п отн}}$, $R'_{\text{о отн}}$ и $R_{\text{о отн}}$ – значения соответствующих величин относительно R_0.

Анализ данных зависимостей позволяет сделать следующие выводы.

1. При выполнении условия

$$x = \frac{a'_0}{a'_1} \tag{4.11}$$

существует зона ($x \approx 0{,}2 \div 0{,}4$), в пределах которой оба метода формирования ПРИ используют одинаковые средние сетевые ресурсы.

2. В случае, если

$$x < \frac{a'_0}{a'_1}, \tag{4.12}$$

т.е. значения степени недоступности общих сетевых ресурсов МСС находится в пределах $0 \le x \le (0{,}2 \div 0{,}4)$, «Статистический» метод формирования ПРИ использует меньше сетевых ресурсов, чем «Лавинный».

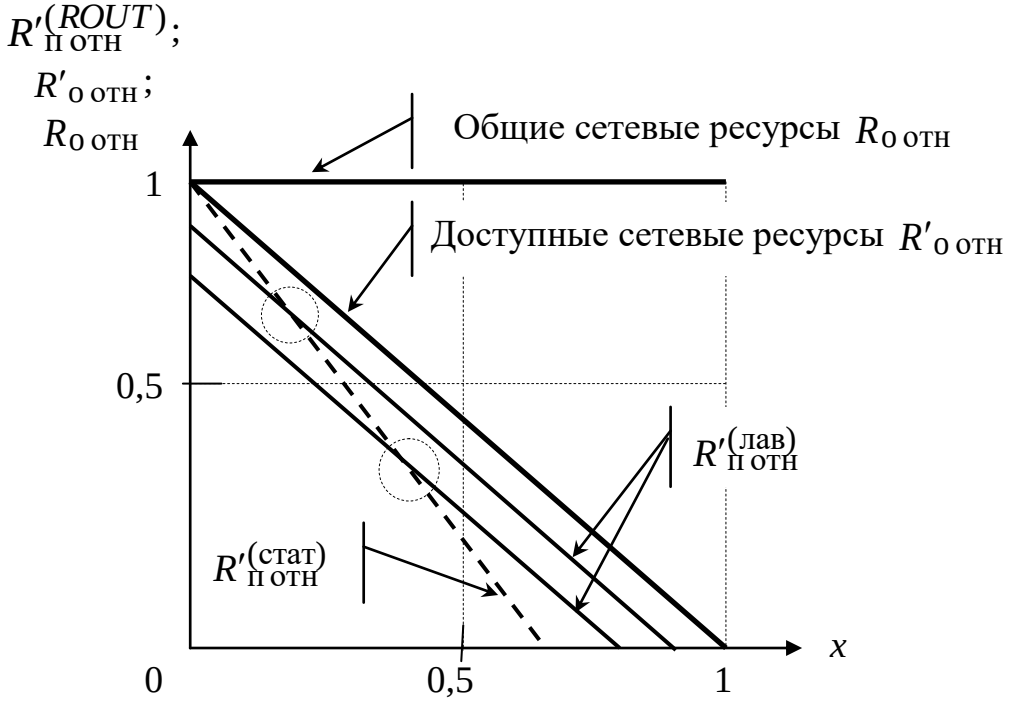


Рисунок 4.1 – Зависимости средних сетевых ресурсов от степени недоступности общих сетевых ресурсов МСС x для «Лавинных» методов формирования ПРИ

3. С увеличением степени недоступности общих сетевых ресурсов МСС x от $(0{,}2 \div 0{,}4)$ до 1 «Статистический» метод формирования ПРИ дает худшие результаты, по сравнению с «Лавинным» методом.

4. В условиях внешнего деструктивного воздействия $\Psi_{-}(t)$, при котором примерно 30% сетевых ресурсов выходит из строя, целесообразно применять «Лавинные» методы формирования ПРИ.

Приведем пример оценки объема пользовательских сетевых ресурсов $R_{\text{П}}$ (4.2), доступных пользователям для различных методов формирования ПРИ в условиях внешнего деструктивного воздействия $\Psi_{-}(t)$ [68, 75].

Допустим, что за время наблюдения T сеть связи, содержащая S=100 УК, имеет следующие средние параметры:

– блок данных B=8·1000 бит;

– каждый УК генерирует K=100 блоков данных маршрутной информации;

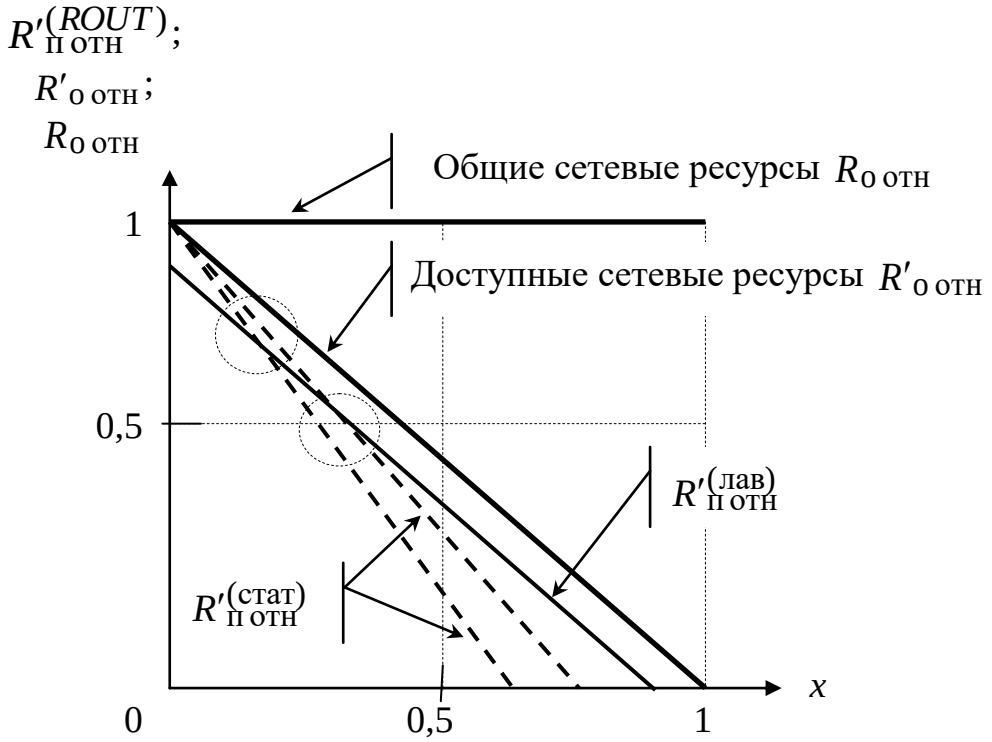


Рисунок 4.2 – Зависимости средних сетевых ресурсов от степени недоступности общих сетевых ресурсов МСС x для «Статистических» методов формирования ПРИ

– общий сетевой ресурс (суммарная пропускная способность всех каналов связи) равен R_0 =10 Мбит/с;

– интервал генерации маршрутной информации (зонд-сигналов) в сети «Лавинным» методом формирования ПРИ равен $\Delta t = 30$ с;

– сигнальная информация, генерируемая «Статистическим» методом формирования ПРИ, подчиняется линейному закону с постоянными коэффициентами a_0=0 и a_1=20 Мбит/с (ПРИ на сети задается администратором сети вручную).

Оценим объем пользовательских сетевых ресурсов $R_{\text{П}}$ (4.2), доступных пользователям для различных методов формирования ПРИ в условиях внешнего деструктивного воздействия $\Psi\_(t)$ (при степени недоступности общих сетевых ресурсов МСС $x = 0{,}1$ и $x = 0{,}5$).

Для «Лавинного» метода формирования ПРИ в соответствии с (4.6) составит:

при условии $x = 0{,}1$

$$R_{\text{П}}^{(\text{лав})} = (1-x)\cdot R_{\text{О}} - \frac{K\cdot B\cdot S}{\Delta t} = (1-0{,}1)\cdot 10^7 - \frac{100\cdot 1000\cdot 8\cdot 100}{30} = 6{,}33 \text{ Мбит/с;}$$

если $x = 0{,}5$

$$R_{\text{П}}^{(\text{лав})} = (1-x)\cdot R_{\text{О}} - \frac{K\cdot B\cdot S}{\Delta t} = (1-0{,}5)\cdot 10^7 - \frac{100\cdot 1000\cdot 8\cdot 100}{30} = 2{,}33 \text{ Мбит/с;}$$

Объем пользовательских сетевых ресурсов $R_{\text{П}}$ с применением «Статистического» метода формирования ПРИ (4.8) в зависимости от степени недоступности общих сетевых ресурсов МСС:

при $x = 0{,}1$

$$R_{\text{П}}^{(\text{стат})} = (1-x)\cdot R_{\text{О}} - a_1\cdot x = (1-0{,}1)\cdot 10^7 - 0{,}1\cdot 20 = 7 \text{ Мбит/с;}$$

при $x = 0{,}5$

$$R_{\text{П}}^{(\text{стат})} = (1-x)\cdot R_{\text{О}} - a_1\cdot x = (1-0{,}5)\cdot 10^7 - 0{,}5\cdot 20 = -5 \text{ Мбит/с.}$$

Знак минус означает, что при степени недоступности общих сетевых ресурсов МСС $x = 0{,}5$ объем средних сетевых ресурсов, необходимых для организации процедуры маршрутизации «Статистическим» методом, превышает общий объем сетевых ресурсов сети (пользовательские сетевые ресурсы отсутствуют). Это приводит к отказу передачи пользовательской информации. При этом «Лавинный» метод формирования ПРИ обеспечивает передачу пользовательской информации.

4.3 Разработка математической модели маршрутизации в условиях входного самоподобного трафика и внешних деструктивных воздействий на элементы мультисервисной сети связи

4.3.1 Разработка концепции логической структуры математической модели

На рисунке 4.3 представлена концепция математической модели для сопоставительного анализа маршрутизации в мультисервисной сети связи [7, 75, 78, 155, 156, 158].

Исходными данными являются:

– структура мультисервисной сети связи с множеством УК и ЛС;

– метод маршрутизации;

– входящий в МСС асинхронный поток пакетов различных приложений, доступных пользователям;

– степень тяготения узлов-источников к узлам-получателям для передачи пакетов сообщений ε-го приложения МСС;

– внешнее деструктивное воздействие на элементы мультисервисной сети связи.

Каждое приложение МСС характеризуется вероятностно-временными характеристиками (скорость передачи, время задержки, временной джиттер, вероятность ошибочного приема на символ, пакет, сообщение и многие другие). Не поддержание данных параметров (со стороны МСС) приводит к отказу в обслуживании данных приложений, следовательно, к снижению QoS мультисервисной сети связи. В этой связи обобщающим параметром качества функционирования МСС примем вероятность отказа в обслуживании, выбранных пользователями приложений.

Таким образом, критериями функционирования МСС примем:

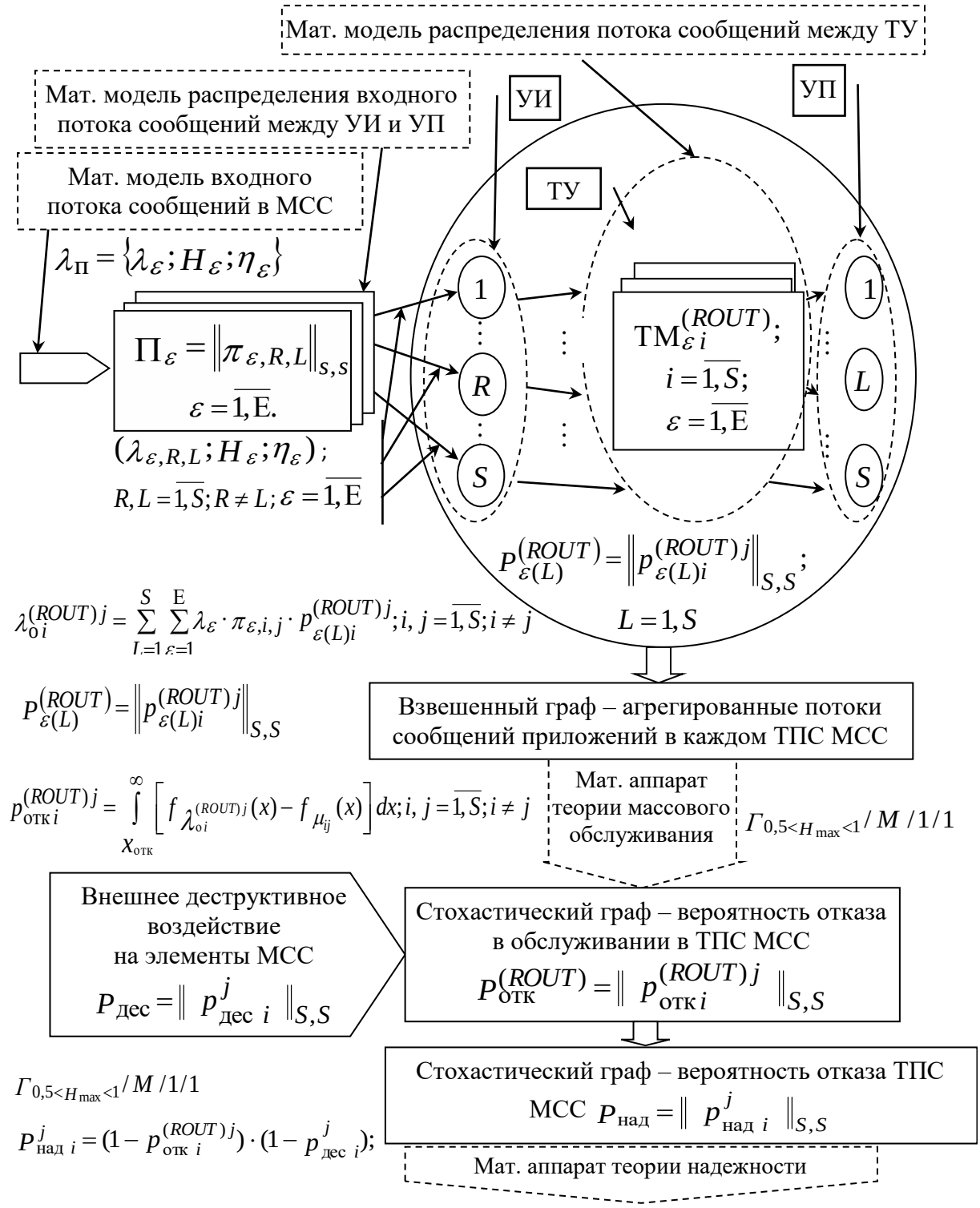


Рисунок 4.3 – Концепция математической модели маршрутизации в МСС

– вероятность отказа в обслуживании в целом по мультисервисной сети связи – интегральная оценка;

– вероятность отказа в обслуживании между каждой парой узел-источник и узел-получатель в мультисервисной сети связи – дифференциальная оценка.

Порядок определения искомых вероятностей следующий.

Входящий в МСС информационный поток пакетов сообщений ε-го приложения в соответствии со степенью тяготения узлов-источников к узлам получателям дезагрегируется на отдельные потоки, которые поступают в соответствующие УИ для последующей передачи в соответствующие УП.

В каждом тракте передачи сообщений формируются виртуальные каналы (ВК) и виртуальные тракты (ВТ) передачи сообщений. Это означает что, на канальном уровне МВОС в трактах передачи сообщений формируется асинхронный поток пакетов (Π_i) (рисунок 4.4) [80].

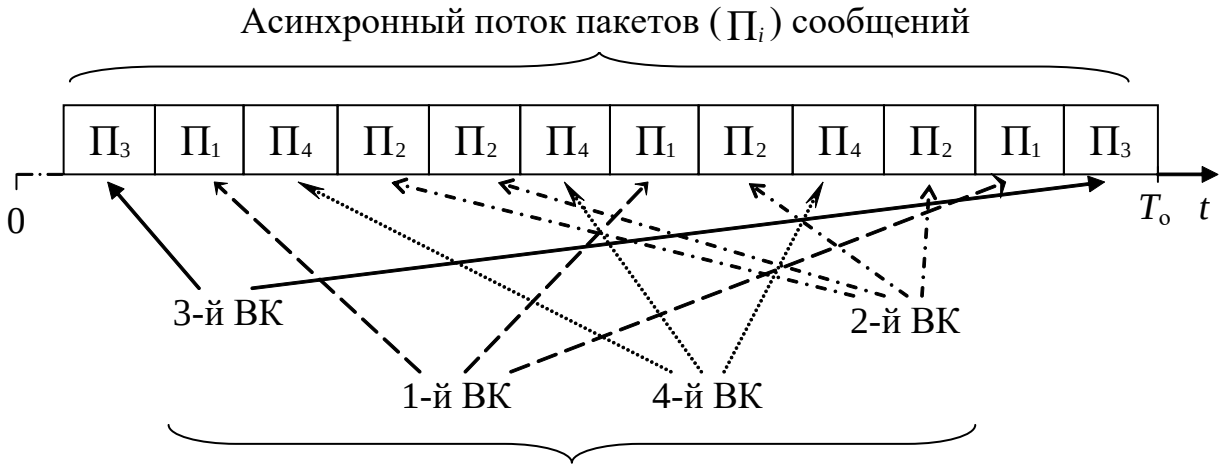


Рисунок 4.4 – Пример формирования ВК в одном ВТ за время наблюдения T_o

Подчиняясь заранее определенной процедуре маршрутизации, потоки сообщений различных приложений в каждом УК (УИ и транзитных узлах (ТУ)) распределяются по всем трактам передачи сообщений МСС. Далее, агрегируя распределенные потоки сообщений в каждом тракте, определяется суммарный поток каждого тракта передачи сообщений МСС. Учитывая, что ТПС обладает определенной пропускной способностью, то появляется возможность применить

аппарат теории массового обслуживания. А именно, определить вероятность отказа в обслуживании агрегируемого потока сообщений в каждом тракте МСС. В результате получаем стохастический граф, ребрам которого присвоены вероятности отказа обслуживания приложений МСС.

Внешнее деструктивное воздействие реализуется в заранее заданных вероятностях отказа ТПС мультисервисной сети связи. Если допустить, что вероятности отказа обслуживания приложений МСС в каждом ТПС и вероятности отказа самих ТПС (по причине внешних деструктивных воздействий) являются независимыми событиями, то данные вероятности перемножаются. В результате получаем новый стохастический граф, ребрам которого присвоены вероятности их отказа.

Далее используя математический аппарат теории надежностей, имеется возможность расчета искомых значений:

– вероятность отказа в обслуживании в целом по мультисервисной сети связи – интегральная оценка;

– вероятность отказа в обслуживании между каждой парой узел-источник и узел-получатель в мультисервисной сети связи – дифференциальная оценка.

Таким образом, изменяя:

– основные параметры МСС (структуру, пропускные способности ТПС);

– вероятностно-временные параметры (интенсивность поступления, плотность распределения) входящего в МСС информационного потока пакетов сообщений ε-го приложения;

– параметры внешнего деструктивного воздействия на МСС (вероятности выхода ТПС из строя),

имеется возможность провести сопоставительный анализ функционирования различных методов маршрутизации в МСС.

4.3.2 Формальное описание исходных данных математической модели маршрутизации в условиях самоподобного трафика

Формализуем исходные данные математической модели анализа маршрутизации в мультисервисной сети связи в условиях:

– входного самоподобного трафика;

– внешнего деструктивного воздействия на элементы мультисервисной сети связи.

1. Структуру мультисервисной сети связи представим в виде неориентированного графа $G[A_S, M_S]$ с множеством:

– вершин $A_S = \{a_i\}; i = \overline{1, S}$, соответствующих УК;

– ребер $M_S = \{m_{ij}\}; i, j = \overline{1, S}; i \neq j$, соответствующих трактам передачи сообщений.

Каждый ТПС характеризуется пропускной способностью $\mu_{ij}; i, j = \overline{1, S}; i \neq j$ – наибольшим количеством пакетов, передаваемых за единицу времени. В качестве допущения примем, что длительность обслуживания пакетов сообщений, поступающего асинхронного потока данных в ТПС между a_i и a_j УК $i, j = \overline{1, S}; i \neq j$ (рисунок 4.4) подчиняется экспоненциальному закону с параметром:

$$w_{ij} = \frac{1}{\mu_{ij}}; i, j = \overline{1, S}; i \neq j. \qquad (4.13)$$

2. Метод маршрутизации (3.14) $ROUT = \{ROUT_{\text{тм}} \uparrow ROUT_{\text{сс}}\}$ зададим процедурой выбора исходящих трактов передачи сообщений на множестве S пошаговых таблиц маршрутизации для ε-го приложения:

$$P_{\varepsilon}^{(j)} = \left\| p_{\varepsilon,i,\nu}^{(j)} \right\|_{(S-1),\chi_j} = \left(\overline{p_{\varepsilon,1}^{(j)}}, \ldots, \overline{p_{\varepsilon,i}^{(j)}}, \ldots, \overline{p_{\varepsilon,j-1}^{(j)}}, \overline{p_{\varepsilon,j+1}^{(j)}}, \ldots, \overline{p_{\varepsilon,S}^{(j)}} \right), \varepsilon = \overline{1,\mathrm{E}}, \qquad (4.14)$$

где

$$\overline{P_{\varepsilon,i}^{(j)}} = (p_{\varepsilon,i,\nu}^{(j)}); \sum_{\nu=1}^{\chi_j} p_{\varepsilon,i,\nu}^{(j)} = 1; \nu = \overline{1,\chi_j}; i, j = \overline{1,S};$$

χ_j – степень a_j-го УК.

Матрицей (4.14) по аналогии с (3.1) задается план распределения информации для ε-го приложения.

Элементы вектора $\overline{p_{\varepsilon,i}^{(j)}}$ определяют вероятность того, что для ε-го приложения на этапе поиска маршрута к a_j-му УП в a_i-м транзитном УК, начиная с УИ, будет выбрана ν-я исходящая ЛС.

3. Входящий в МСС информационный поток характеризуется интенсивностью ($\lambda_{\varepsilon,R,L}$) поступления пакетов сообщений ε-го приложения в a_R-й УИ для последующей передачи в a_L-й УП. До недавнего времени считалось, что интервалы времени между пакетами (заявками) ε-го приложения подчиняются Пуассоновскому закону распределения [10, 38, 45, 121] с параметром $\lambda_{\varepsilon,R,L}$. В работах [1, 32, 33, 65, 89 ÷ 94, 113, 141 ÷ 143, 171, 173, 175, ÷ 177] и многих других доказано, что периодически возникают моменты времени, в которых резко возрастает количество пакетов, поступающих в МСС. Причиной этого является использование пользователями высокоскоростных приложений, функционирующих в реальном масштабе времени, а так же зависимость количества пакетов сообщений на заданном интервале времени от предыдущих событий. Это означает, что трафик в МСС обладает эффектом самоподобия. Не учет этого обстоятельства на этапе проектирования ТКС приводит к переполнению буферов памяти коммутационного оборудования. В результате увеличивается время задержки передачи пакетов и вероятность их потери в сети.

Как правило, в математических моделях потоков сообщений в телекоммуникационных системах, учитывающих эффект самоподобия, используют субэкспоненциальные законы распределения: Вейбулла, гамма, логнормальное, гиперэкспоненциальное и Парето. Такие модели дают более точные результаты расчета размеров буферов памяти коммутационного оборудования.

Анализ результатов исследования статистических параметров трафика в сетях с технологией коммутации пакетов [32, 105, 141, 142] позволяет сделать следующие выводы по применению соответствующих распределений для моделирования:

– для интервалов между запросами к web-ресурсам, размеров передаваемых файлов, трафика VoIP – распределение Парето;

– для процессов поступления протокольных блоков FTP – распределение Вейбулла;

– для интервалов поступления пакетов в локальные вычислительные сети, времени между вызовами в Call-центрах – логнормальное распределение.

В работах [9, 29, 36, 92 ÷ 94, 176] предлагается использовать для входного потока пакетов в мультисервисную сеть связи гамма-распределение. Путем варьирования его параметров можно добиться практически любой степени самоподобия входного трафика.

Степень самоподобия классически оценивают с помощью параметра Херста H [89]. Многочисленные исследования [1, 9, 29, 36, 52, 89 ÷ 92, 105, 113, 141, 142] статистических параметров трафика показывают, что параметр Херста для различных приложений мультисервисных сетей связи находится в пределах:

$$0{,}5 < H < 1.$$

Таким образом, поступающий в a_R-й УИ мультисервисной сети связи информационный поток для последующей передачи в a_L-й УП будем характеризовать комбинацией параметров:

$$(\lambda_{\varepsilon,R,L}; H_\varepsilon; \eta_\varepsilon), \tag{4.15}$$

где:

H_ε – параметр Херста ε-го приложения;

η_ε – средняя длина пакетов сообщений ε-го приложения.

Плотность распределения вероятностей последовательности промежутков между вызовами поступления пакетов сообщений ε-го приложения в a_R-й УИ для последующей передачи в a_L-й УП определим выражением:

$$f(x) = \begin{cases} \dfrac{\lambda_{\varepsilon,R,L}^{H_\varepsilon} \cdot x^{H_\varepsilon - 1} \cdot e^{-\lambda_{\varepsilon,R,L} \cdot x}}{\Gamma(H_\varepsilon)}; R, L = \overline{1,S}; R \neq L; \varepsilon = \overline{1,\mathrm{E}}; x \geq 0; \\ 0, \qquad\qquad x < 0, \end{cases} \tag{4.16}$$

где

$$\Gamma(H_\varepsilon) = \int_0^\infty x^{H_\varepsilon - 1} \cdot e^{-x} dx$$

гамма-функция.

В работах [1, 113, 175, 177] получены результаты, утверждающие, что при агрегировании самоподобных потоков результирующий поток будет тоже самоподобным с параметрами:

$$H = \max_i (H_i); i = \overline{1,N}; \lambda = \sum_{i=1}^{N} \lambda_i. \tag{4.17}$$

Следовательно, интенсивность потока данных ε-го приложения, поступающего в МСС, составит:

$$\lambda_{\varepsilon} = \sum_{R,L=1}^{S} \lambda_{\varepsilon,R,L}.$$

4. Вероятность поступления потока данных ε-го приложения в a_R-й УИ для его последующей передачи a_L-му УП определяется матрицей тяготений:

$$\Pi_{\varepsilon} = \left\| \pi_{\varepsilon,R,L} \right\|_{S,S},$$

где

$$0 \le \pi_{\varepsilon,R,L} = \frac{\lambda_{\varepsilon,R,L}}{\lambda_{\varepsilon}} \le 1; \sum_{R,N=1}^{S} \pi_{\varepsilon,R,L} = 1; \varepsilon = \overline{1,\mathrm{E}}.$$

5. Внешнее деструктивное воздействие на элементы МСС представим в виде матрицы:

$$P_{\text{дес}} = \| \ p^{j}_{\text{дес } i} \ \|_{S,S},$$

где

$p^{j}_{\text{дес } i}$ – вероятность выхода из строя ребра $m_{i,j}$ исходного графа $G[A_S, M_S]$, описывающего структуру мультисервисной сети связи.

Критериями оценки функционирования МСС примем:

$$\{\hat{P}_{\text{отк}}; \hat{p}^{(R,L)}_{\text{отк}}\} = f\{G[A_S, M_S]; \Pi_{\varepsilon}; \lambda_{\varepsilon}; H_{\varepsilon}; \mu; ROUT; P_{\text{дес}}\}; R, L = \overline{1,L}; R \ne L; \varepsilon = \overline{1,\mathrm{E}}, \quad (4.18)$$

где

$\hat{P}_{\text{отк}}$ – вероятность отказа в обслуживании в целом по сети – интегральная оценка;

$\hat{P}_{\text{отк}}^{(R,L)}; R,T=\overline{1,L}; R\neq L$ – вероятность отказа в обслуживании между УИ (a_R) и УП (a_L) – дифференциальная оценка.

4.3.3 Разработка математической модели распределения потока сообщений между транзитными узлами мультисервисной сети связи

Отождествим вершины графа (сети) $G[A_S, M_S]$ с состояниями конечной цепи Маркова. Из набора векторов (4.14) для метода маршрутизации $ROUT$ и ε-го приложения МСС при поиске a_L-го УК можно получить матрицу переходных вероятностей [77, 80]:

$$P_{\varepsilon(L)}^{(ROUT)} = \left\| p_{\varepsilon(L)i}^{(ROUT)j} \right\|_{S,S} i, j = \overline{1,S},$$

где $p_{\varepsilon(L)i}^{(ROUT)j}; i, j = \overline{1,S}$ – вероятность перехода из состояния a_i в a_j конечной цепи Маркова для метода маршрутизации $ROUT$ и ε-го приложения МСС при поиске a_L-го УК. Причем состояние a_L, соответствующее a_L-му УК (УП), определим поглощающим, т.е.

$$P_{\varepsilon(L)L}^{(ROUT)L} = 1.$$

Матрица переходных вероятностей, описывающая вероятности переходов для поиска a_L-го УК при методе маршрутизации $ROUT$ и ε-м приложении МСС, будет иметь вид:

$$\begin{array}{c|cccccc|}
 & 1 & \cdots & L & \cdots & (S-1) & S \\
1 & 0 & \cdots & p_{\varepsilon(L)\ 1}^{(ROUT)L} & \cdots & p_{\varepsilon(L)\ 1}^{(ROUT)S-1} & p_{\varepsilon(L)\ 1}^{(ROUT)S} \\
\vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \vdots \\
L & 0 & \cdots & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \vdots \\
S-1 & p_{\varepsilon(L)\ S-1}^{(ROUT)1} & \cdots & p_{\varepsilon(L)\ S-1}^{(ROUT)L} & \cdots & 0 & p_{\varepsilon(L)\ S-1}^{(ROUT)S} \\
S & p_{\varepsilon(L)\ S}^{(ROUT)1} & \cdots & p_{\varepsilon(L)\ S}^{(ROUT)L} & \cdots & p_{\varepsilon(L)\ S}^{(ROUT)S-1} & 0
\end{array}. \quad (4.19)$$

Интенсивность потоков в ТПС $m_{ij}; i, j = \overline{1,S}; i \neq j$ при поиске a_L-го УК, методе маршрутизации $ROUT$ и ε-м приложении МСС составит:

$$\lambda_{\varepsilon(L)i}^{(ROUT)j} = p_{\varepsilon(L)i}^{(ROUT)j} \cdot \lambda_{\varepsilon,i,L}; i, j = \overline{1,S}; i \neq j,$$

причем из свойства конечных цепей Маркова (с учетом 4.17) имеем:

$$\lambda_{\varepsilon,i,L} = \sum_{j=1}^{S} \lambda_{\varepsilon(L)i}^{(ROUT)j}; i, j = \overline{1,S}; i \neq j.$$

Общие интенсивности потоков всех $\varepsilon = \overline{1,\mathrm{E}}.$ приложений в ТПС $m_{i,j}; i, j = \overline{1,S}; i \neq j$ при заданном методе маршрутизации $ROUT$ определятся из системы уравнений:

$$\lambda_{\mathrm{o}\,i}^{(ROUT)j} = \sum_{L=1}^{S}\sum_{\varepsilon=1}^{\mathrm{E}} \lambda_{\varepsilon(L)i}^{(ROUT)j} = \sum_{L=1}^{S}\sum_{\varepsilon=1}^{\mathrm{E}} p_{\varepsilon(L)i}^{(ROUT)j} \cdot \lambda_{\varepsilon,i,L}; i, j = \overline{1,S}; i \neq j$$

или

$$\lambda_{\mathrm{o}\,i}^{(ROUT)j} = \sum_{L=1}^{S}\sum_{\varepsilon=1}^{\mathrm{E}} \lambda_{\varepsilon} \cdot \pi_{\varepsilon,i,j} \cdot p_{\varepsilon(L)i}^{(ROUT)j}; i, j = \overline{1,S}; i \neq j, \quad (4.20)$$

где

λ_ε – интенсивность поступления потока данных ε-го приложения в МСС;

$\pi_{\varepsilon,i,j}$ – элемент матрицы тяготений Π_ε;

$p_{\varepsilon(L)\,i}^{(ROUT)\,j}$ – элемент матрицы переходных вероятностей $P_{\varepsilon(L)}^{(ROUT)}$.

В результате получаем взвешенный граф, каждому ребру которого присвоены агрегированные потоки сообщений всех E приложений:

$$\lambda_{\text{o}}^{(ROUT)} = \| \lambda_{\text{o}\,i}^{(ROUT)\,j} \|_{S,S}. \qquad (4.21)$$

Так как входящие информационные потоки в мультисервисную сеть связи подчиняются гамма-распределению с параметрами $(\lambda_{\varepsilon,R,L}; H_\varepsilon; \eta_\varepsilon)$, то с учетом (4.17) можно утверждать, что и агрегированные потоки сообщений (4.21) тоже подчиняются гамма-распределению. При этом параметр Херста выбирается максимальным из всех $H_\varepsilon; \varepsilon = \overline{1,\text{E}}$.

Принятое ограничение (4.13) (экспоненциальный закон распределения длительности обслуживания пакетов сообщений) с параметром

$$w_{ij} = \frac{1}{\mu_{ij}}; i, j = \overline{1,S}; i \neq j,$$

позволяет для расчета вероятности отказа в обслуживании агрегированных потоков сообщений (4.21) в ТПС между a_i и a_j УК воспользоваться математическим аппаратом теории массового обслуживания.

Каждое ребро графа (4.21) в обозначениях Кендалла представим как $\Gamma_{0,5<H_{\max}<1}/M/1/1$. Здесь $\Gamma_{0,5<H_{\max}<1}$ – обозначение гамма-распределения (с параметром Херста $0,5 < H_{\max} < 1$ и интенсивностью $\lambda_{\text{o}\,i}^{(ROUT)\,j}; i, j = \overline{1,S}; i \neq j$) случайной длины интервала между соседними требованиями входного потока;

M – экспоненциальная функция распределения случайного времени обслуживания агрегированных потоков сообщений с параметром:

$$w_{ij} = \frac{1}{\mu_{ij}}; i, j = \overline{1,S}; i \neq j.$$

Из графического представления плотности распределения случайной длины интервала между соседними требованиями входного потока ($f_{\lambda_{\text{o}i}^{(ROUT)j}}(x)$) и плотности распределения случайного времени обслуживания агрегированных потоков сообщений ($f_{\mu_{ij}}(x)$) (рисунок 4.5) определим общее выражение вероятности отказа в обслуживании агрегированных потоков сообщений (4.21) в ТПС между a_i и a_j УК:

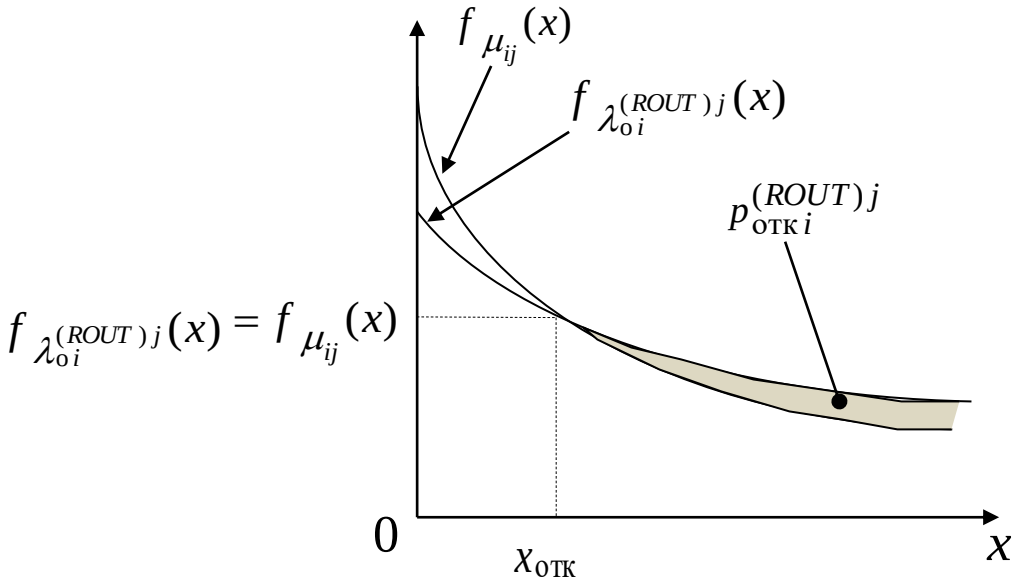


Рисунок 4.5 – Графическое определение общего выражения вероятности отказа в обслуживании агрегированных потоков сообщений в ТПС

$$p_{\text{отк}i}^{(ROUT)j} = \int_{x_{\text{отк}}}^{\infty} \left[f_{\lambda_{\text{o}i}^{(ROUT)j}}(x) - f_{\mu_{ij}}(x) \right] dx; i, j = \overline{1,S}; i \neq j. \qquad (4.22)$$

Окончательно получим:

$$p_{\text{отк } i}^{(ROUT)j} = \int\limits_{x_{\text{отк}}}^{\infty} \left[\frac{\lambda_{\text{o}\,i}^{(ROUT)} H_{\max j} \cdot x^{H_{\max}-1} \cdot e^{-\lambda_{\text{o}\,i}^{(ROUT)j \cdot x}}}{\int\limits_{0}^{\infty} x^{H_{\max}-1} \cdot e^{-x} dx} - \mu_{ij} e^{-\mu_{ij} \cdot x} \right] dx; i, j = \overline{1,S}; i \neq j. \quad (4.23)$$

Для практических исследований воспользуемся результатом работы [92], в которой искомая вероятность отказа в обслуживании получена для случая $\Gamma_{0,5}/M/1/N$:

$$p = \frac{\left(1 - \frac{\rho}{4} - \sqrt{\frac{\rho^2}{16} + \frac{\rho}{2}}\right)}{1 - \left(\frac{\rho}{4} + \sqrt{\frac{\rho^2}{16} + \frac{\rho}{2}}\right)^{N+1}} \left(\frac{\rho}{4} + \sqrt{\frac{\rho^2}{16} + \frac{\rho}{2}}\right), N$$

где $\rho = \frac{\lambda}{\mu}$; λ – интенсивность поступления заявок на входе системы массового обслуживания (СМО); μ – производительность обслуживающей линии СМО.

Таким образом, вероятность отказа в обслуживании агрегированных потоков сообщений в ТПС между a_i и a_j УК будем определять следующим образом:

$$p_{\text{отк}\,i}^{(ROUT)j} = \frac{\left(1 - \frac{\rho_i^{(ROUT)j}}{4} - \sqrt{\frac{\rho_i^{(ROUT)j\ 2}}{16} + \frac{\rho_i^{(ROUT)j}}{2}}\right)}{1 - \left(\frac{\rho_i^{(ROUT)j\ 2}}{4} + \sqrt{\frac{\rho_i^{(ROUT)j\ 2}}{16} + \frac{\rho_i^{(ROUT)j}}{2}}\right)^2} \times$$

$$\times\left(\frac{\rho_i^{(ROUT)J}}{4}+\sqrt{\frac{\rho_i^{(ROUT)j\ 2}}{16}+\frac{\rho_i^{(ROUT)j}}{2}}\right);i,\ j=\overline{1,S};i\neq j.$$

В результате получим стохастический граф, ребрам которого присвоены вероятности отказа в обслуживании в каждом ТПС для всех $\varepsilon=\overline{1,\mathrm{E}}.$ приложений МСС:

$$P_{\text{отк}}^{(ROUT)}=\|\ p_{\text{отк}\ i}^{(ROUT)j}\ \|_{S,S}. \tag{4.24}$$

Допустим, что внешнее деструктивное воздействие на элементы МСС и вероятности событий (4.24) являются независимыми. Тогда вероятности надежности ТПС МСС определим следующим образом:

$$P_{\text{над}\ i}^{j}=(1-p_{\text{отк}\ i}^{(ROUT)j})\cdot(1-p_{\text{дес}\ i}^{j});i,\ j=\overline{1,S};i\neq j. \tag{4.25}$$

В результате имеем стохастический граф, ребрам которого присвоены вероятности надежности всех ТПС МСС:

$$P_{\text{над}}=\|\ p_{\text{над}\ i}^{j}\ \|_{S,S}. \tag{4.26}$$

Далее, используя математический аппарат теории надежности [6, 21, 28 35, 62, 81, 85, 95, 96, 102], появляется возможность определить искомые значения (4.18). Для этого воспользуемся методом полного перебора оценки структурной надежности телекоммуникационной системы.

Пронумеруем элементы множества $M=\{m_{ij}\};i,\ j=\overline{1,S};i\neq j$ числами натурального ряда $M=\{m_{ij}\}=\{m_{\upsilon}\};i,\ j=\overline{1,S};i\neq j;\varphi=\overline{1,\kappa}.$ Каждое ребро анализируемого графа может находиться в двух состояниях:

$$\begin{cases} \sigma_\varphi = 1 \ (m_{ij} \text{ исправно}) \text{ с вероятностью } p_\varphi = p^j_{\text{над}\,i}; i, j = \overline{1,S}; i \neq j; \varphi = \overline{1,\kappa}; \\ \sigma_\varphi = 0 \ (m_{ij} \text{ вышло из строя}) \text{ с вероятностью } q_\varphi = 1 - p_\varphi. \end{cases}$$

В этом случае анализируемый граф может находиться в одном из $k = \overline{1,2^\kappa}$ состояний. Вероятность каждого из возможных состояний графа определяется:

$$p_k = \prod_{\varphi=1}^{\kappa} p_\varphi^{\sigma_\nu} \cdot q_\varphi^{1-\sigma_\varphi}; k = \overline{1,2^\kappa}.$$

Введем переменные:

$$Q_o^{(k)} = \begin{cases} 1, \text{если граф, находясь в } k \text{ - м состояни, связен;} \\ 0, \text{ в противном случае;} \end{cases}$$

$$Q_{ij}^{(k)} = \begin{cases} 1, \text{если граф, находясь в } k \text{ - м состоянии,} \\ \quad \text{обеспечивает связность вершин } a_i \text{ и } a_j; \\ 0, \text{в противном случае.} \end{cases}$$

В результате функционал (4.18) определяется выражениями:

$$\hat{p}_{\text{отк}}^{(R,L)} = 1 - \sum_{k=1}^{2^\kappa} Q_{RL}^{(k)} \cdot p_k = 1 - \sum_{k=1}^{2^\kappa} Q_{RL}^{(k)} \cdot \Big(\prod_{\varphi=1}^{\kappa} p_\varphi^{\sigma_\varphi} \cdot q_\varphi^{1-\sigma_\varphi} \Big); R, L = \overline{1,S}; \qquad (4.27)$$

$$\hat{P}_{\text{отк}} = 1 - \sum_{k=1}^{2^\kappa} Q_o^{(k)} \cdot p_k = 1 - \sum_{k=1}^{2^\kappa} Q_o^{(k)} \prod_{\varphi=1}^{\kappa} p_\varphi^{\sigma_\varphi} \cdot q_\varphi^{1-\sigma_\varphi}. \qquad (4.28)$$

Таким образом, методика математического моделирования маршрутизации в мультисервисных сетях связи состоит в решении следующей системы уравнений:

$$
\begin{cases}
P_{\varepsilon(L)}^{(ROUT)} = \left\| P_{\varepsilon(L)i}^{(ROUT)\,j} \right\|_{S,S} i, j = \overline{1,S}; \\
\lambda_{\text{o}\,i}^{(ROUT)\,j} = \sum_{L=1}^{S} \sum_{\varepsilon=1}^{\text{E}} \lambda_{\varepsilon} \cdot \pi_{\varepsilon,i,j} \cdot p_{\varepsilon(L)i}^{(ROUT)\,j}; i, j = \overline{1,S}; i \neq j; \\
p_{\text{отк}\;i}^{(ROUT)\,j} = \int\limits_{x_{\text{отк}}}^{\infty} \left[\dfrac{\lambda_{\text{o}\,i}^{(ROUT)} H_{\max\,j} \cdot {}_{x}H_{\max}{}^{-1} \cdot e^{-\lambda_{\text{o}\,i}^{(ROUT)\,j \cdot x}}}{\int\limits_{0}^{\infty} {}_{x}H_{\max}{}^{-1} \cdot e^{-x} dx} - \mu_{ij} e^{-\mu_{ij} \cdot x} \right] dx; i, j = \overline{1,S}; i \neq j; \\
P_{\text{над}\;i}^{j} = (1 - p_{\text{отк}\;i}^{(ROUT)\,j}) \cdot (1 - p_{\text{дес}\;i}^{j}); i, j = \overline{1,S; i \neq j}; \\
\hat{p}_{\text{отк}}^{(R,L)} = 1 - \sum_{k=1}^{2^{\kappa}} Q_{RL}^{(k)} \cdot p_k = 1 - \sum_{k=1}^{2^{\kappa}} Q_{RL}^{(k)} \cdot \left(\prod_{\varphi=1}^{\kappa} p_{\varphi}^{\sigma_{\varphi}} \cdot q_{\varphi}^{1-\sigma_{\varphi}} \right); R, L = \overline{1,S}; \\
\hat{P}_{\text{отк}} = 1 - \sum_{k=1}^{2^{\kappa}} Q_{o}^{(k)} \cdot p_k = 1 - \sum_{k=1}^{2^{\kappa}} Q_{o}^{(k)} \prod_{\varphi=1}^{\kappa} p_{\varphi}^{\sigma_{\varphi}} \cdot q_{\varphi}^{1-\sigma_{\varphi}}.
\end{cases}
\tag{4.29}
$$

4.3.3.1 Оценка структурной надежности сети связи методом статистического моделирования

Составление формул (4.27) и (4.28) для конкретных структур сетей связи и последующее их решение является (в общем случае) практически единственным точным численным методом оценки величины надежности всего стохастического графа и между произвольной парой вершин.

Однако составление аналитических выражений в первом случае и решение во втором – исключительно трудоемкие процессы, так как в их основе лежит перебор всех состояний анализируемого графа.

В работах [81, 102, 115] приведен достаточно большой обзор аналитических методов оценки структурной надежности сети связи. Каждый из них имеет свои преимущества и недостатки.

Возможность применения того или иного метода определяется типом и размерностью анализируемой системы, а также требуемой точностью анализа.

Для оценки структурной надежности телекоммуникационной системы большой размерности наиболее приемлемым остается метод статистического моделирования [6, 13, 21, 35, 62, 81, 85, 96].

Осуществляют N_o независимых испытаний, каждое из которых состоит из двух этапов.

На первом этапе вырабатывают κ независимых случайных равномерно распределенных в интервале (0,1) чисел X_φ. Затем значения X_φ последовательно сравнивают с величинами надежностей p_φ каждого элемента графа, описывающего структуру анализируемой сети, по следующему правилу:

$$\begin{cases} \text{если } X_\varphi \geq p_\varphi \Rightarrow \text{элемент графа считается выведеным из строя;} \\ \text{если } X_\varphi < p_\varphi \Rightarrow \text{элемент графа находится в исправном состоянии.} \end{cases} \quad (4.30)$$

Второй этап – проверка графа, полученного в результате выхода его элементов из строя, на связность. Если граф связен, то исход испытания относится к числу благоприятных. Отношение числа благоприятных исходов к общему числу испытаний N_o и будет оценкой структурной надежности графа.

Абсолютная погрешность результата вычисления определяется формулой:

$$\Delta_a = N_o^{-0,5} \cdot \sigma \cdot t_\beta, \quad (4.31)$$

где

Δ_a – абсолютное значение ошибки (половина доверительного интервала);

σ – среднеквадратичное отклонение от искомой величины $\hat{p}_{\text{отк}}^{(R,L)}$ или $\hat{P}_{\text{отк}}$;

$$\sigma^2 = \hat{P}_{\text{отк}} \cdot (1 - \hat{P}_{\text{отк}}) \text{ или } \sigma^2 = \hat{P}_{\text{отк}}^{(R,L)} \cdot (1 - P_{\text{отк}}^{(R,L)});$$

β – достоверность полученной оценки;

t_β – функция, обратная нормальной при аргументе $(1+\beta)^{-1}$.

Из (4.31) можно сделать вывод о скорости сходимости метода статистического моделирования – для практических целей эта скорость совершенно неудовлетворительная. Действительно, уменьшение погрешности на порядок приводит к увеличению количества испытаний на два порядка. Одновременно с этим выделяется, во-первых, та область, где применение данного метода наиболее целесообразно – это область невысоких точностей решений, здесь метод статистического моделирования составляет несомненную конкуренцию классическим аналитическим методам. Во-вторых, просматриваются и пути повышения эффективности метода путем построения таких вероятностных моделей, которые характеризовались бы минимальной дисперсией оцениваемых функционалов.

Таким образом, сокращение времени, затрачиваемого ЭВМ на решение задачи, можно обеспечить двумя путями:

– разработкой методов, позволяющих уменьшить количество испытаний с сохранением точности результатов моделирования;

– разработкой алгоритмов меньшей сложности для оценки структурной надежности сети связи.

Решение первой проблемы связано с уменьшением дисперсии оценок результатов моделирования. Во втором случае необходимо разработать алгоритмы для проверки графа на связность меньшей сложности.

4.3.3.2 Уменьшение дисперсии оценок результатов моделирования

Вероятность того, что граф окажется связен (в одном из испытаний статистического моделирования), существенным образом зависит от величины p_φ. Если всем элементам графа задать одинаковые величины p_φ, то при большом количестве N_o число элементов графа, которое будет выходить из строя, в среднем будет равно целому $[(1-p_\varphi)\cdot 100]$ от общего числа элементов графа. Таким образом, можно утверждать, что если вместо операции (4.30) на первом этапе каждого испытания выводить из строя случайным образом ровно $[(1-p_\varphi)\cdot 100]$ от общего количества элементов графа, то тем самым уменьшится дисперсия наступления события "граф связен" [78, 86].

Покажем это следующим образом.

Пусть:

$$p = p_\varphi; 0 \le p_\varphi \le 1; \nu = \overline{1,\kappa};$$

$$q = 1 - p;$$

I_q – есть целое от $[q\cdot 100]$;

выходы элементов графа из строя являются независимыми событиями.

Тогда вероятность наступления события, что при j-м испытании ($j = \overline{1, N_o}$) из строя будет выведено ровно I_q элементов графа, определяется частной теоремой о повторении опытов и равна:

$$P_{I_q}^{(j)} = C_n^{I_q} \cdot P^{I_q} \cdot q^{(S-I_q)}. \qquad (4.32)$$

Дисперсия $P_{I_q}^{(j)}$ составит:

$$\sigma_{I_q}^{(j)^2} = P_{I_q}^{(j)} \cdot (1 - P_{I_q}^{(j)}). \tag{4.33}$$

Подставив (4.32) и (4.33) в (4.31), определим то количество испытаний, которое необходимо выполнить, чтобы с заданной погрешностью было выведено из строя ровно I_q элементов сети:

$$N_{oI_q}^{(j)} = \{C_n^{I_q} \cdot P^{I_q} \cdot q^{(S-I_q)} \cdot [1 - C_n^{I_q} \cdot P^{I_q} \cdot q^{(S-I_q)}]\} \cdot t_\beta^2 \cdot \Delta_a^{-2}. \tag{4.34}$$

Таким образом, применяя предложенный подход, достаточно выполнить

$$\Lambda = N_o - N_{oI_q}^{(j)} \tag{4.35}$$

испытаний, чтобы получить результат оценки с сохранением абсолютной погрешности вычислений.

Данный подход имеет ограничение. Его применение возможно в сетях, элементы которого имеют одинаковые параметры надежности.

Приведем пример. В работе [28] представлены результаты расчета структурной надежности транспортной сети для различных структур (радиально-узловая, кольцевая и т.д.). В каждом варианте структур коэффициенты готовности для всех ЛС выбирались одинаковыми и изменялись в некоторых пределах. Розыгрыш состояний элементов анализируемой сети осуществлялся по алгоритму (4.30). Количество испытаний рассчитывалось с достоверностью $\beta = 0{,}95$. Обратимся к рисунку 3 работы [28, стр. 58]. На графике варианта 2 (кольцевая структура) выберем точку, соответствующую параметрам: $K_{\Gamma ij} = 0{,}5$ (в наших обозначениях $p = p_\varphi = 0{,}5; 0 \le p_\varphi \le 1; \varphi = \overline{1,\kappa}; \kappa = 10$); $M_{\text{ОТН}}^*(X) = 60$ (в наших

обозначениях $\hat{P}_{\text{отк}} = 0{,}6$). Допустим, что расчеты проводились с абсолютной погрешностью $\Delta_a = 0{,}01$.

Таким образом, подставляя в формулу (4.31) исходные данные $\hat{P}_{\text{отк}} = 0{,}6$; $\beta = 0{,}95$; $t_\beta = 1{,}96$; $\Delta_a = 0{,}01$, получим необходимое количество испытаний $N_o = 9220$ для одной точки кривой.

Теперь проведем расчет необходимого количества испытаний с использованием предлагаемого подхода. Подставим в формулу (4.34) исходные данные: $I_q = 5$ ($p = p_\varphi = 0{,}5$) ; $n = 10$; $t_\beta = 1{,}96$; $\Delta_a = 0{,}01$). Получим $N_{oI_q}^{(j)} = 7145$. В результате для обеспечения абсолютной погрешности $\Delta_a = 0{,}01$ результатов счета достаточно выполнить всего $\Lambda = N_o - N_{oI_q}^{(j)} = 2075$ испытаний.

4.3.3.3 Анализ и разработка методов проверки графа сети на связность

При оценке структурной надежности сети связи в каждом испытании статистического моделирования выполняется процедура проверки графа на связность, на которую тратится основное время ЭВМ от общего объема. Таким образом, сокращение времени ЭВМ на величину $\Delta\tau_{\text{св}}$ для проверки графа на связность в одном испытании дает сокращение времени ЭВМ на оценку структурной надежности сети связи на $(N_{\text{о}} \cdot \Delta\tau_{\text{св}})$.

Проведем сопоставительный анализ известных методов проверки графа на связность с позиций их вычислительной сложности.

Метод «Разрастания» [112] состоит в следующем. На графе выбирается произвольная вершина. Поочередно выписываются смежные вершины. Выписываются новые вершины, которые соединены ребрами хотя бы с одной из уже выписанных вершин. Если по окончании указанной процедуры остались не

выписанными некоторые вершины, то это и указывает на несвязность анализируемого графа.

В работе [21] рассмотрен вариант данного метода, который состоит в представлении процедур, участвующих в проверке графа на связность в векторной форме, что весьма удобно при его реализации. При этом анализируемый граф представляется в виде матрицы смежности порядка *S*:

$$A_S = \left\| a_{ij} \right\|_{S,S} = \left| \overline{a_1}, \ldots, \overline{a_i}, \ldots, \overline{a_S} \right|^T, \tag{4.36}$$

где $\overline{a_i}$ – вектор-строка матрицы; *S* – число вершин в графе.

Процедура проверки графа на связность состоит в последовательном выполнении логического сложения и двух логических умножений векторов-строк $\overline{a_i} = (a_{i1}, \ldots, a_{ij}, \ldots, a_{is})$ матрицы (4.36).

Учитывая, что все действия при проверке графа на связность проводят на матрице смежности (4.36), вычислительная сложность метода «Разрастания» определяется как:

$$Q_{\text{раз}} = f\left(\chi \cdot S^2\right).$$

Здесь A – коэффициент, определяющий основные логические процедуры с вектор-строками (4.36).

В методе ***«Поиск в глубину»*** [100], по аналогии с методом «Разрастания», на первом этапе выбирается произвольная вершина. В вершине выбирается ребро, соединяющее данную вершину со смежной вершиной. Вершины (первоначально выбранная и смежная) и ребро запоминаются. В смежной вершине процедура выбора ребра повторяется. При этом ставится условие: выбор ребра, по которому поиск пришел в данную вершину, осуществляется последним. В первую очередь выбирается любое из ребер, соединяющих ранее не просмотренные вершины.

Таким образом, «Поиск в глубину» последовательно проходит по всем ребрам дважды, попадает во все возможные вершины и возвращается в первоначально выбранную вершину. По окончании процедуры «Поиска в глубину» производят сравнение числа просмотренных вершин с реальным числом вершин анализируемого графа. Если числа совпадают, то граф связен. В противном случае граф несвязен.

В случае представления анализируемого графа в виде матрицы (4.36) вычислительная сложность метода определяется:

$$Q_{\text{гл}} = f\left(2 \cdot \kappa \cdot S^2\right).$$

Здесь κ – число ребер в анализируемом графе. В случае

$$\kappa = \frac{\chi}{2} \cdot S$$

вычислительная сложность метода «Поиск в глубину» определяется как:

$$Q_{\text{гл}} = f\left(\chi \cdot S^3\right),$$

где χ – средняя степень вершины анализируемого графа.

Метод «Свертки» [5, 79] состоит в том, что выполняют одновременное «Соединение» смежных вершин к произвольно выбранной вершине до тех пор, пока граф не представится в виде «Одиночной» вершины (если граф связен, рисунок 4.6) или множества вершин (граф несвязен, рисунок 4.7).

Для пояснения вычислительной сложности метода «Свертки» вложим анализируемый граф в прямоугольную систему координат (рисунок 4.8).

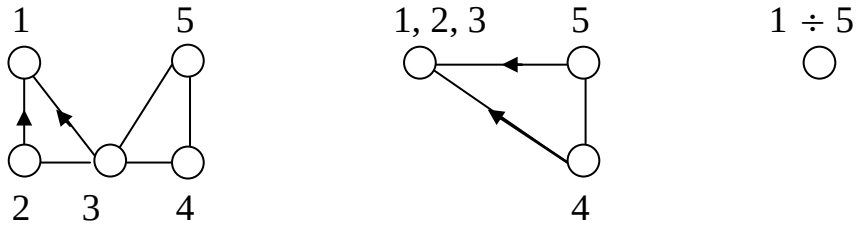
Предположим, что количество вершин по осям *X* и *Y* равно между собой и равно целой положительной величине *L*. Конечно, едва ли следует ожидать, что

реальный граф будет иметь структуру с квадратной ячейкой. Однако оценки, полученные для данной ситуации, дадут представление о вычислительной сложности метода проверки графа на связность.

Общее число вершин в графе будет равно $S = L^2$. В данном случае методу «Свертки» достаточно выполнить $L - 1 = \sqrt{S} - 1$ итераций для определения связности графа. Процедура одновременного «Соединения» смежных вершин к произвольно выбранной вершине сводится к логической операции конъюнкция векторов-строк матрицы смежности (4.36).

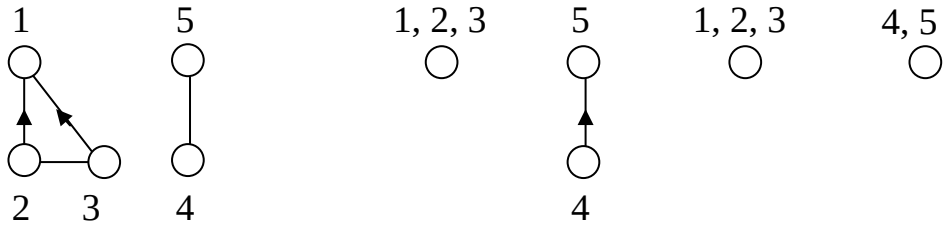
Вычислительная сложность метода «Свертки»:

$$Q_{\text{св}} = f\{\chi \cdot S \cdot (\sqrt{S} - 1)\}.$$



Исходный граф 1 шаг «Свертки» | 2 шаг «Свертки» | 3 шаг «Граф связен»

Рисунок 4.6 – Пример проверки связного графа методом «Свертки»



Исходный граф 1 шаг | 2 шаг | 3 шаг

Рисунок 4.7 – Пример проверки несвязного графа методом «Свертки»

Метод «Разбиения» [61, 76, 79]. Суть данного метода состоит в том, что анализируемый граф разбивают на подграфы, каждый из которых отдельно проверяют на связность методом «Свертка». В результате получают новый граф –

«Суперграф», который в свою очередь проверяют на связность. Если «Суперграф» связен, то делают вывод, что исходный граф связен. В противном случае считают, что граф не связен.

Допустим, что граф (рисунок 4.8) разбивают на N равных подграфов. Колличество итераций методом «Свертка» для определения связности одного подграфа составит:

$$\frac{L}{\sqrt{N}} - 1 = \frac{\sqrt{S}}{\sqrt{N}} - 1.$$

Вычислительная сложность проверки одного подграфа методом «Свертка» составит:

$$Q_{\text{св}}^{(1)} = f\left[\frac{S}{N}\chi \cdot \left(\sqrt{\frac{L}{N}} - 1\right)\right].$$

Вычислительная сложность проверки всех N подграфов методом «Свертка» будет определяться выражением:

$$Q_{\text{св}}^{(N)} = f\left[N \cdot \frac{S}{N}\chi \cdot \left(\sqrt{\frac{L}{N}} - 1\right)\right].$$

Учитывая проверку на связность «Суперграфа», размерность которого равна N, получим оценку вычислительной сложности исходного графа методом «Разбиения»:

$$Q_{\text{раз}} = f\left\{\left[S \cdot \chi \cdot \left(\frac{\sqrt{S}}{\sqrt{N}} - 1\right)\right] + N \cdot \chi \cdot \left(\sqrt{N} - 1\right)\right\}. \quad (4.37)$$

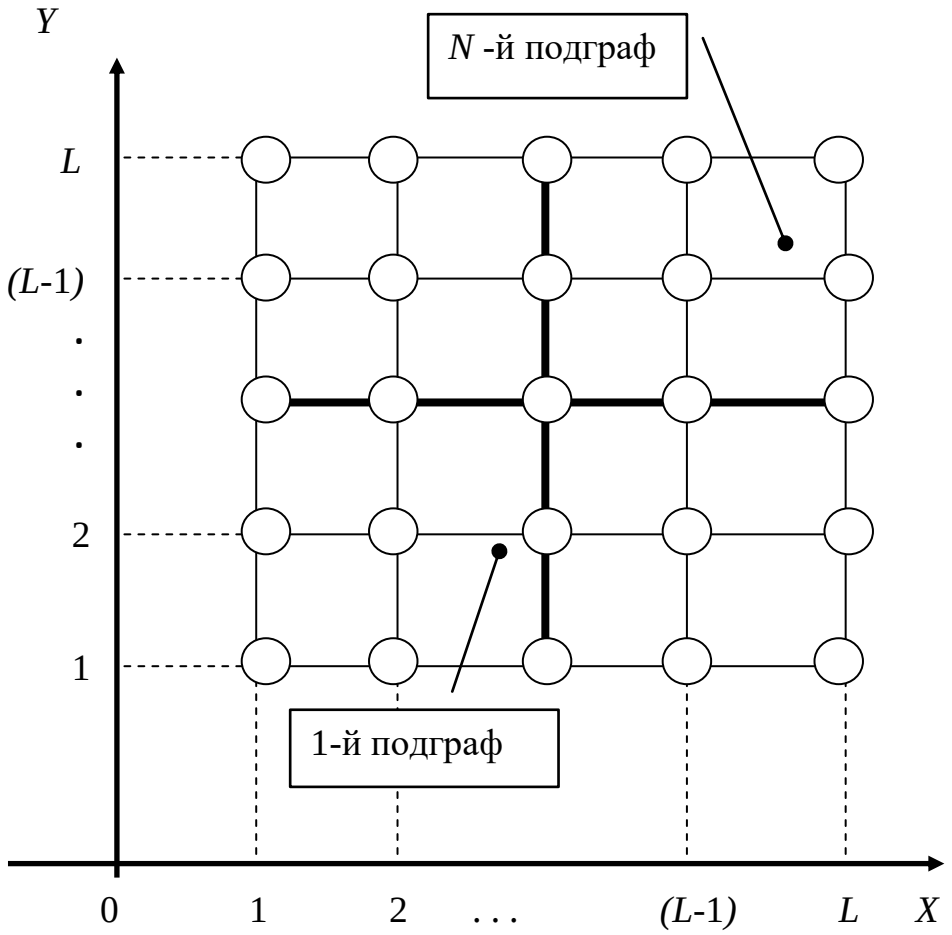


Рисунок 4.8 – Пояснение к оценки вычислительной сложности методом «Разбиения»

Анализируя выражение (4.37), можно сделать вывод, что существует оптимальное число «Разбиений» $N_{\text{опт}}$, при котором $Q_{\text{раз}}$ минимально. Для этого необходимо определить значение *N*, при котром производная первого порядка функции (4.37) равна нулю.

$$\frac{d}{dN^1}\left[S\cdot\chi\cdot\left(\frac{\sqrt{S}}{\sqrt{N}}-1\right)+N\cdot\chi\cdot\left(\sqrt{N}-1\right)\right]=\frac{d\left(\chi\cdot\left(-S+\frac{S^{\frac{3}{2}}}{N}-N+N^{\frac{3}{2}}\right)\right)}{dN}=$$

$$= \chi \cdot \left(-1 - \frac{S^{\frac{3}{2}}}{N^2} + \frac{3 \cdot \sqrt{N}}{2} \right).$$

Анализ полученного выражения позволяет сделать вывод – оптимальное число разбиений пропорцианально $\sqrt{S}$:

$$N_{\text{опт}} = \sqrt{S}$$

Таким образом, оценка вычислительной сложности метода «Разбиения» составит:

$$Q_{\text{раз}} = f\left\{\left[S \cdot \chi \cdot \left(\frac{\sqrt{S}}{\sqrt{\sqrt{S}}} - 1 \right) \right] + S \cdot \chi \cdot \left(\sqrt{\sqrt{S}} - 1 \right) \right\} = f\left\{ \chi \cdot \left(S + \sqrt{S} \right) \cdot \left(\sqrt[4]{S} - 1 \right) \right\}. \quad (4.38)$$

В таблицу 4.1 сведены результаты сопоставительного анализа вычислительной сложности различных методов проверки графа на связность.

Таблица 4.1 – Вычислительная сложность методов проверки графа на связность

№ п/п	Метод проверки графа на связность	Вычислительная сложность
1	«Поиск в глубину»	$Q_{\text{гл}} = f\left(\chi \cdot S^3\right)$
2	«Разрастания»	$Q_{\text{раз}} = f\left(A \cdot S^2\right)$
3	«Свертки»	$Q_{\text{св}} = f\{\chi \cdot S \cdot (\sqrt{S} - 1)\}$
4	«Разбиения»	$Q_{\text{раз}} = f\left\{\chi \cdot \left(S + \sqrt{S}\right) \cdot \left(\sqrt[4]{S} - 1\right)\right\}$

Возьмем отношение вычислительной сложности метода «Свертки» к методу «Разбиения»:

$$\frac{\chi \cdot S \cdot \left(\sqrt{S}-1\right)}{\chi \cdot \left(S+\sqrt{S}\right) \cdot \left(\sqrt[4]{S}-1\right)} \approx \sqrt{S}.$$

Таким образом, за счет разбиения исходного графа на подграфы, появляется возможность работать на пологом участке кривой, отображающей временную зависимость проверки графа на связность, от размерности графа.

Тем самым метод «Свертки» в сравнении с известными методами имеет в $\sqrt{S}$ раз меньшую алгоритмическую сложность.

Данный результат подтвержден экспериментально [5,61,76] На рисунке 4.9 приведена гистограмма относительного временного выигрыша проверки графа сети на связность методом «Разбиения» по отношению к методу «Стягивания». Здесь $T_{\text{стяг.}}$ и $T_{\text{разб.}}$ соответственно время проверки графа сети на связность методом «Стягивания» и предложенного метода «Разбиения». Результаты получены на графе ячеистой структуры со степенью каждой вершины графа равной четырем.

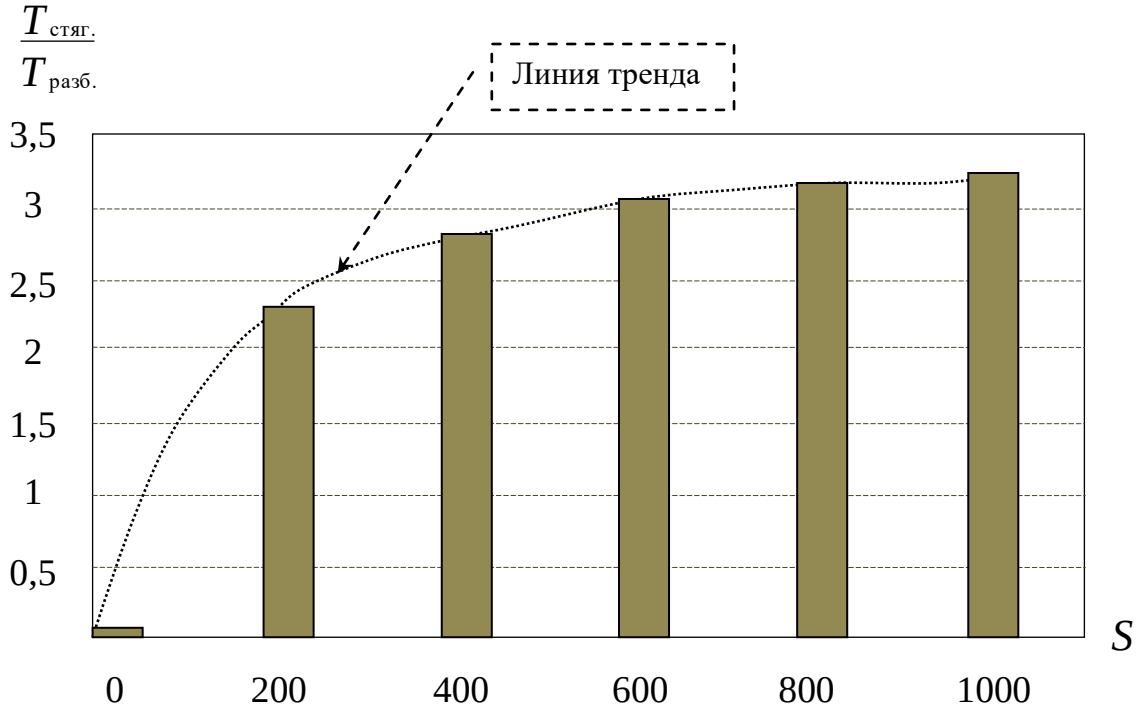


Рисунок 4.9 – Гистограмма относительного временного выигрыша проверки графа сети на связность методом «Разбиения» по отношению к методу «Стягивания»

4.4 Разработка методики определения плана распределения информации на однородной ячеистой сети связи большой размерности

При анализе методов маршрутизации на сетях связи произвольной структуры, имеющих несколько десятков узлов коммутации, возникают проблемы, связанные с решением задач большой размерности. Это объясняется тем, что вычислительная сложность алгоритмов, реализующих тот или иной метод маршрутизации, имеет как минимум, кубическую зависимость от количества УК на сети связи.

В тех случаях, когда структура сети связи приобретает некоторую регулярность, что характерно для ячеистых сетей связи, представляется возможным представить ее в виде регулярной правильной решетки. Результаты, полученные на таких структурах, могут дать асимптотические оценки для анализа методов маршрутизации и значительно уменьшить сложность алгоритмов, моделирующих эти методы.

Выберем для анализа методов маршрутизации ячеистую однородную структуру сети связи с квадратной ячейкой.

Вложим граф $G[A_S, M_S]$, описывающий структуру сети, в прямоугольную систему координат так, чтобы координаты вершин графа принимали только положительные целые числа с шагом, равным единице. Тогда каждая вершина a_i графа $G[A_S, M_S]$ будет иметь свой адрес с координатами $\{i, j\}$.

Исходную вершину графа, соответствующую УИ анализируемой сети связи, поместим в начало координат и далее будем рассматривать процедуру нахождения маршрута между любой вершиной графа $G[A_S, M_S]$ и исходной.

Пусть β_{ij} определяет число кратчайших (по числу промежуточных вершин) маршрутов между исходной вершиной с координатами $\{0,0\}$ и вершиной $\{i, j\}; i = \overline{1, x_{\max}}; j = \overline{1, y_{\max}}$, где $x_{\max}$ и $y_{\max}$ – максимальные количества УК по осям X и Y соответственно.

Величину β_{ij} будем присваивать вершине с координатами $\{i, j\}$, имея при этом в виду, что она относится к паре УК с координатами $\{0,0\}$, $\{i, j\}$. Очевидно, что для однородной ячеистой сети связи с квадратной ячейкой величины β_{ij} и β_{ji} равны между собой. Все вершины графа $G[A_S, M_S]$ по отношению к вершине $\{i, j\}$ будем разделять на два подмножества A_1 и A_2.

В подмножество A_1 входят те узлы, которые не выходят за пределы установленного прямоугольника анализируемой сети связи, ограниченного вершинами с координатами: $\{i, j\}$; $\{i,0\}$; $\{0,0\}$ и $\{0, j\}$ (рисунок 4.10).

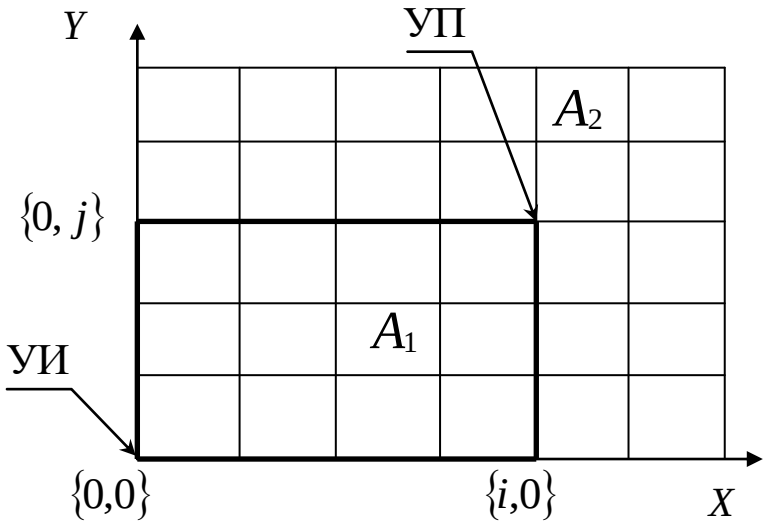


Рисунок 4.10 – Определение числа кратчайших маршрутов между УИ и УП

Справедливо следующее утверждение: число кратчайших маршрутов β_{ij} между исходной вершиной с координатами $\{0,0\}$ и вершиной с координатами $\{i, j\}$ определяется только вершинами, входящими в подмножество A_1.

Учитывая это положение, несложно получить формулу, определяющую β_{ij}:

$$\beta_{ij} = \frac{(i + j)!}{i! \cdot j!}.$$

Для определения самих маршрутов необходимо вычислить величины:

$$p_{ij}^{x} = \frac{\beta_{i-1,j}}{\beta_{i,j}} \text{ и } p_{ij}^{y} = \frac{\beta_{i,j-1}}{\beta_{i,j}},$$

где $\{i-1, j\}$ и $\{i, j-1\}$ – координаты смежных узлов в подмножестве A_1.

Очевидно, что

$$p_{ij}^{x} + p_{ij}^{y} = 1.$$

Подставив в формулы, определяющие p_{ij}^{x} и p_{ij}^{y}, значение

$$\beta_{ij} = \frac{(i+j)!}{i! \cdot j!},$$

получим:

$$p_x = p_{ij}^{x} = \frac{i}{i+j}; \quad p_y = p_{ij}^{y} = \frac{j}{i+j}. \tag{4.39}$$

Таким образом, для выбора более предпочтительного направления в УК по числу кратчайших маршрутов из данного УК, достаточно сопоставить между собой координаты этого узла и продолжить поиск маршрута по направлению координаты X или Y, имеющей большее значение, p_x или p_y соответственно.

Следовательно, используя простые расчеты в каждом УК, можно последовательно строить маршрут от УИ к УП. Причем величины p_x и p_y представлены в форме, удобной для применения в алгоритме маршрутизации как с детерминированным, так и со стохастическим выбором направления в УК.

Если в алгоритме маршрутизации помимо p_x и p_y учитывать и другие параметры ТПС (вероятностно-временные характеристики, определяющие QoS приложений мультисервисной сети связи) в направлении *X* и *Y* соответственно, Ω_{ij}^x и Ω_{ij}^y, исходящих из узла $\{i, j\}$, то тогда коэффициенты, определяющие предпочтительность выбора направления, могут быть получены из следующих выражений:

$$\begin{cases} n_x = \dfrac{p_x \cdot q_x}{p_x \cdot q_x + p_y \cdot q_y}; \\ n_y = \dfrac{p_y \cdot q_y}{p_x \cdot q_x + p_y \cdot q_y}, \end{cases} \tag{4.40}$$

где

$$\begin{cases} q_x = \dfrac{\Omega_x}{\Omega_x + \Omega_y}; \\ q_y = \dfrac{\Omega_y}{\Omega_x + \Omega_y}. \end{cases} \tag{4.41}$$

На рисунке 3.7 приведена классификация методов маршрутизации, из которой следует, что существует большое множество методов маршрутизации. Дадим методику формирования плана распределения информации на сети для некоторых из них, наиболее характерных для каждой группы [73, 78].

«Градиентный вероятносто-детерминированный последовательный с логическим методом формирования плана распределения информации» предусматривает установление маршрутов между парой УИ и УП с минимальным количеством транзитных УК. В случае отсутствия маршрутов с минимальным количеством транзитных УК заявка, поступившая на обслуживание от пользователя УИ, получает отказ. Выбор ТПС в каждом УК осуществляется детерминировано в соответствии с коэффициентами, рассчитанными по формуле (4.39). Однако в случае $p_x = p_y$ выбор исходящего ТПС осуществляется вероятностно.

Пусть $\{i, j\}$ – координаты УИ; $\{i', j'\}$ – координаты УП $\left(i, i' = \overline{1, x_{\max}}; j, j' = \overline{1, y_{\max}}\right)$. Тогда величины

$$D_x = i' - i \text{ и } D_y = j' - j$$

определяют количество транзитных УК от УИ до УП по осям X и Y соответственно. Причем знаки у D_x и D_y указывают геометрическое расположение УП относительно УИ. Покажем это следующим образом:

$$\begin{cases} \text{если} \quad D_x > 0, \quad \text{то} \quad 2\text{-е направление;} \\ \text{если} \quad D_x < 0, \quad \text{то} \quad 4\text{-е направление;} \\ \text{если} \quad D_y > 0, \quad \text{то} \quad 1\text{-е направление;} \\ \text{если} \quad D_y < 0, \quad \text{то} \quad 3\text{-е направление.} \end{cases} \tag{4.42}$$

В этом случае алгоритм маршрутизации состоит в вычислении в каждом транзитном УК, начиная с УИ, выражений:

$$\begin{cases} \downarrow \\ D_x = i' - i; \\ D_y = j' - j; \\ P_x = \dfrac{|D_x|}{|D_x| + |D_y|}; \\ P_y = \dfrac{|D_y|}{|D_x| + |D_y|}. \end{cases} \tag{4.43}$$

Сравнивая коэффициенты P_x и P_y между собой по алгоритму:

$$\begin{cases} \text{если} \quad P_x > p_y, \quad \text{то продолжение поиска по оси } X; \\ \text{если} \quad P_x < p_y, \quad \text{то продолжение поиска по оси } Y; \\ \text{если} \quad P_x = p_y, \quad \text{то выбор поиска осуществляется вероятностно,} \end{cases} \tag{4.44}$$

принимается решение о продолжении поиска маршрута между УИ и УП. Затем, определив знак у D_x, если сделан выбор по оси X, или у D_y, если сделан выбор по оси Y, определяется одно из четырех направлений (4.42), которое считается

предпочтительным. Если вычисленное направление доступно, то оно подключается к ранее набранному маршруту. В случае не доступности определяется менее предпочтительное направление. Если и данном случае ТПС не доступен, то поиск маршрута прерывается и заявке, поступившей на облуживание от УИ, дается отказ. Таким образом, значения элементов матрицы переходных вероятностей (4.19) определяются по (4.43).

На рисунке 4.11 а) приведен пример установления соединения между УИ и УП с координатами, соответственно $\{2,2\}$ и $\{6,5\}$. На рисунке 4.11 б) показана попытка организации маршрута между узлами с координатами $\{7,2\}$ и $\{2,4\}$.

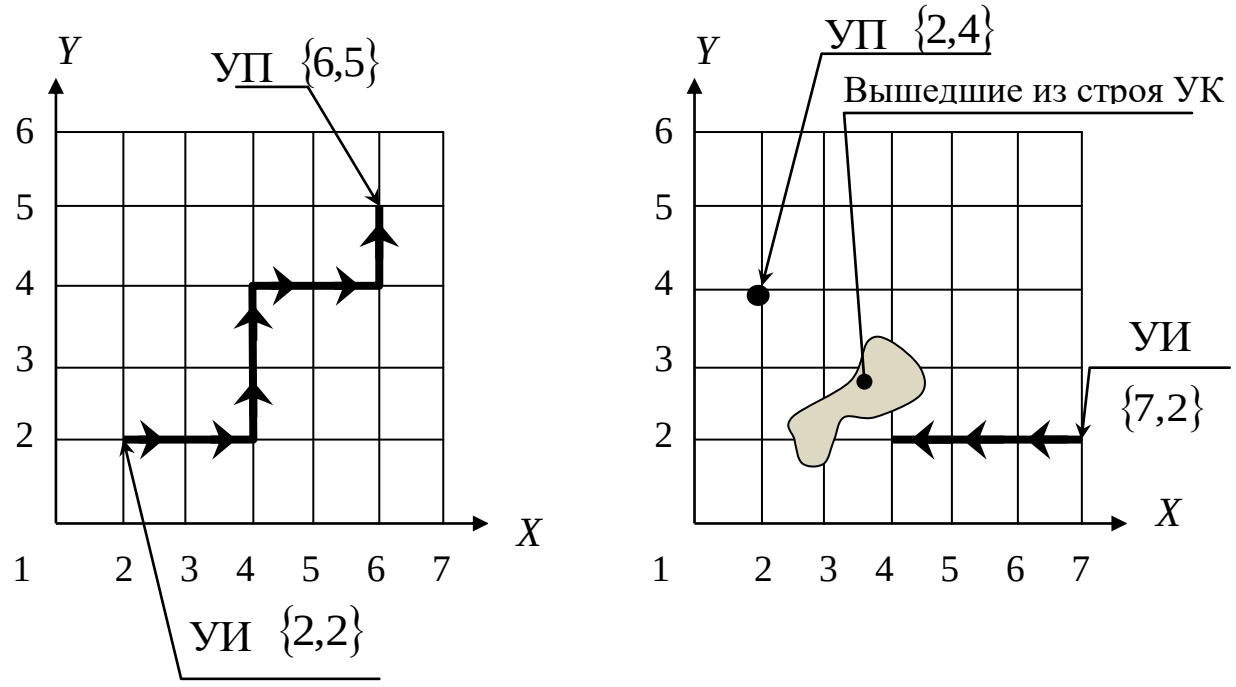


Рисунок 4.11 – «Градиентный вероятносто-детерминированный последовательный с логическим методом формирования плана распределения информации» метод маршрутизации

УК, вышедшие из строя, не дают возможности установить маршрут с минимальным числом ТУ между УИ и УП (хотя кратчайший маршрут существует), поэтому заявка, поступившая от пользователя УИ, получает отказ в обслуживании.

Особенностью МСС является поддержка параметров QoS приложений. В этой связи необходимо учитывать ВВХ трактов передачи сообщений (пропускная

способность, скорость передачи пакетов, время задержки, временной джиттер, вероятность ошибочного приема на символ, пакет и т.д.), участвующих в формировании маршрутов между УИ и УП. В этой связи при расчетах коэффициентов, определяющих предпочтительность выбора исходящих ТПС в каждом УК, необходимо воспользоваться формулами (4.40) и (4.41).

Если один из коэффициентов (n_x или n_y) больше, то выбор исходящего ТПС в УК выполняется детерминировано. В случае равенства n_x и n_y между собой то выбор исходящего ТПС осуществляется вероятностно. Если не существует возможности установления маршрута с минимальным числом транзитных УК между УИ и УП, то заявка, поступившая от пользователя в УИ, получает отказ в обслуживании. Таким образом, в данном случае необходимо последовательно вычислять в каждом УК, начиная с УИ, значения:

$$\begin{cases} D_x = i' - j; \\ D_y = j' - j; \\ P_x = \dfrac{|D_x|}{|D_x| + |D_y|}; \\ P_y = \dfrac{|D_y|}{|D_x| + |D_y|}; \\ q_x = \dfrac{\Omega_{ij}^x}{\Omega_{ij}^x + \Omega_{ij}^y}; \\ q_y = \dfrac{\Omega_{ij}^y}{\Omega_{ij}^x + \Omega_{ij}^y}; \\ n_x = \dfrac{P_x \cdot q_x}{P_x \cdot q_x + P_y \cdot q_y}; \\ n_y = \dfrac{P_y \cdot q_y}{P_x \cdot q_x + P_y \cdot q_y}, \end{cases} \tag{4.45}$$

где

$\{i, j\}$ – координаты УИ;

$\{i', j\}$; $\left(i, i' = \overline{1, x_{\max}}; j, j' = \overline{1, y_{\max}}\right)$ – координаты УП;

Ω_{ij}^{x} и Ω_{ij}^{y} – параметры ТПС (вероятностно-временные характеристики, определяющие QoS приложений мультисервисной сети связи) в направлении оси *X* и оси *Y* соответственно.

Затем, сравнивая n_x и n_y между собой по алгоритму:

$$\begin{cases} \text{если} \quad n_x > n_y, & \text{то продолжение поиска по оси } X; \\ \text{если} \quad n_x < n_y, & \text{то продолжение поиска по оси } Y; \\ \text{если} \quad n_x = n_y, & \text{то выбор поиска осуществляется вероятностно,} \end{cases}$$

принимается решение о предпочтительности выбора направления (по оси *X* или по *Y*) поиска маршрута.

Знак у D_x, если сделан выбор по оси *X*, или у D_y, если сделан выбор по оси *Y*, определяет (4.42) одно из четырех направлений, которое считается предпочтительным в сравнении с остальными по числу кратчайших маршрутов и по ВВХ трактов передачи сообщений между УИ и УП. Если вычисленное направление доступно, то оно подключается к ранее набранному маршруту. В случае недоступности ТПС вычисляется второе, менее предпочтительное. Если в данном случае ТПС не доступен, то данной заявке дается отказ в обслуживании.

Для данного метода маршрутизации значения элементов матрицы переходных вероятностей (4.19) определяются по (4.45).

«Диффузный без возвращения назад вероятносто-детерминированный последовательный с логическим методом формирования плана распределения информации» метод маршрутизации позволяет организовать маршрут между УИ и УП с неограниченным числом транзитных УК. Однако максимальное число выбора исходящих ТПС в УК не превышает трех. Маршрут от УИ к УП ищется по всем направлениям кроме тех, которые:

– ведут в противоположную сторону от УП;

– при данном поиске ранее были пройдены.

Таким образом, процедура поиска маршрута данным методом состоит в последовательном выполнении операций во всех транзитных УК, начиная с УИ, по правилам (4.42) ÷ (4.44).

Если вычисленное направление доступно, то соответствующий исходящий ТПС подключается к ранее выбранному маршруту. В противном случае вычисляется втрое по предпочтительности направление. При необходимости определяется и третье. Если и в последнем случае исходящий ТПС недоступен, то данной заявке дается отказ в обслуживании. Вычисленные направления не должны прокладывать маршрут в противоположную сторону от УП и участвовать при данном поиске маршрута более одного раза.

На рисунке 4.12 а) приведен пример установления маршрута данным методом между УИ и УП с координатами $\{2,5\}$ и $\{6,3\}$ соответственно. На рисунке 4.12 б) показана попытка организации маршрута между узлами с координатами $\{7,5\}$ и $\{2,4\}$. УК, вышедшие из строя, не дают возможности установить маршрут, в результате чего заявка, поступившая от пользователя УИ, получает отказ в обслуживании.

Для получения элементов матрицы переходных вероятностей (4.19) необходимо пронормировать обратные величины расстояний (количество транзитных УК) от исходного УК до УП по трем возможным направлениям поиска маршрута.

Окончательные формулы расчета вероятностей перехода по трем направлениям будут иметь вид:

$$P_1 = \frac{L+1}{3 \cdot L + 2};\ P_2 = \frac{L+1}{3 \cdot L + 2};\ P_3 = \frac{L}{3 \cdot L + 2},$$

где $L = |D_x| + |D_y|$; P_1, P_2 и P_3 – вероятности перехода по первому, второму и третьему направлениям поиска маршрута соответственно.

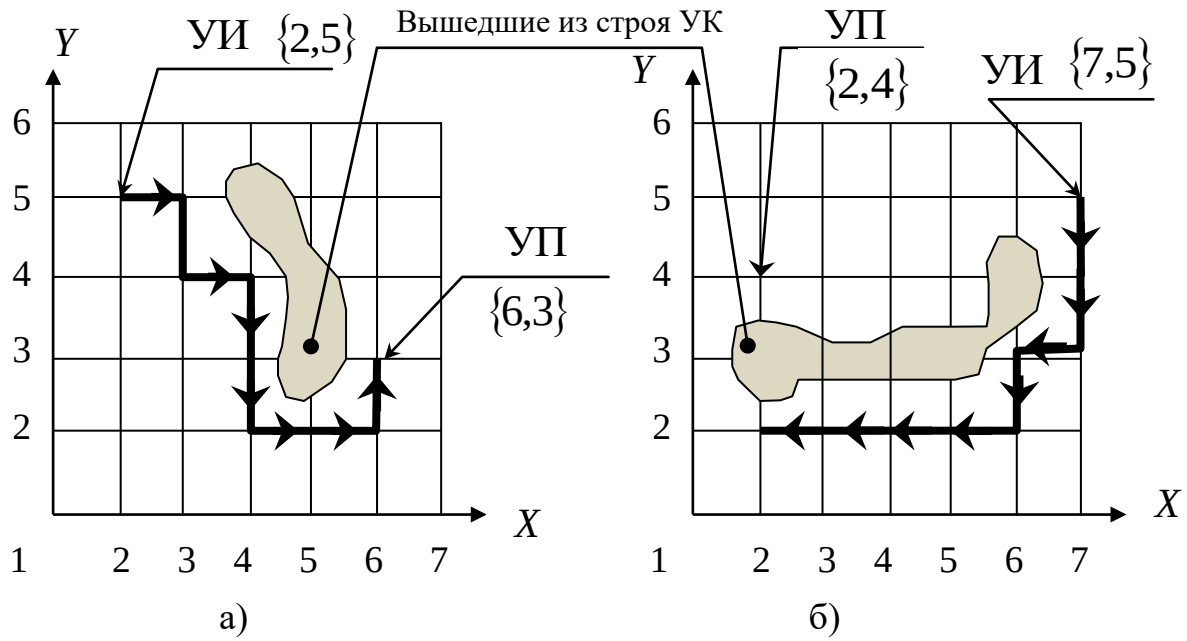


Рисунок 4.12 – «Диффузный без возвращения назад вероятносто-детерминированный последовательный с логическим методом формирования плана распределения информации» метод маршрутизации

«Диффузный вероятносто-детерминированный последовательный с логическим методом формирования плана распределения информации» метод маршрутизации позволяет организовать маршрут между УИ и УП с неограниченным числом транзитных УК. Последовательно выполняя операции (4.42), (4.43) и (4.44) вычисляется наиболее предпочтительное направление (одно из четырех) по числу кратчайших маршрутов. Если выбранное направление доступно, то оно подключается к ранее набранному маршруту. В противном случае вычисляется новое, менее предпочтительное направление. Данная процедура повторяется до тех пор, пока не найдется доступный, исходящий ТПС. Если же доступные, исходящие ТПС во всех направлениях отсутствуют, то заявке, поступившей от пользователя УИ, дается отказ в обслуживании.

На рисунке 4.13 приведен пример организации маршрута между УИ и УП с координатами $\{3,3\}$ и $\{6,2\}$ соответственно.

Расчет элементов матрицы вероятностных переходов (4.19) осуществляется по аналогии с «Диффузный без возвращения назад вероятносто-детерминированный последовательный с логическим методом формирования плана распределения информации» методом маршрутизации. Однако в данном случае учитываются все 4 направления поиска маршрута. Окончательные формулы расчета вероятностей перехода по четырем направлениям будут иметь вид:

$$P_1 = \frac{L+1}{4 \cdot L+2};\ P_2 = \frac{L+1}{4 \cdot L+2};\ P_3 = \frac{L}{4 \cdot L+2};\ P_4 = \frac{L}{4 \cdot L+2},$$

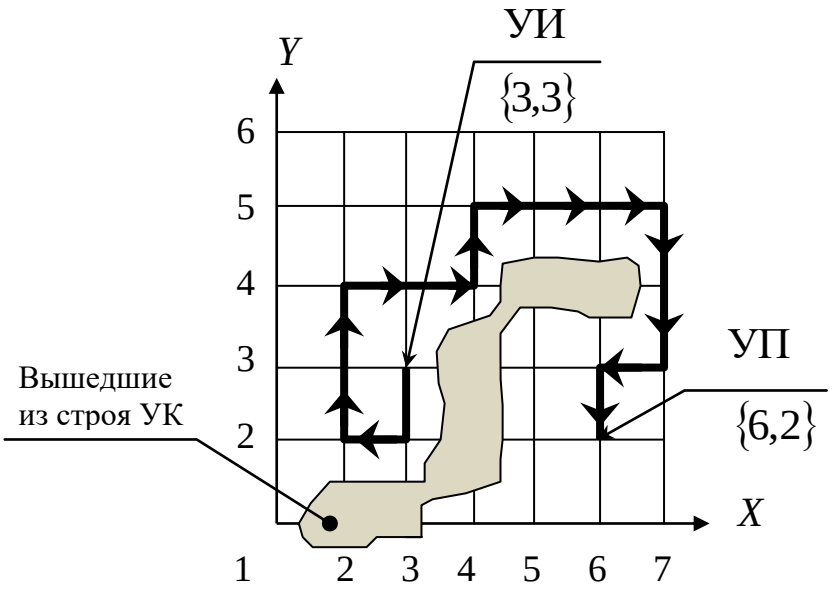


Рисунок 4.13 – Пример организации «Диффузного вероятностно-детерминированного последовательного с логическим методом формирования плана распределения информации» метод маршрутизации

где $L = |D_x| + |D_y|$; P_1, P_2, P_3 и P_4 – вероятности перехода по первому, второму, третьему и четвертому направлениям поиска маршрута соответственно.

«Локально-волновой с детерминированным выбором зоны поиска маршрута и логическим методом формирования плана распределения информации» метод маршрутизации позволяет организовать маршрут между УИ и УП с минимальным количеством транзитных УК. При этом на сети организуется «Лавинный» поиск [45, 134, 147, 165, 166], но не во всех направлениях, а лишь в сторону УП. Поиск распространяется в пределах зоны, охватывающей только кратчайшие маршруты (рисунок 4.9). Если на сети связи между УИ и УП нет кратчайших маршрутов, то заявке, поступившей от УИ, дается отказ в обслуживании.

Таким образом, данный метод состоит в определении всех направлений (используя последовательно операции (4.42), (4.43) и (4.44)), которые могут установить кратчайшие маршруты между парой УК. В случае отсутствия доступных ТПС в вычисленных направлениях, для узлов, расположенных в зоне поиска маршрута, процесс поиска маршрута начинает «Сворачиваться».

На рисунке 4.14 а) показан пример организации маршрута между УИ и УП с координатами, $\{2,2\}$ и $\{7,5\}$. Пунктиром указаны те ТПС, которые остались подключенными на момент установления маршрута между заданной парой УК. Остальные ТПС, участвующие в поиске маршрута, освободились.

Рисунок 4.14 б) показывает попытку установления соединения между парой УК. Однако вышедшие из строя УК не дают возможности организовать такой маршрут и данной заявке, поступившей от УИ $\{2,5\}$, дается отказ в обслуживании.

В силу сложности данного метода маршрутизации (параллельность распространения процессов поиска маршрута от УИ до УП; «Сворачивание» отдельных направлений; выделение одного маршрута из множества просмотренных) расчет (4.45) не пригоден.

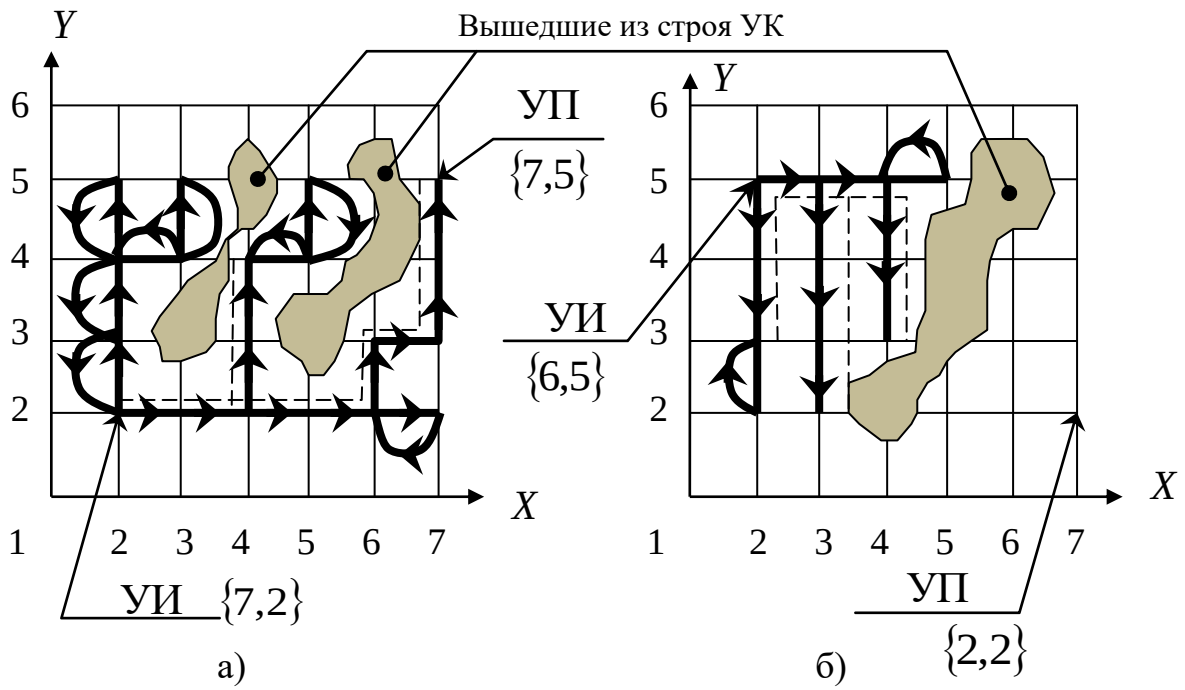


Рисунок 4.14 – «Локально-волновой с детерминированным выбором зоны поиска маршрута и логическим методом формирования плана распределения информации» метод маршрутизации

4.5 Разработка упрощенной имитационной модели маршрутизации

Опишем упрощенную имитационную модель сети связи, в которой выделим процедуру маршрутизации и сгладим процесс передачи пользовательской информации, суть которой сводится к следующему [73, 78].

Каждый из методов маршрутизации использует часть ресурса МСС для нахождения маршрутов (рисунок 3.4) между УИ и УП. Следовательно, количество одновременно установленных соединений (Ξ) с применением различных методов маршрутизации будет различно. Таким образом, в качестве критерия сравнения методов маршрутизации можно использовать способность МСС пропустить максимальную нагрузку между парами узлов-источников и узлов-получателей, выраженную в количестве одновременно установленных соединений (Ξ).

Введем следующие обозначения:

$\tilde{\Xi}$ – среднее количество установленных соединений за $N_{\text{о}}$ испытаний методом статистического моделирования;

$\Xi_{\max}$ – максимально возможное количество соединений на сети, которое рассчитывается следующим образом:

$$\Xi_{\max} = \frac{R_{\text{о}}}{L_{\text{ср}}},$$

где

$R_{\text{о}}$ – общий средний сетевой ресурс МСС, рассчитанный по формуле (4.1);

$L_{\text{ср}}$ – средняя длина маршрута между УИ и УП (рассчитывается в соответствии с матрицей тяготений $\Pi_{\varepsilon} = \left\| \pi_{\varepsilon,R,L} \right\|_{S,S}$).

Тогда выражение

$$W = \frac{\tilde{\Xi}}{\Xi_{\max}} \tag{4.46}$$

будет определять коэффициент пропускной способности сети.

В процессе функционирования МСС количество виртуальных каналов связи и виртуальных трактов передачи сообщений меняется во времени (рисунок 4.4). В качестве допущения примем, что количество ВК и ВТ постоянно (например, примем их средние значения за время наблюдения T_0). Так же опустим понятие ВТ и каждой ЛС сети $G[A_S, M_S]$ присвоим суммарное количество всех ВК. То есть представим граф сети $G[A_S, M_S]$ матрицей виртуальных каналов $K = \left\| k_{i,j} \right\|_{S,S}$, где элемент матрицы $k_{i,j}; i, j = \overline{1,S}; i \neq j$ указывает количество ВК между УК a_i и a_j.

Алгоритм (рисунок 4.15) упрощенной имитационной модели маршрутизации в условиях внешнего деструктивного воздействия на элементы МСС методом статистического моделирования состоит из следующих шагов.

1. Исходными данными являются (оператор 00):

$$K = \left\| k_{i,j} \right\|_{S,S}; ROUT; \Pi_{\varepsilon} = \left\| \pi_{\varepsilon,R,L} \right\|_{S,S}; P_{\text{дес}} = \| \ p^{j}_{\text{дес}\ i} \ \|_{S,S}; N_{\text{о}}; N.$$

Здесь N – количество заявок, поступающих в МСС.

2. В соответствии с матрицей тяготений $\Pi_{\varepsilon} = \left\| \pi_{\varepsilon,R,L} \right\|_{S,S}$ рассчитывается средняя длина маршрута между УИ и УП ($L_{\text{ср}}$) на сети $G[A_S, M_S]$ (оператор 01).

3. Суммированием всех ВК, преобразованной сети $K = \left\| k_{i,j} \right\|_{S,S}$ (с учетом заданной матрицы $P_{\text{дес}} = \| \ p^{j}_{\text{дес}\ i} \ \|_{S,S}$), определяется общий средний сетевой ресурс МСС ($R_{\text{о}}$). Преобразование матрицы $K = \left\| k_{i,j} \right\|_{S,S}$ (с учетом заданных параметров $P_{\text{дес}} = \| \ p^{j}_{\text{дес}\ i} \ \|_{S,S}$) осуществляется аналогично алгоритму вывода из строя элементов сети (4.30). То есть генерируют κ независимых случайных равномерно распределенных в интервале (0,1) чисел X_{φ}. Затем значения X_{φ} последовательно сравнивают с величинами матрицы $P_{\text{дес}} = \| \ p^{j}_{\text{дес}\ i} \ \|_{S,S}$ по следующему правилу:

$$\begin{cases} \text{если } p^{j}_{\text{дес}\,i} \geq p_{\varphi} \Rightarrow \text{элемент графа считается выведенным из строя } k_{ij} = 0; \\ \text{если } p^{j}_{\text{дес}\,i} < p_{\varphi} \Rightarrow \text{элемент графа } k_{ij} \text{ находится в исправном состоянии.} \end{cases} \quad (4.47)$$

Учитывая, что процесс вывода из строя виртуальных каналов $K = \left\| k_{i,j} \right\|_{S,S}$ носит вероятностный характер, то данную процедуру необходимо выполнить $N_{\text{о}}$ раз. После чего вычислить среднее значение общего среднего сетевого ресурса МСС:

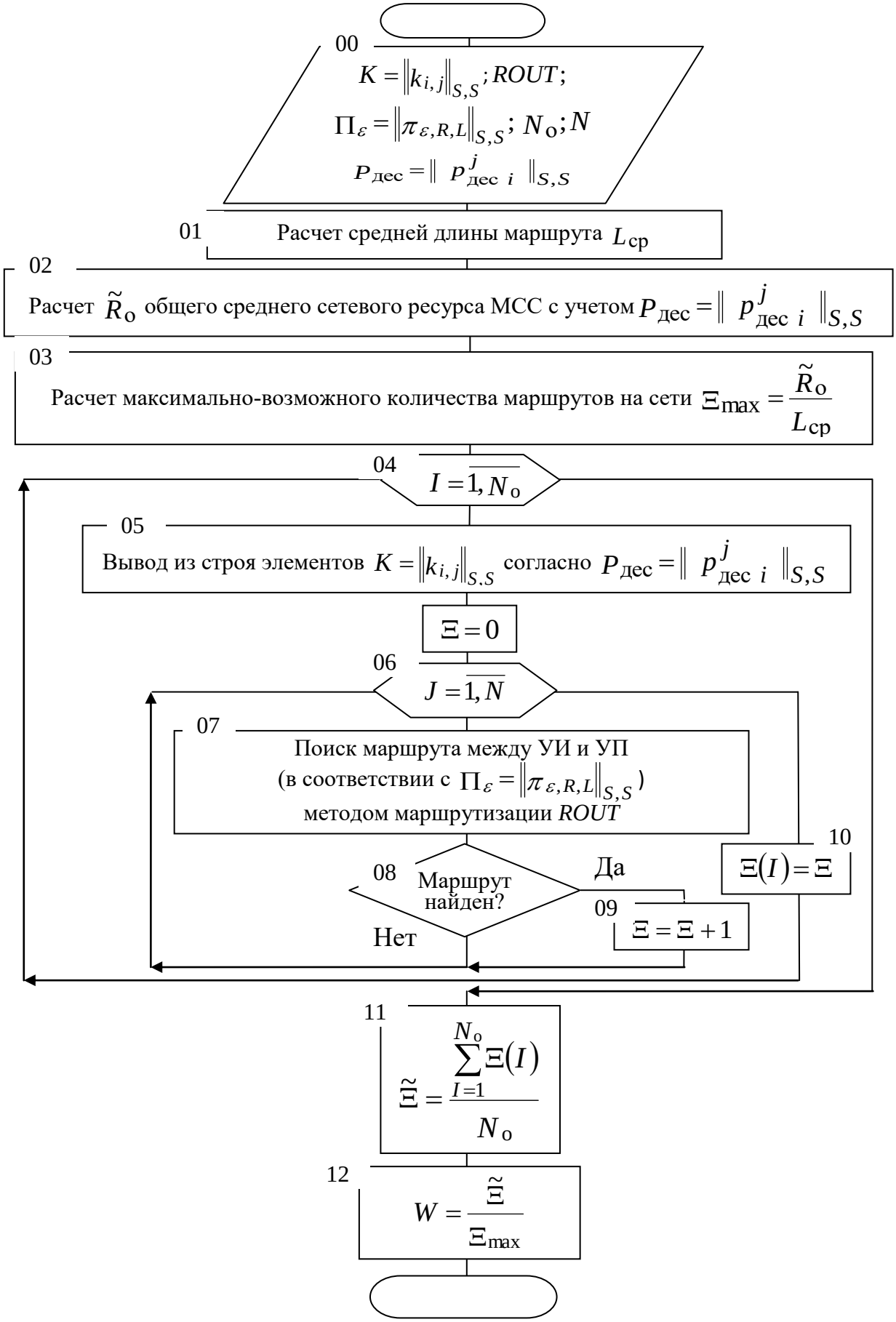


Рисунок 4.15 – Алгоритм упрощенной имитационной модели маршрутизации

$$\widetilde{R}_{\text{o}} = \frac{\sum_{i=1}^{N_{\text{o}}} R_{\text{o}}^{(i)}}{N_{\text{o}}},$$

где

$R_{\text{o}}^{(i)}$ – общий средний сетевой ресурс МСС в *i*-м испытании;

N_{o} – количество испытаний и определяется по формуле (2.11).

4. Оператором 03 вычисляется максимально возможное количество маршрутов на сети $G[A_S, M_S]$:

$$\Xi_{\max} = \frac{\widetilde{R}_{\text{o}}}{L_{\text{ср}}}.$$

5. Начиная с 04 оператора до 10 оператора (рисунок 4.14) выполняется процесс формирования статистических данных за N_{o} испытаний. Каждое испытание состоит из следующих процедур.

6. Оператором 05 имитируется внешнее деструктивное воздействие на элементы МСС. Для этого, используя алгоритм (4.47) выполняется вывод из строя элементов матрицы $K = \left\| k_{i,j} \right\|_{S,S}$.

7. Операторы 06 ÷ 09 (рисунок 4.14) выполняют на преобразованной матрице $K = \left\| k_{i,j} \right\|_{S,S}$ (по окончании процедуры воздействия внешних деструктурирующих факторов на элементы МСС) *N* действий: поиск маршрутов; в случае нахождения маршрута осуществляется занятие соответствующих ВК; подсчет количества установленных маршрутов. Для этого случайным образом в соответствии с матрицей тяготений $\Pi_{\varepsilon} = \left\| \pi_{\varepsilon,R,L} \right\|_{S,S}$ производится выбор УИ и УП. Методом маршрутизации *ROUT* устанавливается соединение между УИ и УП. Если соединение не установлено, то выбирается новая пара УИ и УП и попытка установления повторяется. В случае установления соединения значение

переменной Ξ увеличивается на единицу. Установленное соединение между УИ и УП остается занятым до конца испытания. То есть, соответствующие ВК в преобразованной матрице $K = \|k_{i,j}\|_{S,S}$ (по окончании процедуры воздействия внешних деструктивных факторов на элементы МСС) считаются занятыми. По окончанию действия операторов 06 ÷ 09 подсчитанное значение количества установленных соединений в данном испытании запоминается оператором 10.

8. Оператором 11 рассчитывается среднее значение установленных соединений за $N_{\text{о}}$ испытаний:

$$\tilde{\Xi} = \frac{\sum_{I=1}^{N_{\text{о}}} \Xi(I)}{N_{\text{о}}}.$$

9. Оператором 12 вычисляется искомое значения (4.46).

Таким образом, если при моделировании анализируемые методы маршрутизации получили разные W, то предпочтительным считается тот, у которого коэффициент пропускной способности выше.

4.6 Выводы

1. Разработанные методики и модели (с определенными ограничениями), включающие:

– математическую модель для оценки влияния методов формирования плана распределения информации на объем сетевых ресурсов;

– математическую модель маршрутизации в условиях входного самоподобного трафика и внешних деструктивных воздействий на элементы мультисервисной сети связи;

– методику определения плана распределения информации на однородной ячеистой сети связи большой размерности;

– упрощенную имитационную модель маршрутизации,

позволяют проводить анализ методов маршрутизации с целью выявления тех методов маршрутизации, которые будут наиболее эффективно функционировать в предполагаемых сетях связи и в заданных условиях.

2. Определены и разработаны пути сокращения вычислительной сложности алгоритмов оценки структурной надежности сети связи методом статистического моделирования:

– уменьшение дисперсии оценок результатов моделирования с сохранением точности;

– эффективные методы проверки графа сети на связность.

5 Анализ результатов моделирования маршрутизации в условиях внешних деструктивных воздействий на элементы мультисервисной сети связи

5.1 Постановка задачи

Многочисленные исследования [10, 20, 30, 33, 40, 49, 54, 57, 59, 63, 64, 65, 87, 88, 103, 111, 115, 121, 131, 132, 138, 149, 150, 153, 163, 174, 178, 183 и другие работы] доказывают значительное влияние протоколов сетевого уровня на параметры QoS приложений мультисервисных сетей связи. Данный факт стимулирует разработчиков телекоммуникационного оборудования к исследованию, реализации и внедрению новых, более совершенных программно-аппаратных комплексов, осуществляющих процедуры маршрутизации. Вместе с тем такие комплексы являются структурообразующими для МСС. Это означает, что внедрение новых методов маршрутизации всегда влечет за собой серьезные материальные затраты и проведение глобальных организационно-технических мероприятий на действующих сетях. Желательно иметь универсальные комплексы, реализующие процедуры маршрутизации, способные поддерживать любые технологии формирования пакетов пользовательской информации (ATM, IP всех версий, Ethernet и т.д.). В результате был разработан протокол MPLS [168], реализующий «Статистический» метод формирования ПРИ. Применение MPLS совместно с другими сетевыми технологиями (ATM, IP всех версий, Ethernet и т.д.) обеспечивает QoS неограниченного спектра приложений и не требует значительных материальных затрат на действующих МСС.

«Статистический» метод формирования ПРИ организует маршрут по накопленной статистики ранее установленных соединений. Это является достоинством данного метода и одновременно серьезным недостатком. Можно предположить, что в условиях внешних деструктивных воздействий на элементы

МСС из-за отсутствия статистической информации данный метод будет не эффективно решать задачи процедур маршрутизации. Данные рассуждения подтверждает результат, полученный в разделе 4.2, утверждающий, что в условиях внешнего деструктивного воздействия, при котором примерно 30% сетевых ресурсов мультисервисной сети связи выходит из строя, целесообразно применять «Лавинный» метод формирования плана распределения информации по сравнению со «Статистическим».

В этой связи представляет интерес проведения дополнительного исследования данного результата на сетях связи с различной структурой с использованием различных математических и имитационных моделей.

5.2 Имитационное моделирование мультисервисной сети связи в условиях ограниченных сетевых ресурсов

Существует достаточно много программных продуктов для моделирования сетей связи: COMNETIII производитель CACI Products Company [139]; OPNET от компании OPNET Technologies [162]; NetCracker XA [152]; OMNET++ [161]; NS2 [159]; NS3 [160] (The Network Simulator); CPN (Colored Petri Nets) [140] и многие другие. Подробный сопоставительный анализ наиболее известных продуктов имитационного моделирования сетей связи приведен в работах [25, 27, 31, 34] и многих других. При этом важными критериями выбора того либо иного программного продукта являются:

– удобный графический интерфейс;

– возможность варьирования параметров моделирования во время проведения экспериментов;

– цена программного продукта

и многие другие критерии, необходимые для анализа сетевых процессов телекоммуникационных систем.

Воспользуемся специализированным программным продуктом Opnet Modeler v 14.0 [162]. Данный программный продукт: предназначен для

имитационного моделирования сетей связи; содержит обширную библиотеку программно-аппаратных комплексов (маршрутизаторов, коммутаторов, маршрутизируемых коммутаторов различных уровней и т.д.), реализующих известные на рынке телекоммуникаций сетевые технологии и протоколы.

Для имитационного моделирования выбрана характерная для мультисервисной сети «Ячеистая» структура (рисунок 5.1) [70, 71]. В ее составе 5 локальных сетей связи (Lan), 10 маршрутизаторов (Router1 ÷ Router10) и один сервер (Server_1).

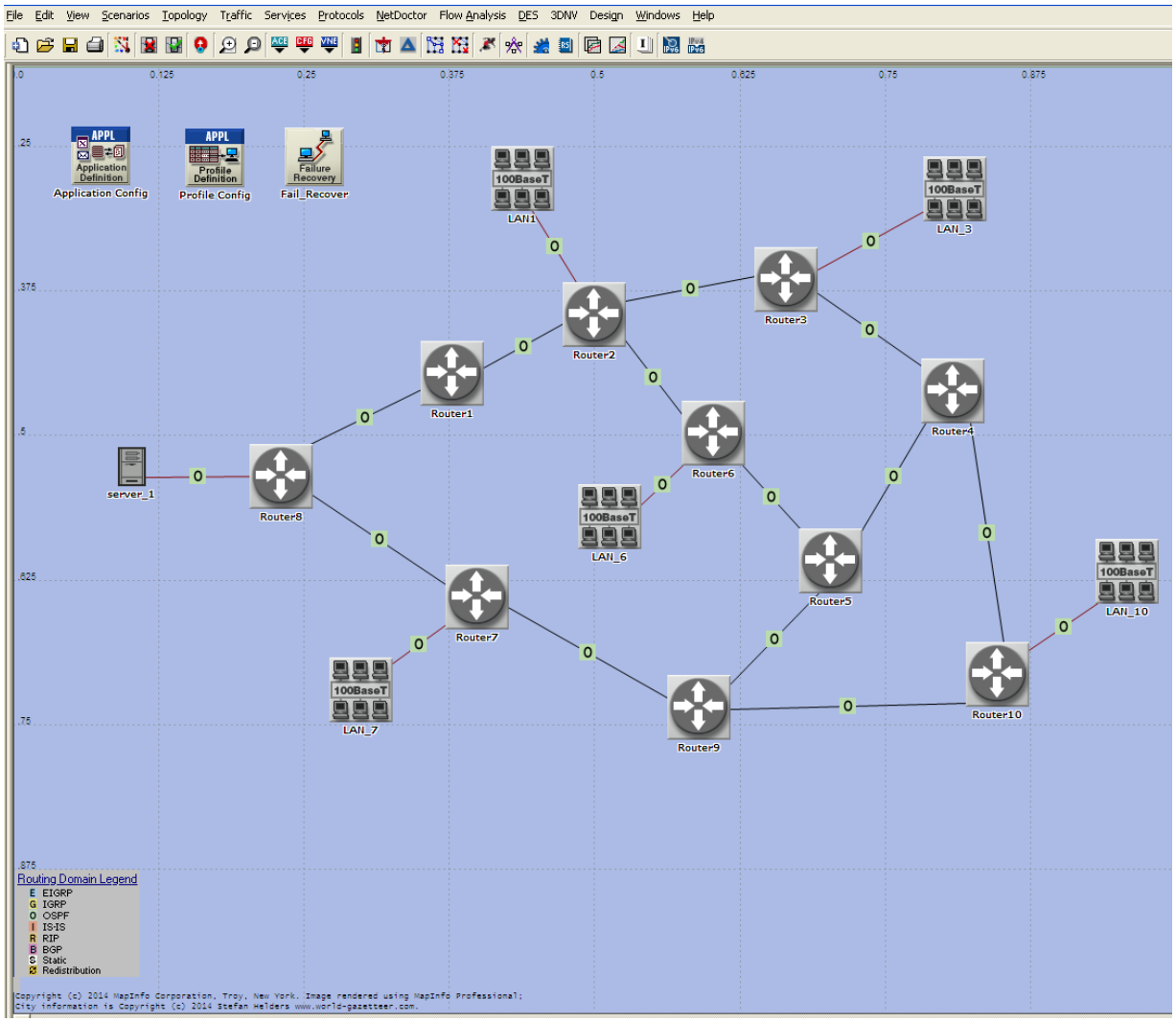


Рисунок 5.1 – Исходная структура анализируемой мультисервисной сети связи

Каждая локальная сеть организована на базе технологии Fast Ethernet:

– содержит 10 компьютеров, подключенных к коммутатору по принципу «Звезда»;

– на транспортном уровне поддерживается протоколами TCP и UDP;

– генерирует трафик видеоконференции (Video Conferencing, VC) со скоростью 1350 кбит/с (размер кадра 128*120 пикселей, частота 10 кадров/с, разрешение 9 бит на пиксель).

Выбор видеоконференции обоснован тем, что данное приложение предъявляет повышенные требования к QoS (высокая скорость и минимальное время задержки при передачи информации).

Учитывая, что в качестве приложения выбрана только видеоконференция, организованная на базе клиент-серверной архитектуры, то характеристики сервера Sun Ultra выбраны минимальными – одноядерный процессор с частотой 333 МГц с поддержкой операционной системы Solaris.

Локальные сети и сервер подключены к соответствующим маршрутизаторам с помощью кабелей, поддерживающих семейство технологий Ethernet, 100 Мбит/с.

Маршрутизаторы между собой на канальном уровне взаимодействуют по протоколу PPP (англ. Point to Point Protocol) и соединены сетевым кабелем с одинаковой заранее определенной (в каждом имитационном испытании) пропускной способностью r=1000 Мбит/с, r=100 Мбит/с и r=10 Мбит/с. Таким образом, в одном имитационном испытании каждая линия связи, соединяющая маршрутизаторы, принимает значение только r=1000 Мбит/с,
в другом r=100 Мбит/с и аналогично в следующем r=10 Мбит/с.

Пошаговое уменьшение пропускной способности сетевого кабеля от 1000 Мбит/с до 10 Мбит/с сокращает общие сетевые ресурсы (4.1)

$$R_{\text{o}} = 12 \cdot r, \tag{5.1}$$

тем самым имитирует процесс внешнего деструктивного воздействия на анализируемую МСС.

Маршрутизаторы анализируемой сети в каждом имитационном испытании поддерживают только один метод формирования плана распределения

информации OSPF [165] ($ROUT_{\text{ТМ}}^{(\text{лав})}$ – «Лавинный») или MPLS [168] ($ROUT_{\text{ТМ}}^{(\text{стат})}$ – «Статистический»).

Таким образом, при заданных:

– методе формирования ПРИ $ROUT_{\text{ТМ}}$;

– общем сетевом ресурсе $R_{\text{О}}$ (суммарные пропускные способности r сетевого кабеля)

одно испытание состоит в тридцати минутной имитации функционирования анализируемой МСС. Причем с с нулевой до пятой минуты МСС функционирует в штатном режиме (в условиях отсутствия внешних деструктивных воздействий) (рисунок 5.2).

На пятой минуте маршрутизатор Router9 выводится из строя. В таком состоянии МСС продолжает функционировать до десятой минуты. На десятой и пятнадцатой минутах, соответственно, дополнительно к Router9 выводятся из строя маршрутизаторы Router5 и Router6.

Данный процесс (последовательный вывод из строя маршрутизаторов Router9, Router5 и Router6) дополнительно к пошаговому уменьшению общих сетевых ресурсов (5.1) имитирует внешнее деструктивное воздействие на анализируемую МСС. В результате структура анализируемой сети связи в процессе одного испытания изменяется от «Ячеистой» до «Линейной» (рисунки 5.3, 5.4, 5.5 и 5.6).

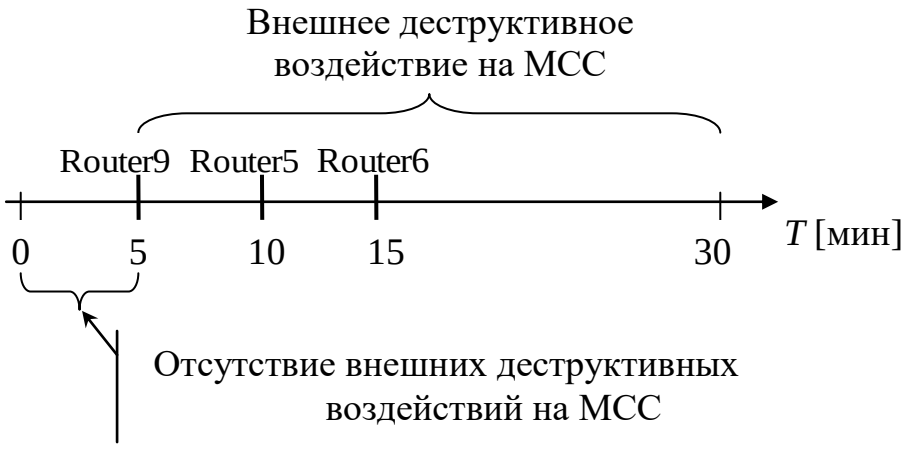


Рисунок 5.2 – Порядок выхода маршрутизаторов из строя

Результатом одного испытания имитационного моделирования является количество потерянных пакетов VC $N_{\text{потерь}}$ за единицу времени.

На рисунках 5.7, 5.8 и 5.9 представлены результаты имитационного моделирования анализируемой мультисервисной сети связи [70].

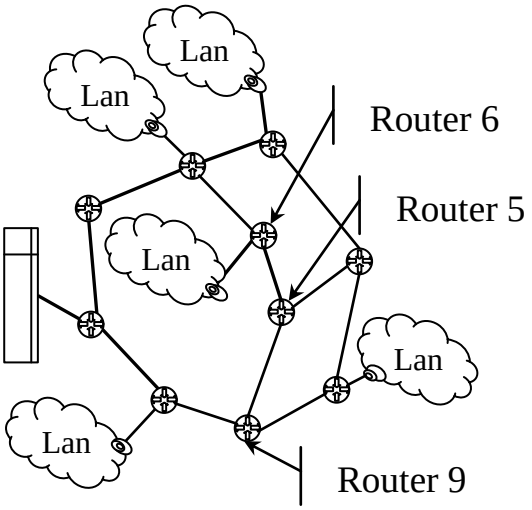


Рисунок 5.3 – Структура анализируемой МСС с 0 по 5 минуту моделирования

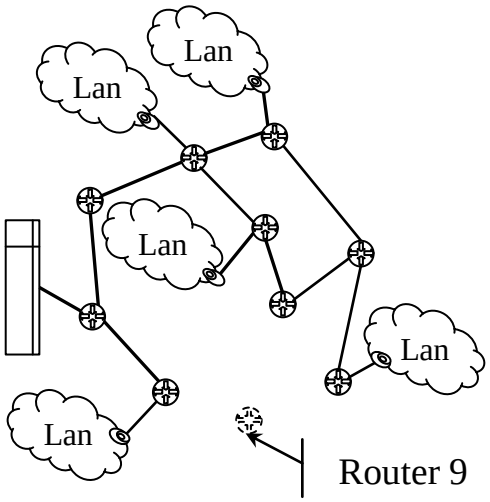


Рисунок 5.4 – Структура анализируемой МСС с 5 по 10 минуту моделирования

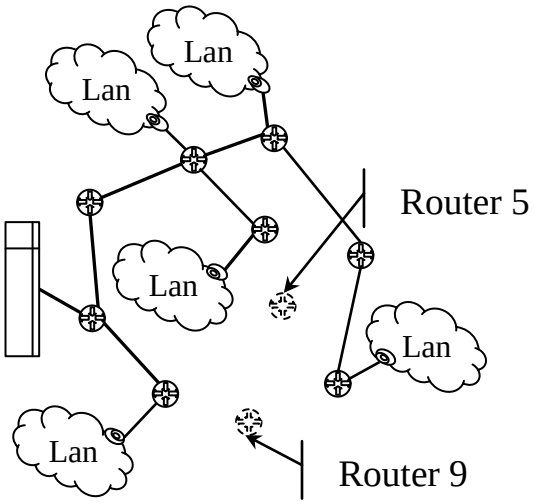


Рисунок 5.5 – Структура анализируемой МСС с 10 по 15 минуту моделирования

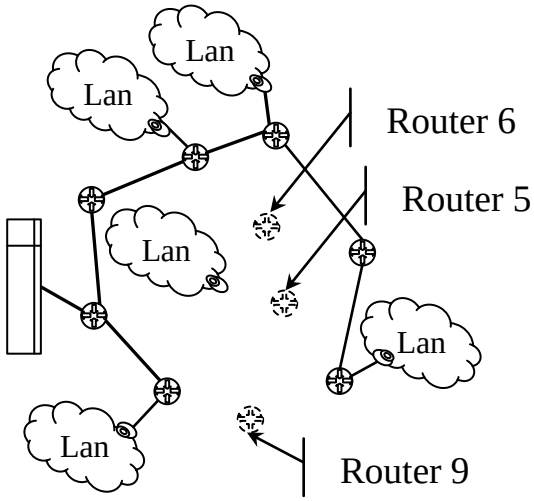


Рисунок 5.6 – Структура анализируемой МСС с 15 по 30 минуту моделирования

Выпишем основные значения полученных результатов моделирования.

Рисунок 5.7 – Пропускная способность r = 1000 Мбит/с

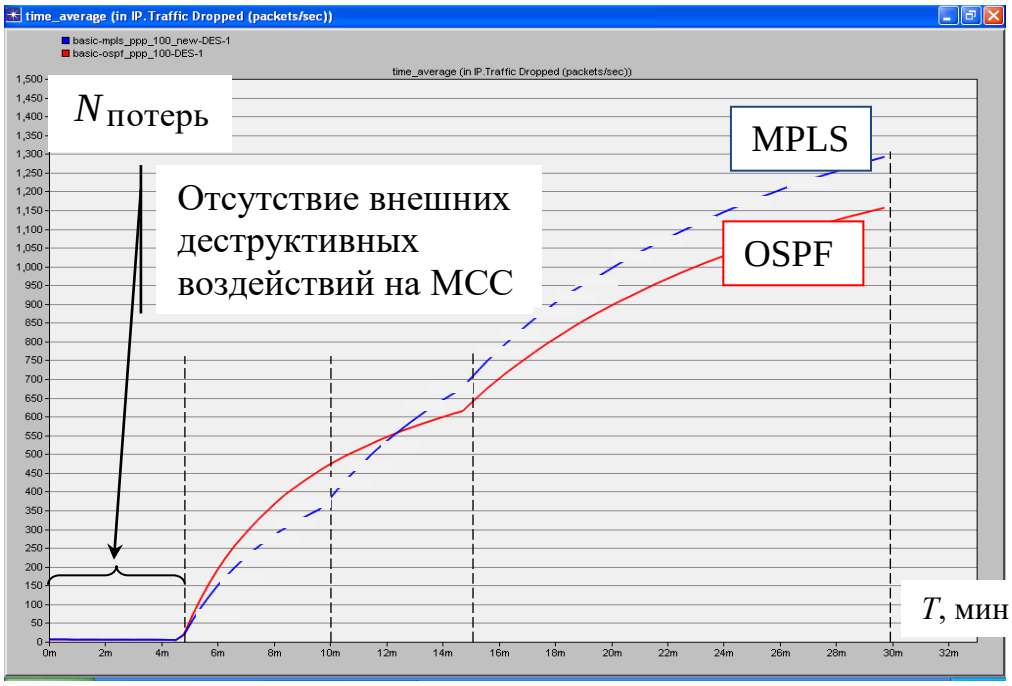


Рисунок 5.8 – Пропускная способность r = 100 Мбит/с

Введем следующие обозначения.

$R_0^{(i)}; i = \overline{1,4}$ – общий сетевой ресурс анализируемой МСС в одном имитационном испытании на соответствующем интервале времени, который определяется:

$$\begin{cases} R_{\text{о}}^{(1)} = 12 \cdot r & \text{интервал моделирования} \quad \text{с } 0 \text{ до } 5 \quad \text{минут;} \\ R_{\text{о}}^{(2)} = 9 \cdot r & \text{интервал моделирования} \quad \text{с } 5 \text{ до } 10 \quad \text{минут;} \\ R_{\text{о}}^{(3)} = 7 \cdot r & \text{интервал моделирования} \quad \text{с } 10 \text{ до } 15 \quad \text{минут;} \\ R_{\text{о}}^{(4)} = 6 \cdot r & \text{интервал моделирования} \quad \text{с } 15 \text{ до } 30 \quad \text{минут.} \end{cases}$$

С учетом (5.1) рассчитаем значение переменной *x*, определяющей степень недоступности общих сетевых ресурсов анализируемой сети, по следующему правилу:

$$x_i = \frac{R_{\text{о}} - R_{\text{о}}^{(i)}}{R_{\text{о}}}; i = \overline{1,4}.$$

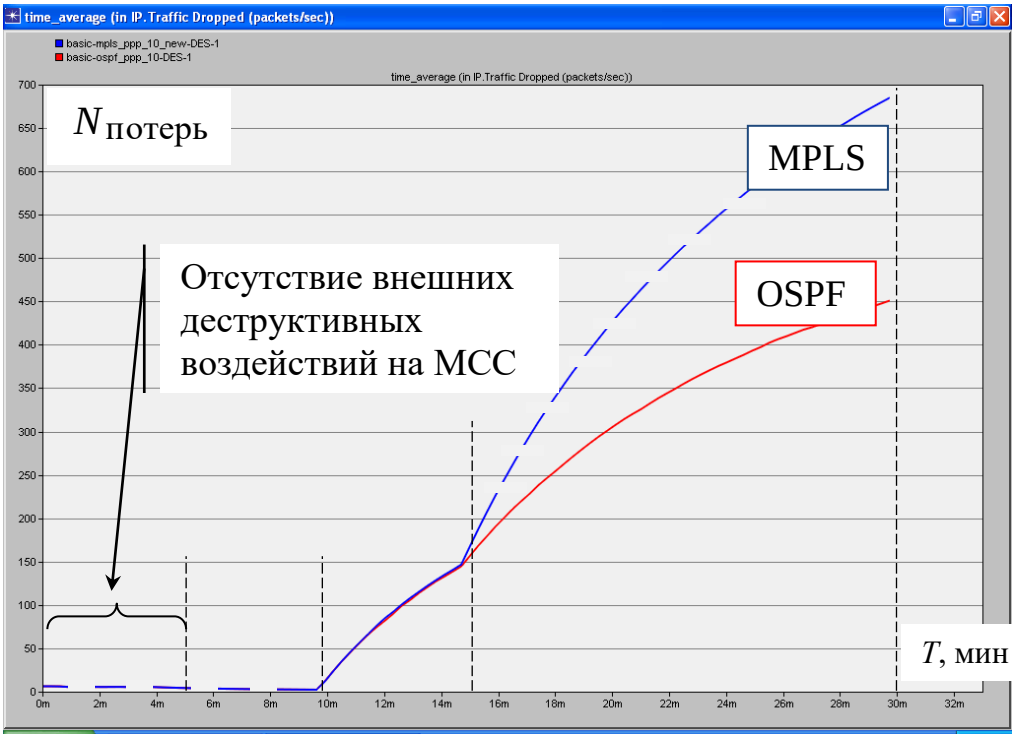


Рисунок 5.9 – Пропускная способность *r* = 10 Мбит/с

Полученные результаты внесем в таблицу 5.1. Опустим индекс *i* при x_i и проведем нормирование значений таблицы 5.1:

$$\overline{N} = 1 - \frac{N_{\text{потерь}}}{N^{(j)}_{\text{потерь(max)}}}; \; j = \overline{1,3},$$

где $N^{(j)}_{\text{потерь(max)}}; j = \overline{1,3}$ – максимальное значение $N_{\text{потерь}}$ в каждом из трех испытаний имитационного моделирования: $N^{(1)}_{\text{потерь(max)}} = 4300;$ $N^{(2)}_{\text{потерь(max)}} = 1300;$ $N^{(3)}_{\text{потерь(max)}} = 750.$

Таблица 5.1 Результаты имитационного моделирования

№ имитационного испытания	r Мбит/с	x_i	$N_{\text{потерь}}$	
			MPLS	OSPF
1	1000	x_1=0	0	0
		x_2=0,25	1400	1800
		x_3=0,42	1800	2300
		x_4=0,5	3200	**4300**
2	100	x_1=0	0	0
		x_2=0,25	350	475
		x_3=0,42	675	600
		x_4=0,5	**1300**	1150
3	10	x_1=0	0	0
		x_2=0,25	0	0
		x_3=0,42	150	150
		x_4=0,5	**700**	450

Полученные результаты расчетов представлены в таблице 5.2 и на рисунках 5.10, 5.11 и 5.12.

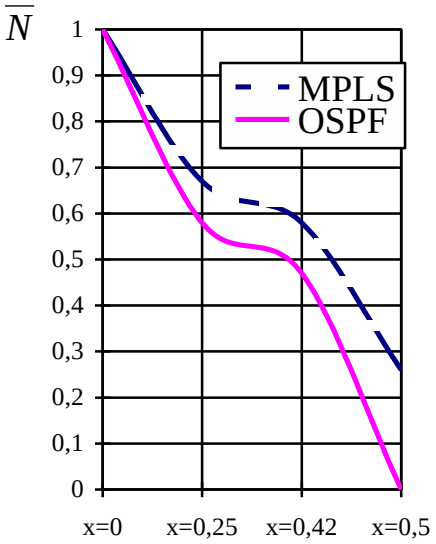


Рисунок 5.10 – Нормированные результаты моделирования при r = 1000 Мбит/с

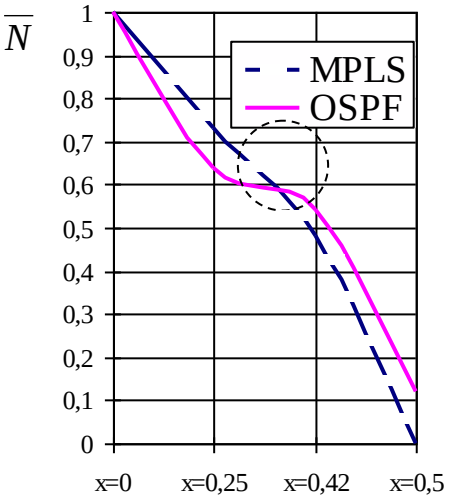


Рисунок 5.11 – Нормированные результаты моделирования при r = 100 Мбит/с

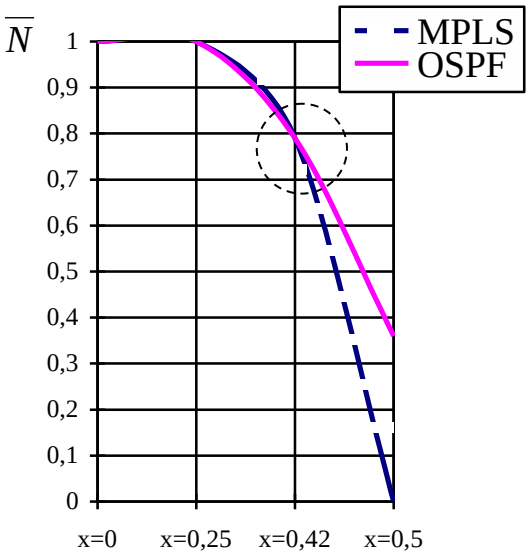


Рисунок 5.12 – Нормированные результаты моделирования при r = 10 Мбит/с

Полученные результаты позволяют утверждать, что в условиях внешнего деструктивного воздействия $\Psi_{-}(t)$, при котором примерно 30% сетевых ресурсов МСС выходит из строя, целесообразно применять «Лавинные» методы формирования плана распределения информации.

Таблица 5.2 Нормированные результаты имитационного моделирования

r Мбит/с	x	$\overline{N}$	
		MPLS	OSPF
1000	0	1	1
	0,25	0,67	0,58
	0,42	0,58	0,47
	0,5	0,26	0
100	0	1	1
	0,25	0,73	0,64
	0,42	0,48	0,54
	0,5	0	0,12
10	0	1	1
	0,25	1	1
	0,42	0,79	0,79
	0,5	0	0,36

5.3 Анализ результатов математического моделирования маршрутизации в условиях входного самоподобного трафика и внешних деструктивных воздействий на элементы мультисервисной сети связи

С использованием разработанной методики (4.29) определим вероятность отказа в обслуживании в целом по МСС (интегральная оценка (4.28)) для различных методов маршрутизации при следующих исходных данных.

1. Структуру мультисервисной сети связи (рисунок 5.13) представим в виде неориентированного графа $G[A_S, M_S]$ с множеством: вершин $A_S = \{a_i\}; i = \overline{1,S}; S = 12$, соответствующих УК; ребер $M_S = \{m_{ij}\}; i, j = \overline{1,S}; i \neq j$, соответствующих трактам передачи сообщений.

Каждый ТПС характеризуются пропускной способностью $\mu = \mu_{ij} = 100 \cdot 10^6; i, j = \overline{1,12}; i \neq j$ пакетов/с. Длительность обслуживания пакетов сообщений поступающего асинхронного потока данных в ТПС между a_i и a_j УК подчиняется экспоненциальному закону с параметром $w = \frac{1}{\mu}$.

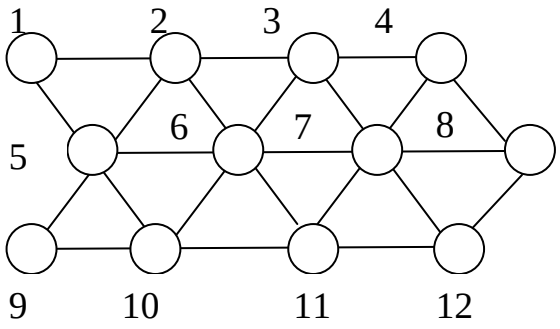


Рисунок 5.13 – Исходная структура МСС

2. Анализируемые методы маршрутизации (согласно классификации, приведенной на рисунке 3.7):

– $ROUT_{\text{посл}}^{(\text{лав})}$ – «Последовательный детерминированный с лавинным методом формирования ПРИ»;

– $ROUT_{\text{пар}}^{(\text{лав})}$ – «Параллельный детерминированный с лавинным методом формирования ПРИ»;

– $ROUT_{\text{посл}}^{(\text{стат})}$ – «Последовательный детерминированный с статистическим методом формирования ПРИ»;

– $ROUT_{\text{пар}}^{(\text{стат})}$ – «Параллельный детерминированный со статистическим методом формирования ПРИ».

3. Пакеты ε-го приложения $(\varepsilon = \overline{1,\mathrm{E}}; \mathrm{E} = 3)$ поступают в мультисервисную сеть связи с интенсивностью $\lambda = \lambda_\varepsilon; \varepsilon = \overline{1,\mathrm{E}}$, величина которой может принимать одно их значений: $\lambda_1 = 10 \cdot 10^6$; $\lambda_2 = 50 \cdot 10^6$.

4. $H = H_\varepsilon = 0{,}5$; $\varepsilon = \overline{1,\mathrm{E}}$ – параметр Херста ε-го приложения.

5. Вероятность поступления потока данных ε-го приложения в a_R-й УИ для его последующей передачи a_L-му УП определяется матрицей тяготений:

$$\Pi_\varepsilon = \left\| \pi_{\varepsilon,R,L} \right\|_{S,S}.$$

Элементы матрицы тяготений:

$$0 \le \pi_{\varepsilon,R,L} \le 1; \sum_{R,N=1}^{S} \pi_{\varepsilon,R,L} = 1; \varepsilon = \overline{1,\mathrm{E}}$$

равны между собой и имеют равновероятный характер.

6. Внешнее деструктивное воздействие на элементы МСС представим в виде матрицы:

$$P_{\text{дес}} = \| \ p^{j}_{\text{дес}\ i} \ \|_{S,S},$$

где $p^{j}_{\text{дес}\ i}$ – вероятность выхода из строя ребра $m_{i,j}$ исходного графа $G[A_S, M_S]$, описывающего структуру мультисервисной сети связи.

Примем $p_{\text{дес}} = p^{j}_{\text{дес}\ i}; i, j = \overline{1,S}$, значение которой будем изменять от 0 до 0,6 с шагом $\Delta p_{\text{дес}} = 0{,}05$.

Графики зависимостей вероятности отказа в обслуживании в целом по мультисервисной сети связи (интегральная оценка (4.28)) при $\lambda_1 = 10 \cdot 10^6$ и $\lambda_2 = 50 \cdot 10^6$ соответственно, представлены на рисунках 5.14 и 5.15 [12, 78, 158]. Погрешность измерений в исследованиях определялась по формуле (4.31) и не превышает одного процента.

Из графиков рисунка 5.14 видно, что при ($\lambda_1 = 10 \cdot 10^6$) низкой интенсивности поступления пакетов ε-го приложения ($\varepsilon = \overline{1,\mathrm{E}}; \mathrm{E} = 3$) в МСС характер влияния методов маршрутизации на интегральную оценку (4.28)) в целом одинаковое.

Возрастание интенсивности поступления пакетов в МСС до $\lambda_2 = 50 \cdot 10^6$ приводит к существенному увеличению вероятности отказа в обслуживании в целом по мультисервисной сети связи. Причем «Лавинные» методы имеют существенное преимущество по сравнению со «Статистическими». Так же подтверждается результат, полученный в разделах 4.2 (рисунок 4.1 и 4.2) и 5.2

(рисунки 5.10, 5.11 и 5.12) – в условиях внешнего деструктивного воздействия, при

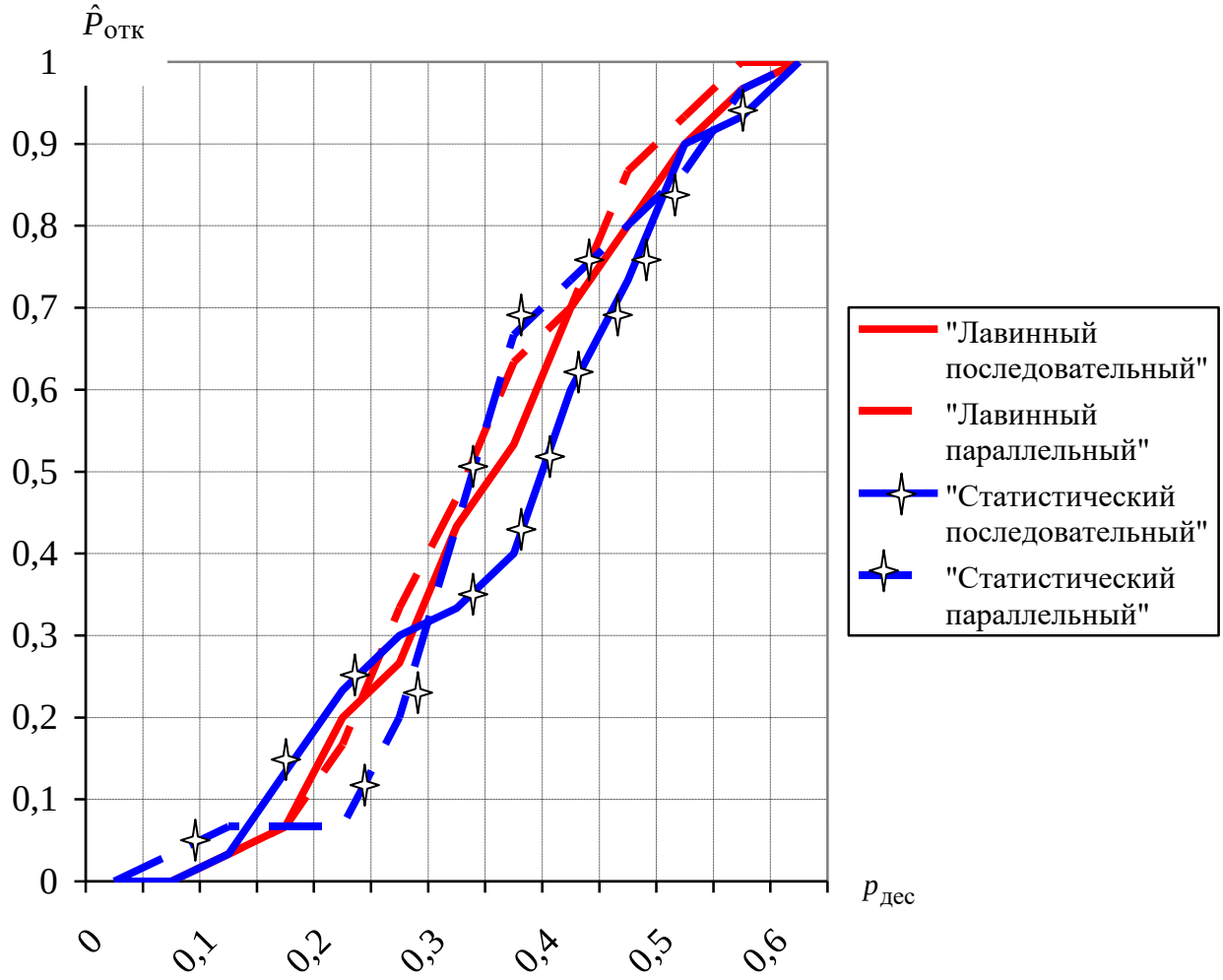


Рисунок 5.14 – Зависимости вероятности отказа в обслуживании в целом по мультисервисной сети связи (интегральная оценка) при $\lambda_1 = 10 \cdot 10^6$

котором около 30% сетевых ресурсов выходит из строя, целесообразно применять «Лавинные» методы формирования плана распределения информации с параллельным выбором исходящих ТПС.

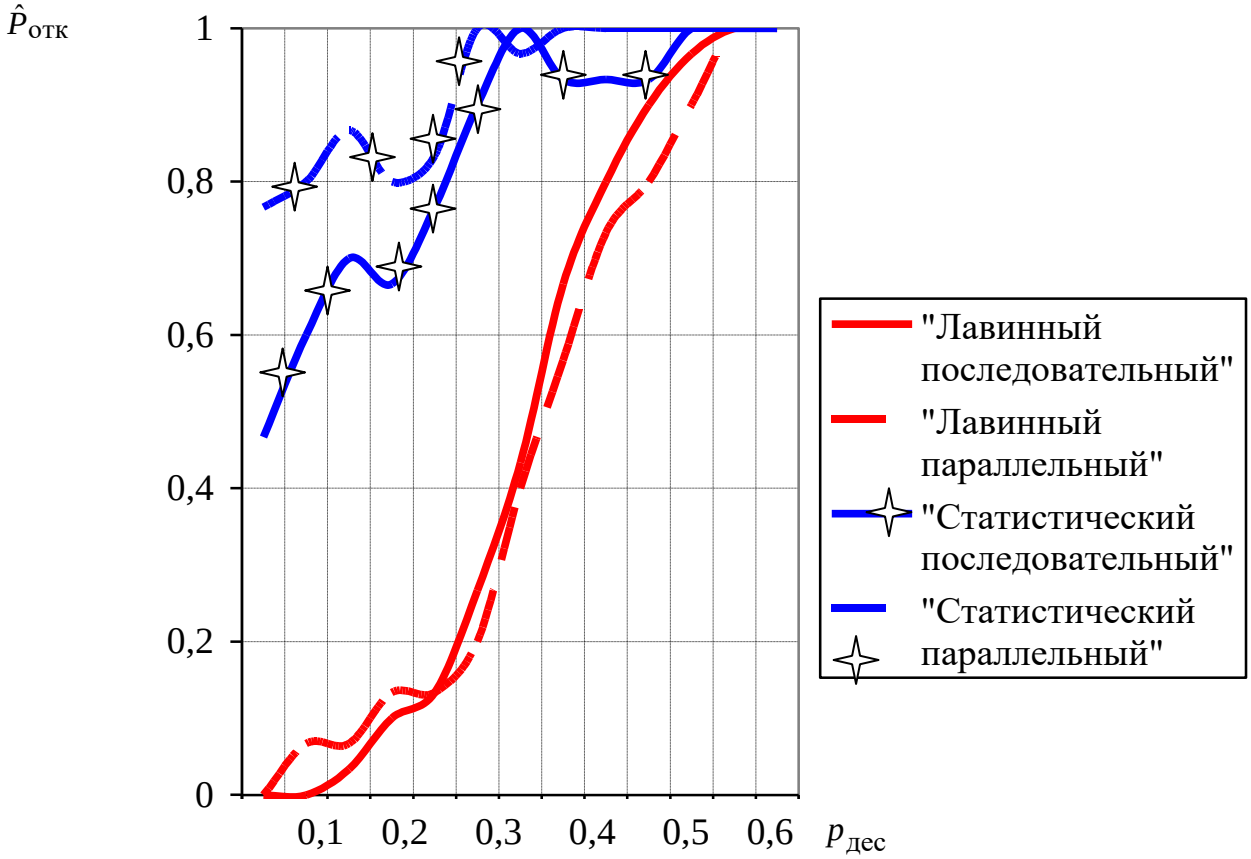


Рисунок 5.15 – Зависимости вероятности отказа в обслуживании в целом по мультисервисной сети связи (интегральная оценка) при $\lambda_2 = 50 \cdot 10^6$

5.4 Анализ результатов статистического моделирования маршрутизации на упрощенной имитационной модели сети связи

Приведем результаты статистического моделирования процедур маршрутизации на упрощенной имитационной модели сети связи (4.47). (4.48) при следующих условиях.

При определении плана распределения информации будем использовать методику для однородной ячеистой сети связи большой размерности представленной в разделе 4.4.

В соответствии с рисунком 4.9 примем: $X_{\max} = 10$ (максимальное количество УК по оси X); $Y_{\max} = 5$ (максимальное количество УК по оси Y); $S = X_{\max} \cdot Y_{\max} = 50$ (количество УК в анализируемой сети связи);

$k_{i,j} = 8; i, j = \overline{1,50}$; $p_{\text{дес}} = p^{j}_{\text{дес}\ i}; i, j = \overline{1,S}$, значение которой будем изменять от 0 до 0,8 с шагом $\Delta p_{\text{дес}} = 0{,}2$; равновероятный выбор УИ и УП, то есть значения элементов матрицы тяготений $\pi_{i,j} = \frac{1}{S^2}; i, j = \overline{1,S}$; $N_{\text{о}} = 1000$; относительная погрешность результатов статистического моделирования не превышает 8 процентов при $\beta = 0{,}955$ (4.31).

При заданных условиях выберем для анализа следующие методы маршрутизации:

$ROUT_{\text{ГВДПЛ}}$ – «Градиентный вероятносто-детерминированный последовательный с логическим методом формирования плана распределения информации»;

$ROUT_{\text{ДБВВДПЛ}}$ – «Диффузный без возвращения назад вероятносто-детерминированный последовательный с логическим методом формирования плана распределения информации»;

$ROUT_{\text{ДВДПЛ}}$ – «Диффузный вероятносто-детерминированный последовательный с логическим методом формирования плана распределения информации»;

$ROUT_{\text{ЛВДЛ}}$ – «Локально-лавинный с детерминированным выбором зоны поиска маршрута и логическим методом формирования плана распределения информации».

На рисунках 5.16 представлены результаты статистического моделирования методов маршрутизации [73, 78].

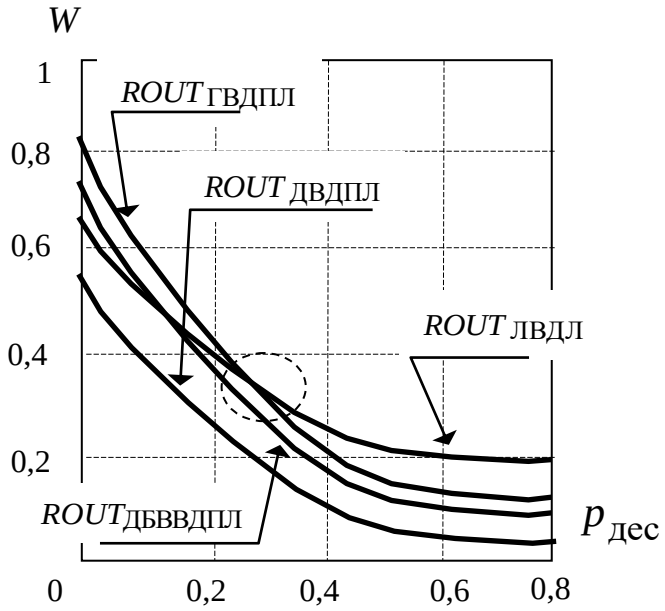


Рисунок 5.16 – Зависимость $W = f(P_{\text{дес}})$
для различных методов маршрутизации

Анализ результатов моделирования методов маршрутизации показал, что при отсутствии или незначительном внешнем деструктивном воздействии (в условиях, при котором до 20 % сетевых ресурсов выходит из строя) целесообразно применять «Статистические» методы маршрутизации. В случае выхода из строя более 20 % сетевых ресурсов необходимо использовать «Лавинные» методы маршрутизации.

5.5 Выводы

Проведенные исследования методов маршрутизации (с использованием различных математических и имитационных моделей) в условиях внешних деструктивных воздействий на элементы мультисервисной сети связи позволяют сделать следующие выводы.

1. Применение того или иного метода маршрутизации актуально для конкретных масштабов внешнего деструктивного воздействия.

2. В условиях отсутствия внешнего деструктивного воздействия «Статистические последовательные» методы маршрутизации обеспечивают

больший пользовательский сетевой ресурс по сравнению с «Лавинными» методами, следовательно, увеличивают возможность передачи большего объема пользовательской информации.

3. Анализ функционирования мультисервисной сети связи в условиях внешних деструктивных воздействий показал (усредненные данные), что в случае выхода из строя более 30% элементов мультисервисной сети связи параллельные методы маршрутизации позволяют понизить до 20% среднюю вероятность отказа заявок пользователей на обслуживание. Данный результат независимо подтвержден на различных структурах мультисервисных сетей связи и с применением различных математических и имитационных моделей.

4. В случае невозможности смены «Статистических последовательных» методов маршрутизации на «Лавинные параллельные» в условиях внешних деструктивных воздействий необходимо на этапе проектирования мультисервисных сетей связи предусматривать не менее 30 % резерва их сетевых ресурсов.

5. В том случае, если на этапе проектирования мультисервисных сетей связи предусматривать не менее 30 % резерва сетевых ресурсов, то это позволит:

– в условиях внешних деструктивных воздействий на элементы мультисервисной сети связи увеличить возможность передачи большего объема пользовательской информации;

– реализовать защиту пользовательской информации (конфиденциальность, доступность и целостность) за счет параллельных (многопутевых) методов маршрутизации путем использования территориально-распределенных ресурсов в мультисервисных сетях связи (каналов связи, криптографических программно-аппаратных комплексов, баз данных и так далее).

6 Разработка методик защиты информации за счет сетевых ресурсов мультисервисной сети связи

6.1 Постановка задачи

Разработанные в предыдущих главах:

– методы обеспечения базовых параметров защиты информации (конфиденциальность, доступность и целостность);

– параллельные (многопутевые) методы маршрутизации

и проведенные исследования методов маршрутизации в мультисервисных сетях связи в условиях внешних деструктивных воздействий позволяют выработать методики защиты информации за счет привлечения территориально-распределенных ресурсов в мультисервисных сетях связи (каналов связи, криптографических программно-аппаратных комплексов, баз данных и так далее).

Целью данных методик является защитить информацию [69] при ее передаче по МСС. Пользователю со стороны МСС (оператора МСС) предоставляется не только выбор приложения (видео, телефония, телеметрия, видеоконференция и т.д.) для передачи информации, но и тарифный план, обеспечивающий защиту информации. Тарифный план может быть представлен в нескольких вариантах, например в виде:

– количественных оценок параметров информационной безопасности (вероятности обеспечения целостности, доступности и конфиденциальности);

– качественных параметров информационной безопасности («Высокая», «Низкая» или «Средняя» степень защищенности).

Пользователь определяет свой профиль защиты информации для выбранного приложения. Система управления, проведя мониторинг свободных ресурсов мультисервисной сети связи, реализует не только соединение,

поддерживающее QoS для выбранного приложения, но и заявленный пользователем профиль [157] в виде структуры соединений защиты информации.

6.2 Разработка методики обеспечения целостности информации за счет сетевых ресурсов мультисервисной сети связи

Суть методики обеспечения целостности информации за счет сетевых ресурсов МСС представлена на рисунке 6.1 в виде алгоритма последовательности действий [2, 67, 77, 78, 83, 107].

Достижение заданной пользователем целостности передаваемой информации ($P_{\text{ц}}^{(\text{п})}$) (оператор 01 алгоритма концепции методики (рисунок 6.1)) обеспечивается за счет реализации *n* параллельных соединений между УИ и УП (рисунок 2.4) и в УП принятия решения по правилу (2.8).

Для этого необходимо, чтобы протоколы маршрутизации (методы формирования плана распределения информации (рисунок 3.7)) провели мониторинг МСС и сформировали базы данных параметров (скорость передачи информации, время задержки, вероятность ошибочного приема на символ и так далее) состояния элементов сети (оператор 02 рисунка 6.1).

В результате формируются таблицы маршрутизации (например, от источника) для каждого приложения $\left(\varepsilon = \overline{1,\mathrm{E}}\right)$ мультисервисной сети связи:

$$M_{\varepsilon}{}^{(j)} = \left(\overline{\mu_{(\varepsilon)1}^{(j)}},\ldots,\overline{\mu_{(\varepsilon)i}^{(j)}},\ldots,\overline{\mu_{(\varepsilon)j-1}^{(j)}},\overline{\mu_{(\varepsilon)j+1}^{(j)}},\ldots,\overline{\mu_{(\varepsilon)S}^{(j)}}\right), \varepsilon = \overline{1,\mathrm{E}}; \tag{6.1}$$

$$\overline{\mu_{(\varepsilon)i}^{(j)}} = \left(\langle \mu_{(\varepsilon)i1}^{(j)}\rangle,\ldots,\langle \mu_{(\varepsilon)iv}^{(j)}\rangle,\ldots\langle \mu_{(\varepsilon)im_j}^{(j)}\rangle\right), i,\ j = \overline{1,S}; i \neq j, \varepsilon = \overline{1,\mathrm{E}}, \tag{6.2}$$

где

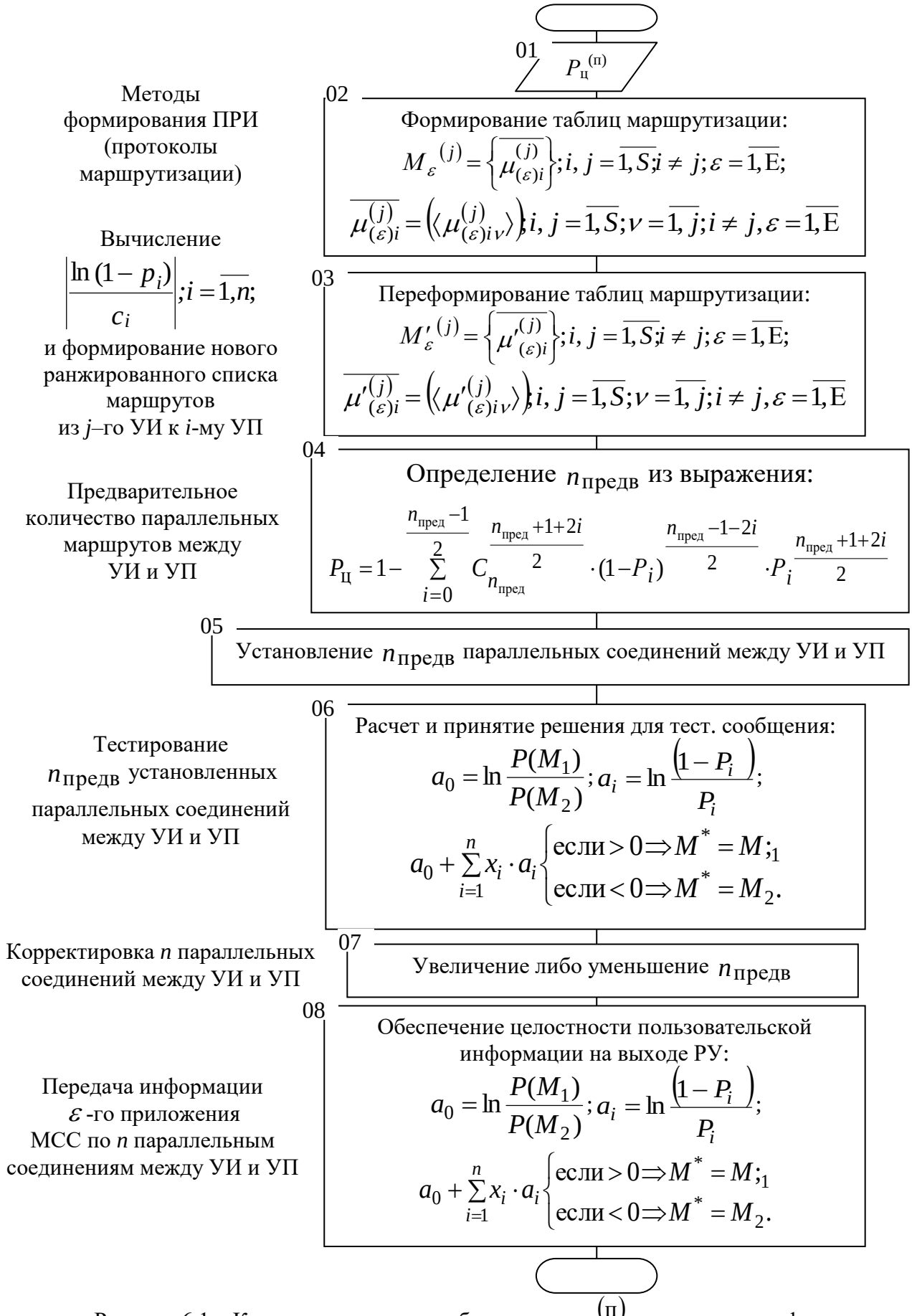


Рисунок 6.1 – Концепция методики обеспечения $P_{\text{ц}}^{(\text{п})}$ целостности информации

$\overline{\mu_{(\varepsilon)i}^{(j)}}$ – ранжированный по предпочтительности список маршрутов из *j*-го УИ к *i*-му УП при передачи информации ε-го приложения МСС;

$\left\langle \mu_{(\varepsilon)i\nu}^{(j)} \right\rangle$ – маршрут (список элементов сети) ν-го по предпочтительности выбора из *j*-го УИ к *i*-му УП при передачи информации ε-го приложения МСС;

m_j – количество маршрутов в ранжированном списке из *j*-го УИ к *i*-му УП.

На следующим этапе (оператор 03 рисунка 6.1) необходимо для каждого маршрута (6.2) таблиц маршрутизации (6.1) вычислить значение (2.17) и в соответствии с ним сформировать новый ранжированный убывающий по предпочтительности список маршрутов из *j*–го УИ к *i*-му УП для каждого ε-го приложения МСС:

$$M'^{(j)}_{\varepsilon} = \left(\overline{\mu'^{(j)}_{(\varepsilon)1}},\ldots,\overline{\mu'^{(j)}_{(\varepsilon)i}},\ldots,\overline{\mu'^{(j)}_{(\varepsilon)j-1}},\overline{\mu'^{(j)}_{(\varepsilon)j+1}},\ldots,\overline{\mu'^{(j)}_{(\varepsilon)S}}\right), \varepsilon = \overline{1,\mathrm{E}}; \tag{6.3}$$

$$\overline{\mu'^{(j)}_{(\varepsilon)i}} = \left(\langle\mu'^{(j)}_{(\varepsilon)i1}\rangle,\ldots,\langle\mu'^{(j)}_{(\varepsilon)i\nu}\rangle,\ldots\langle\mu'^{(j)}_{(\varepsilon)im_j}\rangle\right), i, j = \overline{1,S}; i \neq j, \varepsilon = \overline{1,\mathrm{E}}. \tag{6.4}$$

В качестве параметров формулы (2.17) можно использовать следующие.

Для c_i – вместо стоимости $\left\langle \mu'^{(j)}_{(\varepsilon)i\nu} \right\rangle$-го маршрута можно использовать количество транзитных УК между УИ и УП.

В качестве p_i можно использовать:

– надежность $\left\langle \mu'^{(j)}_{(\varepsilon)i\nu} \right\rangle$-го маршрута, выраженную в вероятностных величинах;

– $(1-p_{\text{ош}\,i})$, где $p_{\text{ош}\,i}$ – вероятность ошибочного приема символа, пакета, сообщения и т.п. при передачи информации по $\left\langle \mu'^{(j)}_{(\varepsilon)i\nu} \right\rangle$-му маршруту;

– $(1-p_{\text{м}\,i})$, здесь $p_{\text{м}\,i}$ – вероятность модификации информации, передаваемой по $\left\langle \mu'^{(j)}_{(\varepsilon)i\nu} \right\rangle$-му маршруту.

Операторы 04 ÷ 07 алгоритма (рисунок 6.1) определяют и устанавливают *n* параллельных соединений между УИ и УП.

Математическое выражение (2.9), позволяющее определить величину *n*, получено при условии, что модификации $M=\{M_1, M_2\}$ на всех соединениях (рисунок 2.4) являются независимыми событиями, а их вероятности равны между собой, т.е. $P_{\text{м}}=P_{\text{м}}^{(i)}; i=\overline{1,n}$. Поэтому определение количества параллельных соединений состоит из двух этапов – предварительного (операторы 04, 05 и 06) и окончательного (оператор 07).

На предварительном этапе, используя значения графиков $P_{\text{ц РУ}} = f(P_{\text{м}})$ (рисунок 2.6), определяется $n_{\text{предв}}$ (оператор 04). Далее система управления МСС, применяя протоколы сигнализации (методы выбора исходящих ТПС (рисунок 3.7)), устанавливает между УИ и УП $n_{\text{предв}}$ соединений (оператор 05).

Окончательное определение величины *n* состоит в:

– тестировании установленных $n_{\text{предв}}$ параллельных соединений (оператор 06);

– принятии решения в УП по правилу (2.8) (оператор 06);

– корректировке *n* (увеличении либо уменьшении $n_{\text{предв}}$) (оператор 07).

После установления *n* параллельных соединений (данную процедуру реализуют методы выбора исходящих ТПС − протоколы сигнализации), считается, что на МСС сформирована структура соединений защиты информации, обеспечивающая ее целостность. Далее, используя правило принятия, представленное оператором 08, решающее устройство, расположенное в УП, реализует целостность информации.

6.3 Разработка методики обеспечения доступности информации за счет сетевых ресурсов мультисервисной сети связи

Концепция методики обеспечения доступности информации за счет сетевых ресурсов МСС представлена на рисунке 6.2 [3, 77, 78, 107].

Достижение заданной пользователем доступности передаваемой информации ($P_{Д}^{(п)}$) (оператор 01), по аналогии с концепцией обеспечения целостности, обеспечивается за счет организации n параллельных соединений между УИ и УП (рисунок 2.4).

Протоколы маршрутизации осуществляют мониторинг МСС и формируют таблицы маршрутизации (6.1) для каждого приложения мультисервисной сети связи $\left(\varepsilon = \overline{1,\mathrm{E}}\right)$ (оператор 02).

На следующим этапе (оператор 03) формируется новый ранжированный, убывающий по предпочтительности список маршрутов (6.3) из j–го УИ к i-му УП для каждого ε-го приложения МСС.

Операторы 04 ÷ 07 определяют и устанавливают n параллельных соединений между УИ и УП.

После установления n параллельных соединений считается, что на МСС сформирована структура соединений защиты информации, обеспечивающая ее доступность.

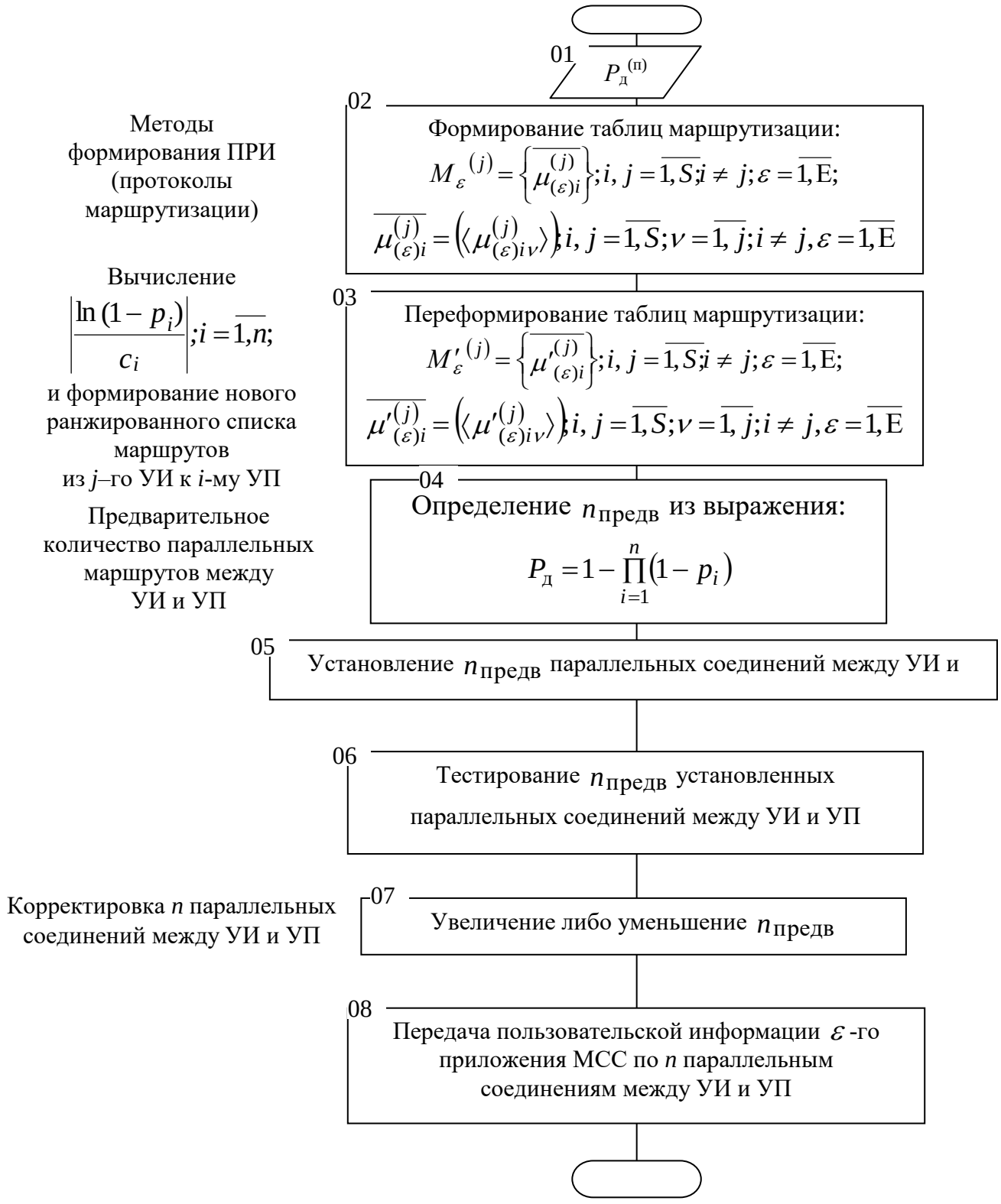


Рисунок 6.2 – Концепция методики обеспечения $P_{\text{д}}^{(\text{п})}$ доступности информации

6.4 Разработка методики обеспечения конфиденциальности информации за счет сетевых ресурсов мультисервисной сети связи

Данная методика может быть применена в МСС для случая обеспечения высокой степени конфиденциальности информации при использовании высокоскоростных приложений, критичных к задержкам, например видеоконференции.

В основу данной методики заложен механизм многократного асимметричного шифрования (2.1) открытой информации в УИ и расшифрования закрытой информации в УП [4, 67, 72, 77, 78, 82]. Демонстрация многократного ассиметричного шифрования представлена на рисунке 2.2.

Концепция методики обеспечения конфиденциальности информации (2.1) представлена на рисунке 6.3.

Для достижения заданной пользователем конфиденциальности $P_{\text{к}}^{(\text{п})}$ передаваемой информации (оператор 01) необходимо наличие (оператор 02):

– установленного протоколами сигнализации (методами выбора исходящих ТПС) соединения между УИ и УП;

– в УИ и УП соответствующего специализированного программно-аппаратного комплекса, обеспечивающего асимметричное шифрование.

В УП генерируется l независимых пар открытых $k_i^{(\text{о})}$ и $k_i^{(\text{с})}$ секретных ключей (оператор 03):

$$\left\{k_i^{(\text{о})}; k_i^{(\text{с})}\right\}, i = \overline{1,l}.$$

Открытые ключи $k_i^{(\text{о})}; i = \overline{1,l}$, по установленному соединению передаются из УП в УИ (оператор 04).

В УИ выполняется процедура многократного асимметричного шифрования (оператор 05):

$$y = E_{k_l^{(\text{о})}}\left\{..E_{k_i^{(\text{о})}}...[E_{k_1^{(\text{о})}}(M)]\right\}$$

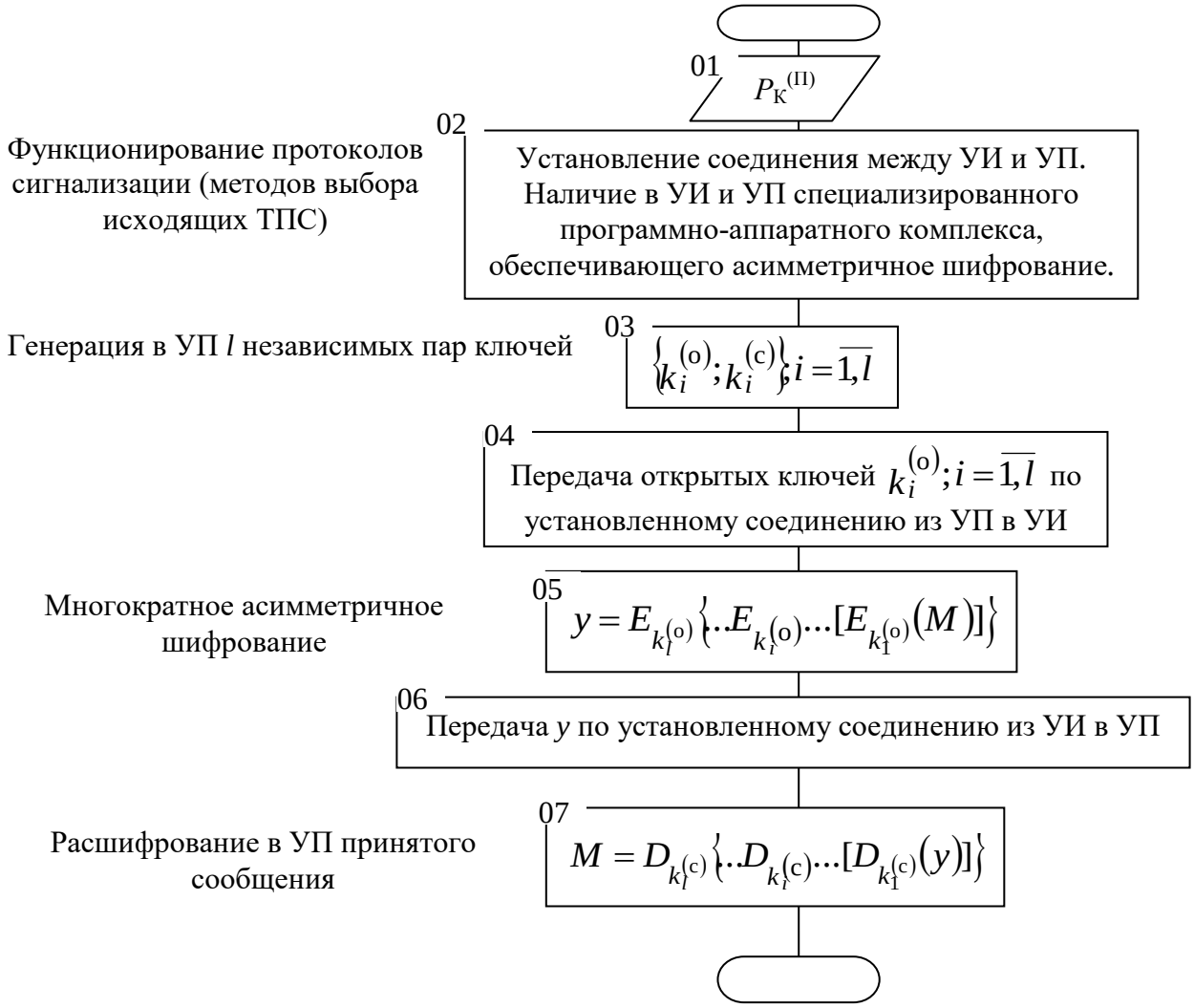


Рисунок 6.3 – Концепция методики обеспечения $P_к^{(п)}$ конфиденциальности информации

Зашифрованное сообщение y передается по установленному соединению из УИ в УП (оператор 06).

Принятое в УП сообщение расшифровывается (оператор 07):

$$M = D_{k_l^{(с)}}\{..D_{k_i^{(с)}}...[D_{k_1^{(с)}}(y)]\}.$$

6.5 Разработка методики защиты информации за счет сетевых ресурсов мультисервисных сетей связи

Концепция методики защиты информации в МСС включает в себя последовательное применение разработанных методик обеспечения доступности, конфиденциальности, целостности и представлена на рисунках 6.4, 6.5 и 6.6 [77, 78, 107].

Достижение заданных пользователем параметров защиты передаваемой информации ($P_{\text{Д}}^{(\text{п})}, P_{\text{К}}^{(\text{п})}, P_{\text{Ц}}^{(\text{п})}$) (оператор 01) обеспечивается за счет организации структуры соединений защиты, представляющей из себя n параллельных соединений между УИ и УП.

С этой целью протоколы маршрутизации осуществляют мониторинг МСС и формируют во всех УК таблицы маршрутизации (например, от источника) (оператор 02) для каждого приложения мультисервисной сети связи $\left(\varepsilon = \overline{1,\text{E}}\right)$:

$$M_{\varepsilon}{}^{(j)} = \left(\overline{\mu_{(\varepsilon)1}^{(j)}},\ldots,\overline{\mu_{(\varepsilon)i}^{(j)}},\ldots,\overline{\mu_{(\varepsilon)\,j-1}^{(j)}},\overline{\mu_{(\varepsilon)\,j+1}^{(j)}},\ldots,\overline{\mu_{(\varepsilon)S}^{(j)}}\right), \varepsilon = \overline{1,\text{E}};$$

$$\overline{\mu_{(\varepsilon)i}^{(j)}} = \left(\langle\mu_{(\varepsilon)i1}^{(j)}\rangle,\ldots,\langle\mu_{(\varepsilon)i\nu}^{(j)}\rangle,\ldots\langle\mu_{(\varepsilon)im_j}^{(j)}\rangle\right); i, j = \overline{1,S}; i \neq j, \varepsilon = \overline{1,\text{E}}.$$

Здесь:

$\overline{\mu_{(\varepsilon)i}^{(j)}}$ – ранжированный по предпочтительности список маршрутов из j-го УИ к i-му УП при передачи информации ε-го приложения МСС;

$\left\langle \mu_{(\varepsilon)i\nu}^{(j)} \right\rangle$ – маршрут (список элементов сети) ν-го по предпочтительности выбора из j-го УИ к i-му УП при передачи информации ε-го приложения МСС;

m_j – количество маршрутов в ранжированном списке из j-го УИ к i-му УП.

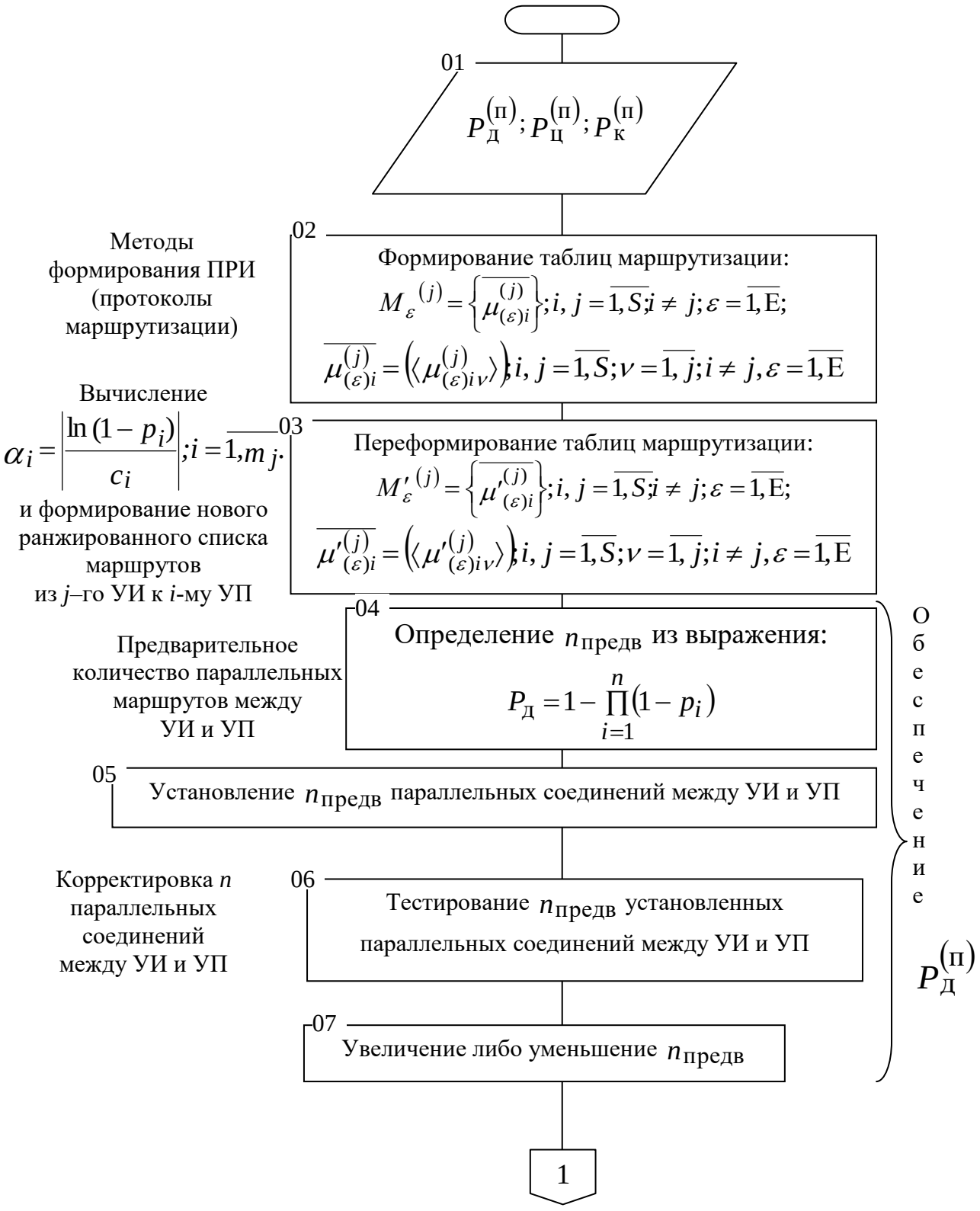


Рисунок 6.4 – Концепция методики защиты информации

На следующим этапе (оператор 03) последовательно выполняются процедуры.

1. Расчет для каждого маршрута $\left\langle \mu_{(\varepsilon)i\nu}^{(j)} \right\rangle$ значения:

$$\alpha_i = \left| \frac{\ln(1-p_i)}{c_i} \right|; i = \overline{1, m_j}.$$

Здесь в качестве переменных c_i и p_i можно использовать следующие.

Для c_i – вместо стоимости $\left\langle \mu^{(j)}_{(\varepsilon) i \nu} \right\rangle$-го маршрута можно использовать количество транзитных УК между УИ и УП.

В качестве p_i можно использовать:

– надежность $\left\langle \mu^{(j)}_{(\varepsilon) i \nu} \right\rangle$-го маршрута, выраженную в вероятностных величинах;

– $(1-p_{\text{ош}\,i})$, где $p_{\text{ош}\,i}$ – вероятность ошибочного приема символа, пакета, сообщения и т.п. при передачи информации по $\left\langle \mu^{(j)}_{(\varepsilon) i \nu} \right\rangle$-му маршруту;

– $(1-p_{\text{м}\,i})$, здесь $p_{\text{м}\,i}$ – вероятность модификации информации при передачи по $\left\langle \mu^{(j)}_{(\varepsilon) i \nu} \right\rangle$-му маршруту.

2. Перестановка маршрутов в новый ранжированный убывающий по предпочтительности список. Более предпочтительным является тот маршрут, у которого $\alpha_i; i = \overline{1, m_j}$ является большим значением.

В результате для каждого ε-го приложения МСС формируются таблицы маршрутизации:

$$M'^{(j)}_{\varepsilon} = \left(\overline{\mu'^{(j)}_{(\varepsilon)1}}, \ldots, \overline{\mu'^{(j)}_{(\varepsilon) i}}, \ldots, \overline{\mu'^{(j)}_{(\varepsilon) j-1}}, \overline{\mu'^{(j)}_{(\varepsilon) j+1}}, \ldots, \overline{\mu'^{(j)}_{(\varepsilon) S}} \right), \varepsilon = \overline{1, \text{E}};$$

$$\overline{\mu'^{(j)}_{(\varepsilon) i}} = \left(\langle \mu'^{(j)}_{(\varepsilon) i 1} \rangle, \ldots, \langle \mu'^{(j)}_{(\varepsilon) i \nu} \rangle, \ldots \langle \mu'^{(j)}_{(\varepsilon) i m_j} \rangle \right), i, j = \overline{1, S}; i \neq j, \varepsilon = \overline{1, \text{E}}.$$

Операторы 04 ÷ 07 определяют и устанавливают n параллельных соединений между УИ и УП для обеспечения доступности ($P_{Д}^{(п)}$) информации в МСС.

Определение количества параллельных соединений состоит из двух этапов – предварительного (операторы 04 ÷ 06) и окончательного (оператор 07).

На предварительном этапе, применяя:

$$P_{Д} = 1 - \prod_{i=1}^{n} (1 - p_i),$$

определяется $n_{предв}$ (оператор 04). Далее система управления МСС, используя протоколы сигнализации, устанавливает между УИ и УП $n_{предв}$ предварительных параллельных соединений (оператор 05).

Окончательное определение величины n состоит в:

– в тестировании $n_{предв}$ установленных предварительных параллельных соединений (оператор 06);

– корректировке n (увеличении либо уменьшении $n_{предв}$) (оператор 07).

По окончании установления n параллельных соединений считается, что на МСС сформирована структура соединений защиты информации, обеспечивающая ее доступность.

Следующим этапом методики является определение необходимого количества параллельных соединений между УИ и УП (рисунок 6.5) для обеспечения целостности информации в МСС (операторы 08 и 09).

Определение количества параллельных соединений состоит из двух этапов – предварительного (оператор 08) и окончательного (оператор 09).

На предварительном этапе со стороны УИ в сторону УП посылается тест–сигнал. Передача тест-сигнала осуществляется по заранее установленным

параллельным соединениям для обеспечения доступности пользовательской информации. Решающее устройство, которое расположено в УП, выполняет:

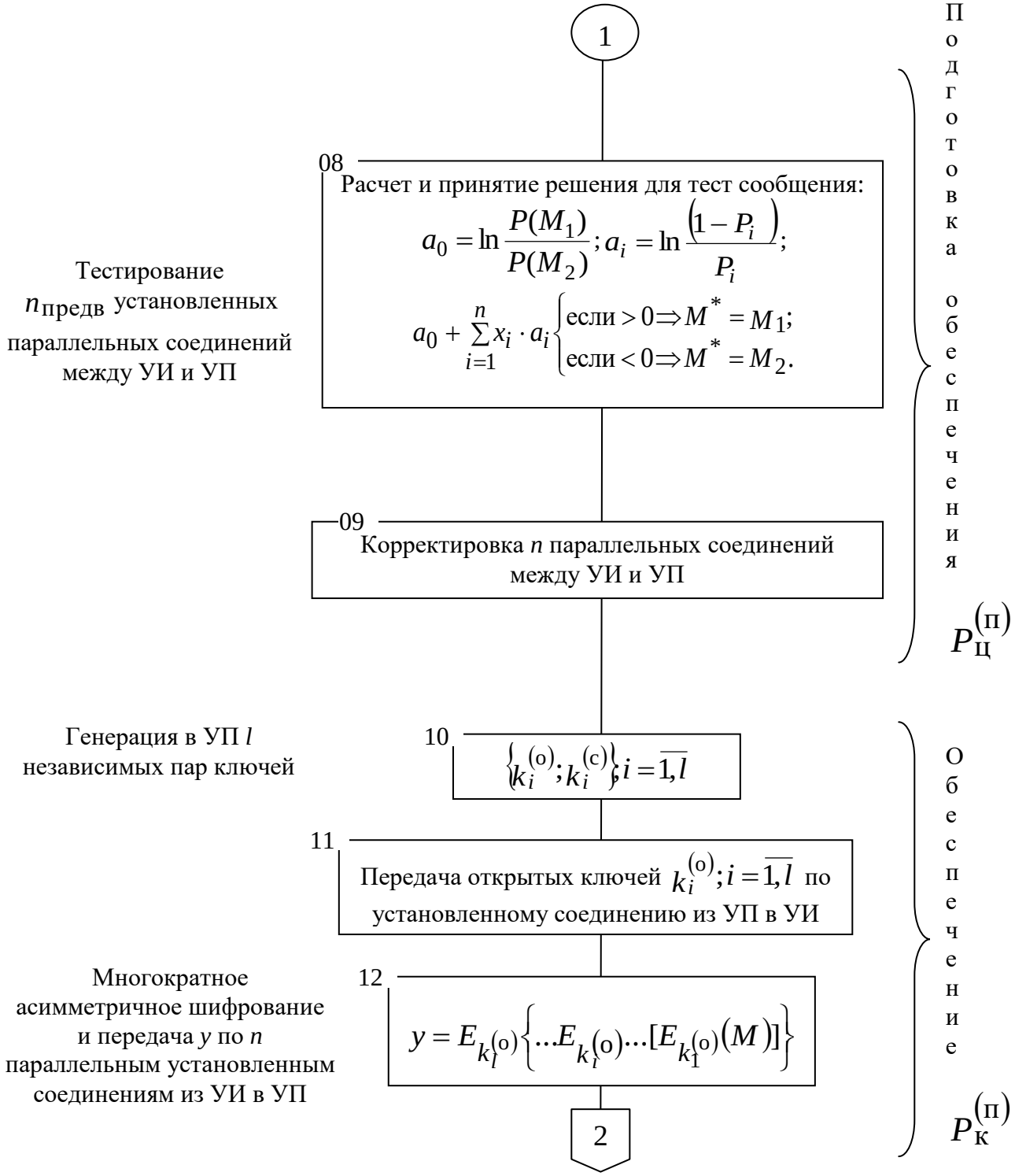


Рисунок 6.5 – Продолжение концепции методики защиты информации

– процедуру восстановления принятого тест-сигнала по правилу:

$$a_0 = \ln \frac{P(M_1)}{P(M_2)};\ a_i = \ln \frac{(1-P_i)}{P_i};$$

$$a_0 + \sum_{i=1}^{n} x_i \cdot a_i \begin{cases} \text{если} > 0 \Rightarrow M^* = M_1; \\ \text{если} < 0 \Rightarrow M^* = M_2; \end{cases}$$

– сравнение принятого тест-сигнала с переданным.

В случае недостаточного значения величины $P_{\text{Ц}}^{(\text{п})}$ принимается решение о добавлении дополнительных параллельных соединений между УИ и УП.

По окончании установления *n* параллельных соединений (данную процедуру реализуют методы выбора исходящих ТПС (протоколы сигнализации)) считается, что на МСС сформирована структура соединений защиты информации, обеспечивающая ее доступность и целостность.

Для достижения заданной пользователем конфиденциальности передаваемой информации ($P_{\text{К}}^{(\text{п})}$) в УП генерируется *l* независимых пар открытых $k_i^{(\text{о})}$ и $k_i^{(\text{с})}$ секретных ключей (оператор 10):

$$\left\{k_i^{(\text{о})}; k_i^{(\text{с})}\right\}; i = \overline{1,l}\,.$$

Открытые ключи $k_i^{(\text{о})}; i = \overline{1,l}$, по установленным соединениям передаются из УП в УИ (оператор 11).

На данном этапе считается, что структура защиты информации между УИ и УП сформирована. МСС готова:

– передавать информацию с QoS выбранного пользователем приложения;

– реализовать заявленный пользователем (по тарифному плану) профиль защиты информации ($P_{\text{Д}}^{(\text{п})}$, $P_{\text{К}}^{(\text{п})}$, $P_{\text{Ц}}^{(\text{п})}$).

В УИ выполняется процедура многократного асимметричного шифрования (оператор 12):

$$y = E_{k_l^{(\text{о})}}\left\{..E_{k_i^{(\text{о})}}...[E_{k_1^{(\text{о})}}(M)]\right\}$$

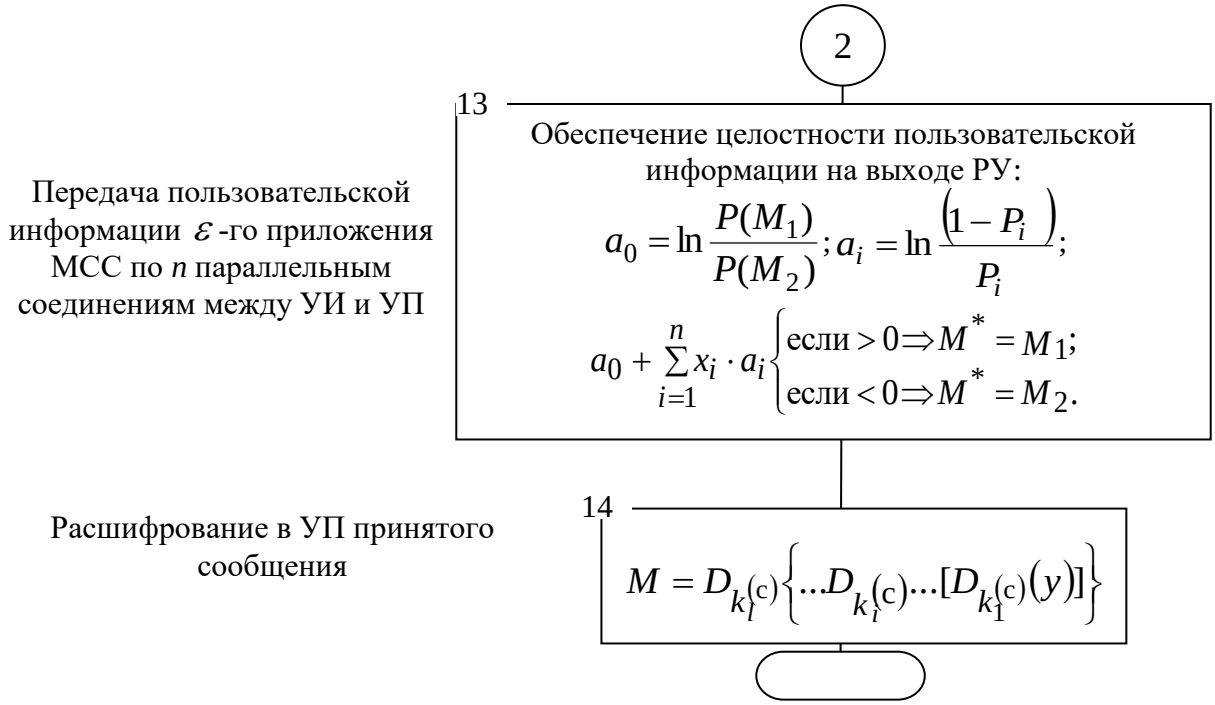


Рисунок 6.6 – Продолжение концепция методики защиты информации

Зашифрованное сообщение y передается по n параллельным установленным соединениям из УИ в УП.

Принятое в УП сообщение обрабатывается решающим устройством (рисунок 6.6, оператор 13) по правилу:

$$a_0 = \ln \frac{P(M_1)}{P(M_2)};\ a_i = \ln \frac{(1-P_i)}{P_i};$$

$$a_0 + \sum_{i=1}^{n} x_i \cdot a_i \begin{cases} \text{если} > 0 \Rightarrow M^* = M_1; \\ \text{если} < 0 \Rightarrow M^* = M_2 \end{cases}.$$

Тем самым реализуется целостность информации.

Далее сообщение y расшифровывается (оператор 14):

$$M = D_{k_l^{(c)}} \{ .. D_{k_i^{(c)}} ... [D_{k_1^{(c)}}(y)] \}.$$

В результате обеспечивается конфиденциальность информации.

По окончанию сеанса связи структура защиты информации между УИ и УП расформировывается. Сетевые ресурсы, задействованные в данном сеансе связи, для защиты и передачи информации с QoS освобождаются.

6.6 Выводы

Предложенные методики позволяют обеспечить защиту информации в мультисервисных сетях связи без снижения QoS высокоскоростных приложений, функционирующих в реальном масштабе времени (критичных к задержкам).

Методики ориентированы на разработчиков в области информационной безопасности телекоммуникационных систем, а так же на операторов мультисервисных сетей связи.

ЗАКЛЮЧЕНИЕ

Выполненные в диссертации исследования и разработанные теоретические положения позволили *решить научную проблему, имеющую важное хозяйственное значение, внедрение которой вносит значительный вклад* в развитие технологий защиты информации в современных телекоммуникационных системах связи. В рамках решения этой проблемы предложена методология защиты информации в мультисервисных сетях связи, отличающаяся тем, что конфиденциальность, целостность и доступность информации обеспечивается за счет технологий сетевого уровня модели взаимосвязи открытых систем (протоколов маршрутизации и сигнализации). Тем самым, на время сеанса связи, для защиты информации пользователям предоставляется возможность привлечения территориально-распределенных ресурсов сети (каналов связи, баз данных, специализированных криптографических, программно-аппаратных комплексов и т.п.) без снижения качества обслуживания высокоскоростных приложений, функционирующих в реальном масштабе времени.

Выполненные в работе научные исследования представлены следующими новыми результатами.

1. *Разработана методология*, основанная на протоколах сетевого уровня мультисервисных сетей связи, которая позволяет обеспечить базовые параметры информационной безопасности (конфиденциальность, доступность, целостность).

2. *Предложен подход* к обеспечению конфиденциальностм информации, использующий многократное асимметричное шифрование ключами меньшей длины позволяет уменьшить время шифрования в l^{c-1} раз, где l – количество асимметричных шифрований, c – постоянная, значение которой определяется криптографическими алгоритмами шифрования.

3. *Предложен критерий*, позволяющий выбирать маршруты с точки зрения обеспечения целостности и доступности передаваемой информации в мультисервисных сетях связи при минимальной стоимости.

4. *Разработаны способ и алгоритм*, отличающиеся тем, что для обеспечения целостности информации используют параллельные (многопутевые) методы маршрутизации, что позволяет уменьшить время задержки передачи информации.

5. *Разработан алгоритм* обеспечения доступности информации в мультисервисных сетях связи, отличающийся тем, что между узлом-источником и узлом-получателем устанавливают параллельные соединения, обеспечивающие вероятностно-стоимостные параметры.

6. *Предложена новая классификация* методов маршрутизации, отличающаяся наличием независимых процедур − формированием плана распределения информации на сети и выбором исходящих трактов передачи информации в узлах коммутации, что позволяет: выявить новые методы маршрутизации; провести целенаправленный анализ и синтез методов маршрутизации, которые будут эффективно функционировать в условиях штатной эксплуатации и внешних деструктивных воздействий на элементы мультисервисной сети связи.

7. *Предложен новый метод* маршрутизации («Гибридный»), отличающийся тем, что в зависимости от степени воздействия внешних деструктивных факторов на мультисервисную сеть связи, используют «Логический», «Статистический» или «Лавинный» методы, что позволяет сократить объем передаваемой служебной информации в мультисервисной сети связи во время ввода узлов коммутации в эксплуатацию, штатной эксплуатации и в условиях внешних деструктивных воздействий на элементы сети.

8. *Разработан инструментарий* (методики, модели, алгоритмы, программные продукты) позволяющий проводить анализ методов маршрутизации в мультисервисной сети связи и включающий в себя:

– математическую модель для оценки влияния методов формирования плана распределения информации на объем сетевых ресурсов;

– математическую модель маршрутизации в условиях входного самоподобного трафика и внешних деструктивных воздействий на элементы мультисервисной сети связи;

– методики определения плана распределения информации на однородной ячеистой сети связи большой размерности;

– упрощенную имитационную модель маршрутизации;

– способ проверки графа сети на связность, отличающийся тем, что анализируемый граф «разбивают» на подграфы; каждый подграф проверяют на связность «стягиванием» смежных вершин, к первоначально выбранной, до тех пор, пока подграф не представится в виде одиночной точки или множества точек; в результате формируется суперграф, который проверяется на связность «стягиванием» смежных вершин, к первоначально выбранной, до тех пор, пока суперграф не представится в виде одиночной точки (исходный граф связен) или множества точек (исходный граф не связен); это позволяет уменьшить алгоритмическую сложность решения задачи в $\sqrt{S}$ (S – количество вершин графа) по сравнению с известными способами.

9. *Проведен анализ* функционирования мультисервисной сети связи в условиях внешних деструктивных воздействий, который показал (усредненные данные), что в случае выхода из строя более 30% элементов мультисервисной сети связи параллельные (многопутевые) методы маршрутизации позволяют понизить до 20% среднюю вероятность отказа заявок пользователей на обслуживание.

10. *Разработан инструментарий* (методики, методы, алгоритмы), позволяющий за счет применения новых методов маршрутизации, реализовать защиту информации с обеспечением показателей качества обслуживания приложений мультисервисной сети связи.

Практическая значимость результатов подтверждена их использованием на ряде предприятий. Практическую ценность представляют:

– разработанные методики, методы, алгоритмы, математические модели, программные продукты для анализа и синтеза систем защиты информации в мультисервисных сетях связи;

– учебно-методические комплексы на основе разработанных методик, методов, алгоритмов, математических моделей и программных продуктов, для проведения всех видов занятий для студентов и магистрантов специальности «Информационная безопасность телекоммуникационных систем» в ВУЗах телекоммуникационного профиля в дисциплинах: «Основы проектирования защищенных телекоммуникационных систем»; «Основы технической эксплуатации защищенных телекоммуникационных систем»; «Живучесть телекоммуникационных систем»; «Телекоммуникационные технологии с гарантированным качеством обслуживания»; «Моделирование систем».

Перспективы дальнейшей разработки темы

Представленные в диссертации подходы к защите информации являются перспективными для реализации параметров информационной безопасности, представленных в ITU-T Recommendation X.805 Security Architecture for Systems providing end-to-end Communications. Особое внимание представляет развитие исследований и разработок, которые могли бы быть использованы в программно-конфигурируемых сетях (SDN, Software-defined Networking).

СПИСОК СОКРАЩЕНИЙ

БД	База данных	
ВВХ	Вероятностно-временная характеристика	
ВК	Виртуальный канал	
ВТ	Виртуальный тракт	
ЕАСС	Единая автоматизированная сеть связи	
КС	Канал связи	
ЛС	Линия связи	
МВОС	Модель взаимосвязи открытых систем	
МСС	Мультисервисная сеть связи	
ПРИ	План распределения информации	
РУ	Решающее устройство	
ТК	Таблица коммутации	
ТКС	Телекоммуникационная система	
ТМ	Таблица маршрутизации	
ТПС	Тракт передачи сообщений	
ТУ	Транзитный узел	
УИ	Узел-источник	
УК	Узел коммутации	
УП	Узел-получатель	
ЦСИО	Цифровая сеть интегрального обслуживания	
ATM	Asynchronous Transfer Mode	Асинхронный метод передачи
IP	Internet Protocol	Интернет протокол
MPLS	Multiprotocol Label Switching	Многопротокольная коммутация с использованием меток
QoS	Quality of Service	Гарантированное качество обслуживания

СПИСОК УСЛОВНЫХ ОБОЗНАЧЕНИЙ

c_i	Стоимость i-ого соединения между узлом-источником и узлом-получателем
C_o	Стоимость организации параллельных соединений
D_k	Функция расшифрования с помощью секретного ключа k
E_k	Функция зашифрования с помощью секретного ключа k
l	Количество «вложенных» алгоритмов шифрования
L_k	Длина ключа алгоритма зашифрования/расшифрования
M	Исходное сообщение пользователя
$M^{(j)}$	Таблица маршрутизации для j-го узла коммутации
m	Количество транзитных узлов в соединении между узлом-источником и узлом-получателем
n	Количество независимых параллельных маршрутов между узлом-источником и узлом-получателем
N_o	Количество независимых испытаний в методе статистического моделирования
$P_{\text{м}}$	Вероятность модификации сообщения
$P_{\text{ц}}$	Вероятность целостности сообщения
$R_{\text{о}}$	Общий средний сетевой ресурс мультисервисной сети связи
$R_{\text{п}}$	Средний ресурс, выделяемый мультисервисной сетью связи для передачи пользовательской информации
$R_{\text{тм}}$	Средний ресурс, выделяемый мультисервисной сетью связи для передачи служебной информации, участвующей в формировании плана распределения информации
$ROUT$	Способ маршрутизации на сети связи

$ROUT_{\text{сс}}$	Способ формирования таблиц коммутации
$ROUT_{\text{тм}}$	Способ формирования таблиц маршрутизации
S	Количество узлов коммутации в сети
$t_{\text{ш}}$	Время зашифрования исходного сообщения пользователя
Y	Зашифрованное сообщение
Δ_a	Абсолютное значение погрешности (половина доверительного интервала)
χ_j	Количество исходящих трактов передачи сообщений из j-го узла коммутации
$\Psi_{-}(t)$	Отрицательное внешнее воздействие (воздействия внешних деструктурирующих факторов) на мультисервисную сеть связи с целью несанкционированного использования общего сетевого ресурса

СПИСОК ЛИТЕРАТУРЫ

1. Агеев, Д. В. Методика определения параметров потоков на разных участках мультисервисной телекоммуникационной сети с учетом самоподобия [Электронный ресурс] / Д. В. Агеев, А. А. Игнатенко, А. Н. Копылев // Проблемы телекоммуникаций : электрон. науч. специализир. изд.–журнал. – 2011. – № 5. – С. 16–37. – Режим доступа: http://pt.journal.kh.ua.

2. Алгоритм обеспечения целостности пользовательской информации в сетях с гарантированным качеством обслуживания на сетевом уровне : свидетельство об отраслевой регистрации разработки № 15062 / С. Н. Новиков, О. И. Солонская. – № 50200901147 ; заявл. 23.11.2009 ; опубл. 02.12.2009. – 1 с.

3. Алгоритм, позволяющий обеспечить требуемый пользователем уровень доступности информации : свидетельство об отраслевой регистрации разработки № 16227 / С. Н. Новиков, О. И. Солонская. – № 50201001615 ; заявл. 29.09.2010 ; опубл. 05.10.2010. – 1 с.

4. Алгоритм, позволяющий обеспечить требуемый пользователем уровень конфиденциальности информации в мультисервисных сетях связи : свидетельство об отраслевой регистрации разработки № 16462 / С. Н. Новиков, О. И. Солонская. – № 50201050230 ; заявл. 06.12.2010 ; опубл. 08.12.2010. – 1 с.

5. Алгоритм и программа проверки сети на связность способом «Свертка» : листок / А. Н. Данилов, С. Н. Новиков; Гос. ФАП СССР. – № 50850000756, 1985.

6. Анализ живучести сетей : извещение о государственной регистрации в Отраслевом фонде алгоритмов и программ / С. Н. Новиков, А. Н. Гольник. – № 50200100095 ; зарегистрировано 02.04.2001. – 1 с.

7. Анализ методов маршрутизации в широкополосных цифровых сетях интегрального обслуживания (Ш-ЦСИО) : извещение о государственной регистрации в Отраслевом фонде алгоритмов и программ / С. Н. Новиков, А. А. Буров. – № 50200401220 ; зарегистрировано 18.10.2004. – 1 с.

8. Андронов, И.С. Передача дискретных сообщений по параллельным каналам. / И.С. Андронов, Л.М. Финк. – М.: Сов. радио, 1971. – 408 с. : ил.

9. Бахарева, Н. Ф. Анализ и расчет непуассоновских моделей трафика в сетях ЭВМ / Н. Ф. Бахарева, И. В. Карташевский, В. Н. Тарасов // Инфокоммуникационные технологии. – 2009. – Т. 7, № 4. – С. 61–66.

10. Бертсекас, Д. Сети передач данных : пер. с англ. / Д. Бертсекас, Р. Галлагер. – М. : Мир, 1989. – 544 с.

11. Богатырев, В. А. Надежность двухуровневой отказоустойчивой компьютерной системы при дублировании связей между узлами / В. А. Богатырев // Вестн. компьютер. и информ. технологий. – 2009. – № 1. – С. 2–7.

12. Буров, А. А. Исследование влияния маршрутизации на качество обслуживания в мультисервисных сетях связи, функционирующих в экстремальных условиях : автореф. дис. … канд. техн. наук : 05.12.13 / А. А. Буров. – Новосибирск, 2009. – 22 с.

13. Бусленко, Н. П. Моделирование сложных систем / Н. П. Бусленко. – М. : Наука, 1968. – 356 с.

14. Бычков, Е. Д. Математические модели управления состояниями цифровой телекоммуникационной сети с использованием теории нечётких множеств : монография / Е. Д. Бычков. – Омск : Изд-во ОмГТУ, 2010. – 236 с.

15. Величко, В. В. Модели и методы повышения живучести современных систем связи / В. В. Величко, Г. В. Попков, В. К. Попков. – М. : Горячая линия-Телеком, 2014. – 270 с. : ил.

16. Вишневский, В. М. Теоретические основы проектирования компьютерных сетей / В. М. Вишневский. – М. : Техносфера, 2003. – 512 с.

17. Гавлиевский, С. Л. Итерационный метод расчета характеристик сетей при использовании для рассылки пакетов направленной волны / С.Л. Гавлиевский // Вестн. Воронеж. гос. ун-та. Сер.: Системный анализ и информационные технологии. – 2011. – № 2. – С. 51–59.

18. Гавлиевский, С. Л. Математическая модель для исследования свойств магистралей транспортных сетей при использовании нескольких классов

обслуживания / С. Л. Гавлиевский // Инфокоммуникационные технологии. – 2011. – Т. 9, N 4. – С. 23–27.

19. Гавлиевский, С. Л. Методы анализа мультисервисных сетей связи с несколькими классами обслуживания / С. Л. Гавлиевский. – М. : ИРИАС, 2010. – 365 с.

20. Гавлиевский, С. Л. Методы анализа мультисервисных сетей связи с несколькими классами обслуживания : автореф. дис. … д-ра техн. наук : 05.12.13 / С. Л. Гавлиевский. – М. : Самара, 2012. – 32 с.

21. Гладкий, В. С. Вероятностные вычислительные модели / В. С. Гладкий. – М. : Наука, 1973. – 300 с.

22. Гладкий, В. С. О некоторых принципах построения единой системы связи / В. С. Гладкий // Сети и системы передачи данных : материалы семинара. – М. : Знание, 1977. – С. 98 – 103.

23. Гладкий, В. С. Об одном методе маршрутизации на сети связи с коммутацией пакетов / В. С. Гладкий, С. Н. Новиков ; Моск. электротехн. ин-т связи. – М., 1984. – 15 с. – Деп. в ЦНТИ «Информсвязь» 28.11.84, № 535.

24. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. – Введ. 2007-08-01. – М. : Изд-во стандартов, 2007. – 22 с.

25. Гудов, А. М. Имитационное моделирование процессов передачи трафика в вычислительных сетях / Гудов А. М., Семехина М. В. // Управление большими системами. Выпуск 31. М.: ИПУ РАН. – 2010. – С. 130–161.

26. Гургенидзе, А. Т. Мультисервисные сети и услуги широкополосного доступа / А. Т. Гургенидзе, В. И. Кореш. – СПб. : Наука и техника, 2003. – 400 с. : ил.

27. Дмитриев, В. Н. Имитационное моделирование системы мониторинга многозвенной сети передачи данных / В. Н. Дмитриев, А. С. Тушнов,

Е. В. Сергеева // Вестник АГТУ Сер.: Управление, вычислительная техника и информатика. – 2013. – № 2. – С. 86–91.

28. Егунов, М. М. Анализ структурной надёжности транспортной сети / М. М. Егунов, В. П. Шувалов // Вестник СибГУТИ. – 2012. – № 1 . – С. 54–60.

29. Елагин, В. С. Модели оперативного перехвата трафика в инфокоммуникационных сетях : автореф. дис. … канд. техн. наук : 05.12.13 / В. С. Елагин. – СПб., 2011. – 20 с.

30. Зайнуллина, Э. Ш. Модели и методы решения задачи оптимальной маршрутизации данных в корпоративных сетях : автореф. дис. … канд. физ.-мат. наук : 05.13.18 / Э. Ш. Зайнуллина. – Казань, 2008. – 16 с.

31. Зайцев, Д. А. Исследование эффективности технологии MPLS с помощью раскрашенных сетей Петри / Д. А. Зайцев, А. Л. Сакун // Зв'язок. – 2006. – № 5. – С. 49–55.

32. Зарубин, А. А. Исследование контакт-центров в NGN : автореф. дис. … канд. техн. наук : 05.12.13 / А. А. Зарубин. – СПб., 2004. – 19 с.

33. Иванов, И. П. Математические модели, методы анализа и управления в корпоративных сетях : автореф. дис. … д-ра техн. наук : 05.13.15 / И. П. Иванов. – М., 2010. – 34 с.

34. Игнатенко, А. П. Противодействие атакам на отказ в сети интернет: выбор среды моделирования / А. П. Игнатенко, Д. В. Цицкун // Проблеми програмування. – 2008. № 2-3. Спеціальний випуск С. 579–586.

35. Интерфейс "Пользователь - ЭВМ" для анализа живучести телекоммуникационных систем : извещение о государственной регистрации в Отраслевом фонде алгоритмов и программ / С. Н. Новиков, Е.В Сафонов. – № 50200100421 ; зарегистрировано 24.10.2001. – 1 с.

36. Карташевский, И. В. Программно-реализованная имитационная модель массового обслуживания общего вида / И. В. Карташевский, В. Н. Тарасов // Инфокоммуникационные технологии. – 2009. – Т. 7, № 2. – С. 63–68.

37. Квашненков, В. В. Метод отказоустойчивой передачи сообщений в сетях связи с многомерной маршрутизацией / В. В. Квашненков, Э. Н. Солдатенко // Телекоммуникации. – 2008. – № 5. – С. 6–9.

38. Клейнрок, Л. Вычислительные системы с очередями : пер. с англ. / Л. Клейнрок. – М. : Мир, 1979. – 600 с.

39. Концептуальные положения по построению мультисервисных сетей на ВСС России. – М. : Минсвязи, 2001. – 35 с.

40. Костин, А. А. Модели и методы проектирования систем управления телекоммуникационными сетями : автореф. дис. д-ра техн. наук : 05.12.13 / А. А. Костин. – СПб., 2003. – 33 с.

41. Крук, Б. И. Телекоммуникационные системы и сети. В 3 т. Т.1. Современные технологии : учеб. пособие / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под ред. В.П. Шувалова. – 3-е изд., испр. и доп. – М. : Горячая линия-Телеком, 2003. – 647 с.

42. Крылов, В. В. Теория телетрафика и ее приложения / В.В. Крылов, С.С. Самохвалова. – СПб. : БХВ-Петербург, 2005. – 288 с.

43. Кулаков, Ю. А. Алгоритмы безопасной маршрутизации для мобильных компьютерных сетей / Ю. А. Кулаков, А. А. Деревянчук // Проблемы информатизации и управления : Зб. наук. пр. – К.: НАУ, 2009. – Вып. 3 (27). – С. 99–103.

44. Кулаков, Ю. А. Многопутевая маршрутизация в беспроводных сетях / Ю. А. Кулаков, А. В. Левчук // Электроника и системы управления. – М. : НАУ, 2010. – № 4 (26). – С. 142–147.

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

46. Лазарев, В. Г. Игровой метод динамического управления сетью связи / В.Г. Лазарев // Построение управляющих устройств и систем / В. Г. Лазарев, Н. Я. Паршенков. – М. : Наука, 1974. – С. 161–172.

47. Лазарев, В. Г. Интеллектуальные цифровые сети : справочник /

В. Г. Лазарев ; под ред. Н. А. Кузнецова. – М. : Финансы и статистика, 1996. – 224 с. : ил.

48. Лазарев, В. Г. Метод динамической маршрутизации в У-ЦСИО / В. Г. Лазарев, Е. В. Гончаров // Электросвязь. –1999. – N 7. – С. 34–36.

49. Лемешко, А. В. Вероятностно-временная модель QoS маршрутизации с предвычислением путей в условиях неидеальной надежности элементов телекоммуникационной сети / А. В. Лемешко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2005. – Вып. 142. – С.

50. Лемешко, А. В. Модель многопутевой QoS-маршрутизации в мультисервисной телекоммуникационной сети / А. В. Лемешко, О. А. Дробот // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2006. – Вып. 144. – С. 16–22.

51. Лемешко, А. В. Тензорная модель многопутевой маршрутизации агрегированных потоков с резервированием сетевых ресурсов, представленная в пространстве с кривизной / А. В. Лемешко // Праці УНДІРТ. – Одесса, 2004. – Вып. №4 (40). – С. 12–18.

52. Лосев, Ю. И. Анализ моделей вероятности потери пакетов в буфере маршрутизатора с учетом фрактальности трафика / Ю. И. Лосев, К. М. Руккас // Вестн. харьк. нац. ун-та. Сер. «Мат. моделирование информ. технологий. Автоматизир. системы упр.». – 2008. – № 833. – С. 163–169.

53. Мао, В. Современная криптография: теория и практика : пер. с англ. / В. Мао. – М. : Издат. дом «Вильямс», 2005. – 768 с.

54. Мартынова, О. П. Адаптация многокритериальной маршрутизации к изменению состояний компьютерной сети / О. П. Мартынова // Весник ДУІКТ. – 2010. – Т. 8, № 2. – С. 101–106.

55. Мартынова, О. П. Применение многокритериальной маршрутизации для повышения информационной безопасности компьютерных сетей / О. П. Мартынова, А. А. Засядько, В. Л. Баранов // Проблемы информатизации та управления : зб. наук. пр. – К. : НАУ, 2007. – Вып. 3(21). – С. 109–113.

56. Маршрутизация и защита информации на сетевом уровне в мультисервисных сетях связи / А. А. Буров, А. А. Киселев, С. Н. Новиков, Е. В. Сафонов, О. И. Солонская ; под ред. С. Н. Новикова ; ГОУ ВПО СибГУТИ. – Новосибирск, 2004. – 221 с. – Деп. в ВИНИТИ 04.11.04, № 1732-В2004.

57. Математические модели исследования маршрутизации в сетях передачи данных / М. П. Березко, В. М. Вишневский, Е. В. Левнер, Е. В. Федотов // Информационные процессы. – 2001. – Т. 1, № 2. – С. 103–125.

58. Медведев, Н. В. Проблема разделения секрета на эллиптических кривых / Н. В. Медведев, С. П. Баутин, С. С. Титов // Проблемы прикладной математики и механики : сб. науч. тр. / УрГУПС. – Екатеринбург, 2008. – № 65(148). – С. 160–174.

59. Мейкшан, В. И. Анализ влияния отказов оборудования на функционирование мультисервисной сети с адаптивной маршрутизацией / В. И. Мейкшан // Доклады АН ВШ РФ. – 2010. – № 2(5). – С. 69–79.

60. Мелентьев, О. Г. Теоретические аспекты передачи данных по каналам с группирующимися ошибками / О. Г. Мелентьев ; под ред. проф. В. П. Шувалова. – М. : Горячая линия-Телеком, 2007. – 232 с.

61. Метод проверки телекоммуникационной системы на связность : свидетельство об отраслевой регистрации разработки № 2377 / С. Н. Новиков, А. А. Буров. – № 50200300153 ; заявл. 20.02.2003 ; опубл. 28.02.2003. – 1 с.

62. Методы расчета структурной надежности многоцелевых территориальных мультисервисных систем связи / Н. Н. Тютин, И. М. Успенский, С. М. Чудинов, О. Н. Кривошеев // Науч. ведомости БелГУ. Сер.: История. Политология. Экономика. Информатика. – 2009. – № 9-1-1. – С. 60–68.

63. Михеенко, В. С. Определение надежности и живучести сетей связи с адаптивной маршрутизацией сообщений / В. С. Михеенко // Электросвязь. – 2004. – № 8. – С. 36–39.

64. Мочалов, В. П. Разработка распределенных систем управления телекоммуникационными сетями и услугами : автореф. дис. … д-ра техн. наук : 05.13.01 / В. П. Мочалов. – Ставрополь, 2006. – 32 с.

65. Мошак, Н. Н. Модели, методы и алгоритмы анализа процессов функционирования инфотелекоммуникационных транспортных систем : автореф. дис. … д-ра техн. наук: 05.13.13 / Н. Н. Мошак. – СПб., 2009. – 32 с.

66. Новиков, А. А. Уязвимость и информационная безопасность телекоммуникационных технологий : учеб. пособие / А. А. Новиков, Г. Н. Устинов. – М. : Радио и связь, 2003. – 294 с.

67. Новиков, С. Н Основы обеспечения комплексной защиты пользовательской информации в мультисервисных сетях связи [Электронный ресурс] / С. Н. Новиков // Интернет-журнал "Технологии техносферной безопасности". – 2013. – № 2 (48). – 10 с. – Режим доступа: http://ipb.mos.ru/ttb.

68. Новиков, С. Н. Анализ влияния методов маршрутизации на объем доступных сетевых ресурсов / С. Н. Новиков, А. А. Буров // Науч.-техн. ведомости СПбГПУ. – 2009. – С. 41–47.

69. Новиков, С. Н. Защита информации в корпоративных телекоммуникационных системах / С. Н. Новиков // Экономика и производство. – 2003. – № 1. – С. 38–41.

70. Новиков, С. Н. Имитационное моделирование мультисервисной сети связи в условиях внешних, деструктивных воздействий / С. Н. Новиков, Д. А. Тахтараков // Современныеипроблемы телекоммуникаций : материалы Российской науч. - техн. конференции. – Новосибирск, 2015. – С. 602–608.

71. Новиков, С. Н. Исследование влияния внешних деструктивных воздействий на элементы мультисервисной сети связи / С. Н. Новиков, С. А. Петров // Вестник СибГУТИ. – 2016. – № 1. – С. 108–117.

72. Новиков, С. Н. Исследование возможности обеспечения конфиденциальности в мультисервисных сетях связи / С. Н. Новиков, О. И. Солонская // Доклады ТУСУР. – 2012. – № 1(25), ч. 2. – С. 213–215.

73. Новиков, С. Н. Исследование и разработка метода маршрутизации на ячеистых сетях связи в экстремальных условиях : автореф. дис. … канд. техн. наук : 05.12.14 / С. Н. Новиков. – М., 1986. – 20 с.

74. Новиков, С. Н. Классификация методов маршрутизации в мультисервисных сетях связи / С. Н. Новиков // Вестник СибГУТИ. – 2013. – № 1 (21). – С. 57–67.

75. Новиков, С. Н. Математическая модель анализа многоадресной маршрутизации в мультисервисной сети связи / С. Н. Новиков, В. О. Жарикова // Доклады ТУСУР. – 2012. – № 1(25), ч. 2. – С. 92–96.

76. Новиков, С. Н. Метод проверки графа на связность / С. Н. Новиков, С. А. Гончаров // Сети, узлы и распределение информации : сб. науч. тр. учеб. ин-тов связи / ЛЭИС. – Л., 1990. – С. 111–114.

77. Новиков, С. Н. Методологические аспекты защиты информации с использованием ресурсов мультисервисных сетей связи / С. Н. Новиков // Доклады ТУСУР. – 2014. – № 2 (32). – С. 130–136.

78. Новиков, С. Н. Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи / С. Н. Новиков ; под ред. В. П. Шувалова. – М. : Горячая линия - Телеком, 2015. – 128 с.

79. Новиков, С. Н. Методы защиты информации : учеб. пособие / С. Н. Новиков, О. И. Солонская ; Сиб. гос. ун-т телекоммуникаций и информатики. – Новосибирск, 2009. – 120 с.

80. Новиков, С. Н. Методы маршрутизации на цифровых широкополосных сетях связи.: учеб. пособие по специальности 200900-сети связи и системы коммутации / С. Н. Новиков. – Новосибирск : СибГУТИ.

Ч. 1.- 2001. – 83 с.

Ч. 2.- 2004.– 58 с.

81. Новиков, С. Н. Методы оценки структурной надежности телекоммуникационных систем : учеб. пособие : метод. комплекс / С. Н. Новиков, Е. В. Сафонов. – Новосибирск, 2004. – 44 с.

82. Новиков, С. Н. Обеспечение конфиденциальности передаваемой информации на сетевом уровне / С. Н. Новиков, О. И. Солонская // Науч.-техн.

ведомости СПбГПУ. Сер. «Информатика. Телекоммуникации. Управление». – 2009. − № 4 (82). – С. 60–64.

83. Новиков, С. Н. Обеспечение целостности в мультисервисных сетях / С. Н. Новиков, О. И. Солонская // Доклады ТУСУР . – 2009. – № 1(19), ч. 2. – С. 83–85.

84. Новиков С. Н. Разработка системы параметров оценки рисков нарушения информационной безопасности организаций / А. С. Поморцев, С. Н. Новиков // Доклады ТУСУР – 2014. № 2 (32).– С. 170−174.

85. Новиков, С. Н. Расчет структурной надежности на сети связи / С. Н. Новиков, Т. В. Куцева // Сети, узлы и распределение информации : сб. науч. тр. учеб. ин-тов связи / ЛЭИС. – Л., 1987. – С. 99–102.

86. Новиков, С. Н. Уменьшение дисперсии оценки структурной надежности сети связи при статистического моделирования / С. Н. Новиков // Вестник СибГУТИ. – 2013. – № 2 (22). – С. 69–74.

87. Обзор и сравнительный анализ основных моделей и алгоритмов многопутевой маршрутизации в мультисервисных телекоммуникационных сетях / В. В. Поповский, А. В. Лемешко, Л. И. Мельникова, Д. В. Андрушко // Прикладная радиоэлектроника. – 2005. – Т.4, вып. 4. – С. 372–382.

88. Перепелкин, Д. А. Методы и алгоритмы адаптивной маршрутизации в корпоративных вычислительных сетях : автореф. дис. … канд. техн. наук : 05.13.13 / Д. А. Перепелкин. – Рязань, 2009. – 32 с.

89. Петров, В. В. Структура телетрафика и алгоритм обеспечения качества обслуживания при влиянии эффекта самоподобия : дис. … канд. техн. наук : 05.12.13 / В. В. Петров. – М., 2004. – 199 с.

90. Петров, М. Н. Самоподобие в системах массового обслуживания с ограниченным буфером / М. Н. Петров, Д. Ю. Пономарев // Электросвязь. – 2002. – № 2. – С. 35–39.

91. Пирс, У. Построение надежных вычислительных машин. / У. Пирс. М.: Мир, 1968. – 270 с.

92. Пономарев, Д. Ю. Исследование моделей потоков вызовов [Электронный ресурс] / Д. Ю. Пономарев. – Режим доступа: http://www.nsc.ru/ws/YM2004/ 8509/index.html.

93. Пономарев, Д. Ю. Исследование моделей телекоммуникационных систем с непуассоновскими входными потоками / Д. Ю. Пономарев // Проблемы информатизации региона. ПИР-2001: сб. науч. тр. – Красноярск, 2002. – С. 145–152.

94. Пономарев, Д. Ю. Об обслуживании в системе с входным гамма потоком [Электронный ресурс] / Д. Ю. Пономарев. – Режим доступа: http:// www.sbras.ru/ws/YM2004/8510/

95. Попков, В. К. Математические модели связности / В. К. Попков ; отв. ред. А. С. Алексеев. – 2-е изд., испр. и доп. – Новосибирск : Изд - во ИВМиМГ СО РАН, 2006. – 490 с.

96. Программа оценки структурной надежности сетей связи / С. Н. Новиков, В. С. Гладкий, А. Н. Данилов ; Гос. ФАП СССР. – № 50870001283, 1987.

97. Пьянов, С. М. Сравнительный анализ стойкости некоторых классов схем разделения секрета : магист. дис. / С. М. Пьянов ; МГУ им. М.В. Ломоносова. – Москва, 2013. – 67 с.

98. Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации : Рекомендации по стандартизации. – Введ. 2006-01-01. – М. : Изд-во стандартов, 2005. – 13 с.

99. Р 50.1.056-2005. Техническая защита информации. Основные термины и определения : Рекомендации по стандартизации. – Введ. 2006-06-01. – М. : Изд-во стандартов, 2005. – 20 с.

100. Рейнгольд, Э. Комбинаторные алгоритмы. Теория и практика : пер. с англ. / Э. Рейнгольд, Ю. Нивергельд, Н. Део. – М. : Мир, 1980.– 476 с.

101. Рябко, Б. Я. Основы современной криптографии и стеганографии: монография / Б. Я. Рябко, А. Н. Фионов. – М. : Горячая линия-Телеком, 2010. – 232с.

102. Селифанов, В. А. Методы оценки структурной надежности мультисервисных систем при реализации инфокоммуникационных услуг на региональном уровне : автореф. дис. … канд. техн. наук / В. А. Селифанов. – М., 2011. – 19 с.

103. Сергеева, Т. П. Методы расчета динамической маршрутизации на международной телефонной сети России / Т. П. Сергеева, С. Е. Королькова // Электросвязь. – 2004. – № 8. – С. 25–29.

104. Сикарев, А.А., Оптимальный прием дискретных сообщений. / А.А. Сикарев, А.И. Фалько. – М.: Связь, 1978. – 328 с.

105. Симонина, О. А. Характеристики трафика в сетях IP / О. А. Симонина, Г. Г. Яновский // Тр. учеб. заведений связи. – 2004. – № 177. – С. 8–14.

106. Соколов, А. Н. Методы анализа задержек IP-пакетов в сети следующего поколения : автореф. дис. … канд. техн. наук : 05.12.13 / А. Н. Соколов. – СПб., 2011. – 20 с.

107. Солонская, О. И. Алгоритмы и методика защиты пользовательской информации в мультисервисных сетях связи : дис. … канд. техн. наук : 05.13.19 / О. И. Солонская. – Новосибирск, 2010. – 22 с.

108. Способ обеспечения целостности передаваемой информации : пат. 2513725 Рос. Федерация / С. Н. Новиков, О. И. Солонская. – Опубл. 20.04.14 // Изобретения. Полезные модели : Офиц. бюл. Федеральной службы по интеллектуальной собственности, № 11 – 2014, 20.04 2014.

109. Столингс, В. Криптография и защита сетей : принципы и практика : пер. с англ. / В. Столингс. – 2-е изд. – М. : Издат. дом «Вильямс», 2001. – 672 с.

110. Тарасюк, М. В. Защищенные информационные технологии. Проектирование и применение / М. В. Тарасюк. – М. : СОЛОН-Пресс, 2004. – 192 с.

111. Телекоммуникационные системы и сети. В 3 т. Т. 3. Мультисервисные сети : учеб. пособие / В. В. Величко, Е. А. Субботин, В. П. Шувалов,

А. Ф. Ярославцев ; под ред. В. П. Шувалова. – М. : Горячая линия-Телеком, 2005. – 592 с.

112. Толчан, А. Я. О связности сети / А. Я. Толчан // Проблемы передачи информации. Принципы построения сетей и систем управления. – М. : Наука, 1964. – Вып. 17. – С. 3–8.

113. Федорова, М. Л. Об исследовании свойства самоподобного трафика мультисервисной сети / М. Л. Федорова, Т. М. Леденева / Вестник ВГУ. Сер.: Системный анализ и информационные технологии. – 2010. – № 1. – С. 46–54.

114. Фергюсон, Н. Практическая криптография: пер. с англ. / Н. Фергюсон, Б. Шнайер. – М. : Издат. дом «Вильямс», 2005. – 424 с.

115. Фисенко, В. Е. Методология анализа и синтеза сложных информационных систем реального времени на основе встречно-соединенных дополнительных древовидных структур : автореф. дис. … д-ра техн. наук : 05.13.01/ Е. В. Фисенко. – Орел, 2008. – 38 с.

116. Финк, Л.М. Теория передачи дискретных сообщений. Изд. 2-е, переработанное, дополненное. / Л.М. Финк. – М.: Советское радио, 1970 – 728 с.

117. Фороузан, Б. А. Криптография и безопасность сетей : учеб. пособие / Б. А. Фороузан ; пер. с англ. под ред. А. Н. Берлина. – М. : Интернет – ун-т информ. технологий : Бином, 2010. – 783 с.

118. Харкевич, А. А. Информация и техника / А. А. Харкевич // Коммунист. – 1962. – № 17.− С.93–102.

119. Черемушкин, А. В. Криптографические протоколы. Основные свойства и уязвимости : учеб. пособие / А. В. Черемушкин. – М. : Академия, 2009. – 271 с.

120. Хорошевский, В.Г. Архитектура вычислительных систем: Учеб. пособие. — 2-е изд., перераб. и доп. / В.Г. Хорошевский — М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. — 520 с.: ил.

121. Шварц, М. Сети ЭВМ. Анализ и проектирование : пер. с англ. / М. Шварц. – М. : Радио и связь, 1981. – 336 с.

122. Шварцман, В. О. Актуальные вопросы теории и практики обеспечения информационной безопасности систем (сетей) общего пользования / В. О. Шварцман // Электросвязь. – 2007. – № 4. – С. 10–15.

123. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М. : Триумф, 2002. – 816 с.

124. Шнайер, Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. – СПб. : Питер, 2003. – 368 с.

125. Шувалов, В. П. Классификация методов многопутевой маршрутизации / В. П. Шувалов, И. Ю. Вараксина // T-Comm – Телекоммуникации и Транспорт. – 2014. – № 1. Том 8. С. 29–32.

126. Шувалов, В. П. Обеспечение показателей надежности телекоммуникационных систем и сетей / В. П. Шувалов, М. М. Егунов, Е. А. Минина. – М. : Горячая линия-Телеком, 2015. – 168 с. : ил.

127. Шувалов, В. П. Прием сигналов с оценкой их качества / В. П. Шувалов. – М. : Связь, 1979. – 240 с.

128. Электронное учебное пособие «Методы маршрутизации на цифровых широкополосных сетях связи» : свидетельство об отраслевой регистрации разработки № 2413 / С. Н. Новиков. – № 50200300206 ; заявл. 12.03.2003 ; опубл. 26.03.2003. – 1 с.

129. Элементы теории передачи дискретной информации / под ред. Л. П. Пуртова. – М. : Связь, 1972. – 232 с.

130. Ященко, В. В. Введение в криптографию / В. В. Ященко. – СПб. : МЦНМО, 2001. – 237 с.

131. A multipath protocol for secure and reliable data collection in wireless sensor networks : technical report / W. Lou, Y. Zhang , W. Liu, Y. Fang ; ECE department, Worcester Polytechnic Institute, June 2004.

132. Anil Kumar, V. Dynamic Broadcast Routing with Security Enhancement / V. Anil Kumar, B. Yakhoob, E. Pradeep // International Journal of Advances in Engineering & Technology. - May 2011. – Vol. 1, Iss. 2. – P. 20–27.

133. Asmuth, C. A modular approach to key safeguarding / C. Asmuth, J. Bloom // IE EE Transactions on Information Theory. – 1983. – Vol. it-29, No. 2. – P. 208–210.

134. ATM Forum Private Network-Network Interface Specification Version 1.1 (PNNI 1.1). ATM Forum – af-pnni-0055.001, March, 2001.

135. ATM Security Specification Version 2.0. ATM Forum – af-sec-0100.002, February, 2002.

136. ATM Security Specification. Version 1.1. af-src-0100.002. The ATM Forum. Technical Committee, March 2001.

137. Blakley, G. R. Safeguarding cryptographic keys / G. R. Blakley // Proc. Of AFIPS Nasiona1 Computer Conference. –1979. – № 48. – P. 313–317.

138. Chen, J. A new approach to routing with dynamic metrics / J. Chen, P. Druschel, D.Subramanian // Proc. IEEE INFOCOM, March 1999. – P. 661–670.

139. CACI Products [Электронный ресурс] : сайт. – Режим доступа: http://www.cacia sl.com.

140. CPN Tools [Электронный ресурс] : сайт. – Режим доступа: http://www.daimi.au.dk/CPNTools.

141. Dang, T. D. Fractal Analysis and Modeling of VoIP Traffic / T. D. Dang, B. Sonkoly, S. Molnar // Telecommunications Network Strategy and Planning Symposium. NETWORKS 2004, 11th International, 2004. – P. 217–222.

142. Downey, A. Lognormal and Pareto distributions in the Internet / A. Downey // Computer Communications. – 2005. – Vol. 28, No 7. – P. 790–801.

143. Elagha, H. On the Self-Similar Nature of ATM Network Traffic / H. Elagha, M. AlShafee // Issues in Informing Science and Information Technology.– 2007. – Vol. 4.

144. Investigating the efficiency of cryptographic algorithms in online transactions // C. Lamprecht, A. Van Moorsel, P. Tomlinson, N. Thomas // I. J. of SIMULATION. – 2006. – Vol. 7, No. 2. – P. 63–75.

145. ISO 7498-2. Information processing systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecture, 1989. . = ГОСТ

7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель.- 41с. – Действует с 01.01.2000.

146. ISO/IEC 10181-1. Information technology. Open Systems Interconnection. Security frameworks for open systems. – Part 1.Overview, 1996.-26 p.

147. 140/ ISO/IEC 10589. Information technology. Telecommunications and information exchange between systems. Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473), Second edition 2002-11-15.- 208 p.

148. Karnin, E. On secret sharing systems / E. Karnin, J. Greene, M. Hellman // IEEE Transactions on information theory. – 1983. – Vol. it-29, No. 1. – P. 35–41.

149. Lee, G. M. A survey of multipath routing for traffic engineering / G. M. Lee // Proc. of LNCS 3391. Springer-Verlag, 2005. - Vol. 4. – P. 635–661.

150. Lou ,W. A multipath routing approach for secure data delivery / W. Lou, Y. Fang // IEEE Military Communications Conference (MILCOM 2001), Mclean, VA, USA, Oct 2001.

151. Lou, W. SPREAD: Enhancing data confidentiality in mobile ad hoc networks / W. Lou, W. Liu, Y. Fang // IEEE INFOCOM 2004, Hong Kong, China, March 2004.

152. Make Systems [Электронный ресурс] : сайт. – Режим доступа: http:// www.make systems.com.

153. Multipath Optimized Link State Routing for Mobile ad hoc Networks / Yi тJiazi, Adnane Asmaa, David Sylvain, Parrein Benoıt // Ad Hoc Networks 9, 1. – 2011. – P. 28–47.

154. Nelakuditi, S. Adaptive proportional routing: A localized QoS routing approach / S. Nelakuditi, Z. Zhang, R.P. Tsang // Proc. IEEE INFOCOM, March 2000. – P. 1566–1575.

155. Novikov, S. N. A Mathematical model of routing in B-ISDN with ATM technology / S. N. Novikov // 6th International conference on actual problems of

electronic instrument engineering proceedings, APEIE – 2002. – Novosibirsk, 2002. – Vol. 1. – P. 173–175.

156. Novikov, S. N. Formal Interpretation of Network Tasks of Model OSI / A. A. Kiselev, S. N. Novikov // The IEEE International Siberian Conference on Control and Communications (SIBCON-2005), Russia, Tomsk, 2005. – P. 16–22.

157. Novikov, S. N. Information Security in Telecommunication Networks: Criteria and Protection profile / A. A. Kiselev, E. V. Safonov, S. N. Novikov // 5-th International Siberian Workshop on Electron Devices and Materials Proceedings, Erlagol, Altai – July 1-5, 2004. – P. 119–121.

158. Novikov, S. N. The Analysis of Probability Time Characteristics of a Telecommunication Network / S. N. Novikov, A. A. Burov // The IEEE International Siberian Conference on Control and Communications (SIBCON-2005), Russia, Tomsk, 2005. – P. 26–29.

159. NS2 [Электронный ресурс] : сайт. – Режим доступа: http://www.isi.edu/nsnam/ns/ns-build.html.

160. NS3 [Электронный ресурс] : сайт. – Режим доступа: http://www.nsnam.org.

161. OMNEST [Электронный ресурс] : сайт. – Режим доступа: http://www.omnest.com.

162. Opnet [Электронный ресурс] : сайт. – Режим доступа: http://www.opnet.com/university_program/itguru_academic_edition/.

163. Prateek, J. SMART: A Secure Multipath Anonymous Routing Technique / Jain Prateek, Bagchi Rupsha // International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN). – 2011. – Vol. 1, Iss. 2. – P. 1–6.

164. RFC 2205. Version 1 Functional Specification. Version 1 Functional Specification, September 1997.

165. RFC 2328. OSPF Version 2, April 1998.

166. RFC 2453. RIP Version 2, November 1998.

167. RFC 2460. Internet Protocol, Version 6 (IPv6) Specification, December 1998.

168. RFC 3031. Multiprotocol Label Switching Architecture, January 2001.

169. RFC 33209. RSVP-TE: Extensions to RSVP for LSP Tunnels. December 2001.

170. RFC 5420. Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE) February 2009.

171. Saksena, V. R. Topological Analysis of Packet Networks / V. R. Saksena // IEEE Journal Selected Areas in Comm. – 1989. – Vol. 7. – P. 1243–1252.

172. Shamir, A. How to share a secret / A. Shamir // Communications of the ACM. – 1979. - Vol. 22, №11. – P. 612-613; NY, USA: ACM, 1979. – T. 22, №11. – C. 612–613.

173. Sheluhin, O. I. Self-similar processes in telecommunications / O. I. Sheluhin, S. M. Smolskiy, A. V. Osin. – John Willey and Sons Ltd, 2007. – 337 p.

174. SPREAD: Improving network security by multipath routing in mobile ad hoc networks / W. Lou, Y. Zhang, W. Liu, Y. Fang // Wireless Netw. – 2009. – Vol. 15. – P. 279–294.

175. Taqqu, M. S. Proof of a Fundamental Result in Self-Similar Traffic Modeling / M. S. Taqqu, W. Willinger, R. Sherman // SIGCOMM Comput. Commun. Rev. – 1997. – Vol. 27, Iss. 2. – P. 5–23.

176. Tilovska, S. Performance Model of Key Points At the IPTV Networks / S. Tilovska, A. Tentov / International Journal of Computer Networks (IJCN). – 2011. – Vol. 3, Iss. 2. – P. 58–70.

177. Tsybakov, B. On self-similar traffic in ATM queues: definition, overflow probability bound, and cell delay distribution / B. Tsybakov, N. D. Georganas // IEEE/ACM Trans. on Networking. – 1997. – Vol. 5, No 3. – P. 397–408.

178. Using Game Theory to Analyze Wireless ad HOC Networks / V. Srivastava, J. Neel, A. B. Mackenzie, R. Menon, L. A. Dasilva, J. E. Hicks, J. H. Reed, R. P. Gilles // IEEE Communications Surveys & Tutorials, Fourth Quarter, 2005. – P. 46–56.

179. UTI-T Recommendation X.200 Open Systems Interconnection (OSI) – Model and notation, service definition, 11/1988.

180. UTI-T Recommendation X.800 Security Architecture for Open Systems Interconnection for CCITT Applications, 1991.

181. UTI-T Recommendation X.805 Security Architecture for Systems providing end-to-end Communications, 2003.

182. UTI-T Recommendation X.810 Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: over View), 1995.

183. Vutukury, S. Multipath routing mechanisms for traffic engineering and quality of service in the Internet / S. Vutukury // PhD Dissertation. University of Kalifornia, 2001. – P. 15.

184. Wiener, Michael J. DES is not a group / Michael J. Wiener,
Keith W. Campbell // Lecture Notes In Computer Science. – 1992. – Vol. 740. – P. 512–520.

СПИСОК ИЛЛЮСТРАТИВНОГО МАТЕРИАЛА

Перечень таблиц

Перечень рисунков

Приложение А

(справочное)

Список работ автора по теме диссертации

Статьи в ведущих рецензируемых журналах и изданиях, входящих в перечень ВАК

1. Новиков, С. Н. Анализ влияния методов маршрутизации на объем доступных сетевых ресурсов / С. Н. Новиков, А. А. Буров // Науч.-техн. ведомости СПбГПУ. – 2009. – С. 41–47.

2. Новиков, С. Н. Защита информации в корпоративных телекоммуникационных системах / С. Н. Новиков // Экономика и производство. – 2003. – № 1. – С. 38–41.

3. Новиков, С. Н. Исследование влияния внешних деструктивных воздействий на элементы мультисервисной сети связи / С. Н. Новиков, С. А. Петров // Вестник СибГУТИ. – 2016. – № 1. – С. 108–117.

4. Новиков, С. Н. Исследование возможности обеспечения конфиденциальности в мультисервисных сетях связи / С. Н. Новиков, О. И. Солонская // Доклады ТУСУР. – 2012. – № 1 (25), ч. 2. – С. 213–215.

5. Новиков, С. Н. Классификация методов маршрутизации в мультисервисных сетях связи / С. Н. Новиков // Вестник СибГУТИ. – 2013. – № 1 (21). – С. 57–67.

6. Новиков, С. Н. Математическая модель анализа многоадресной маршрутизации в мультисервисной сети связи / С. Н. Новиков, В. О. Жарикова // Доклады ТУСУР. – 2012. – № 1 (25), ч. 2. – С. 92–96.

7. Новиков, С. Н. Метод проверки графа на связность / С. Н. Новиков, С. А. Гончаров // Сети, узлы и распределение информации : сб. науч. тр. учеб. ин-тов связи / ЛЭИС. – Л., 1990. – С. 111–114.

8. Новиков, С. Н. Методологические аспекты защиты информации с использованием ресурсов мультисервисных сетей связи / С. Н. Новиков // Доклады ТУСУР. – 2014. – № 2 (32). – С. 130–136.

9. Новиков, С. Н. Обеспечение конфиденциальности передаваемой информации на сетевом уровне / С. Н. Новиков, О. И. Солонская // Науч.-техн. ведомости СПбГПУ. Сер. «Информатика. Телекоммуникации. Управление». – 2009. − № 4 (82). – С. 60–64.

10. Новиков, С. Н. Обеспечение целостности в мультисервисных сетях / С. Н. Новиков, О. И. Солонская // Доклады ТУСУР. – 2009. – № 1 (19), ч. 2. – С. 83–85.

11. Новиков, С. Н. Основы обеспечения комплексной защиты пользовательской информации в мультисервисных сетях связи [Электронный ресурс] / С. Н. Новиков // Интернет-журнал "Технологии техносферной безопасности". – 2013. – № 2 (48). – 10 с. – Режим доступа: http://ipb.mos.ru/ttb.

12. Новиков С. Н. Разработка системы параметров оценки рисков нарушения информационной безопасности организаций / А. С. Поморцев, С. Н. Новиков // Доклады ТУСУР – 2014. № 2 (32).– С. 170−174.

13. Новиков, С. Н. Расчет структурной надежности на сети связи / С. Н. Новиков, Т. В. Куцева // Сети, узлы и распределение информации : тр. учеб. ин-тов связи / ЛЭИС. – Л., 1987. – С. 99–102.

14. Новиков, С. Н. Уменьшение дисперсии оценки структурной надежности сети связи при статистическом моделировании / С. Н. Новиков // Вестник СибГУТИ. – 2013. – № 2 (22). – С. 69–74.

Патент на изобретение

15. Способ обеспечения целостности передаваемой информации : пат. 2513725 Рос. Федерация / С. Н. Новиков, О. И. Солонская. – Опубл. 20.04.14, Бюл. № 11.

Свидетельства на программы для электронных вычислительных машин, зарегистрированные в установленном порядке

16. Алгоритм обеспечения целостности пользовательской информации в

сетях с гарантированным качеством обслуживания на сетевом уровне : свидетельство об отраслевой регистрации разработки № 15062 / С. Н. Новиков, О. И. Солонская. – № 50200901147 ; заявл. 23.11.2009 ; опубл. 02.12.2009. – 1 с.

17. Алгоритм, позволяющий обеспечить требуемый пользователем уровень конфиденциальности информации в мультисервисных сетях связи : свидетельство об отраслевой регистрации разработки № 16462 / С. Н. Новиков, О. И. Солонская. – № 50201050230 ; заявл. 06.12.2010 ; опубл. 08.12.2010. – 1 с.

18. Алгоритм, позволяющий обеспечить требуемый пользователем уровень доступности информации : свидетельство об отраслевой регистрации разработки № 16227 / С. Н. Новиков, О. И. Солонская. – № 50201001615 ; заявл. 29.09.2010 ; опубл. 05.10.2010. – 1 с.

19. Алгоритм и программа проверки сети на связность способом «Свертка» : листок / А. Н. Данилов, С. Н. Новиков; Гос. ФАП СССР. – № 50850000756, 1985.

20. Анализ живучести сетей : извещение о государственной регистрации в Отраслевом фонде алгоритмов и программ / С. Н. Новиков, А. Н. Гольник. – № 50200100095 ; зарегистрировано 02.04.2001. – 1 с.

21. Анализ методов маршрутизации в широкополосных цифровых сетях интегрального обслуживания (Ш-ЦСИО) : извещение о государственной регистрации в Отраслевом фонде алгоритмов и программ / С. Н. Новиков, А. А. Буров. – № 50200401220 ; зарегистрировано 18.10.2004. – 1 с.

22. Интерфейс "Пользователь – ЭВМ" для анализа живучести телекоммуникационных систем : извещение о государственной регистрации **в** Отраслевом фонде алгоритмов и программ / С. Н. Новиков, Е. В. Сафонов. – №50200100421 ; зарегистрировано 24.10.2001. – 1 с.

23. Метод проверки телекоммуникационной системы на связность : свидетельство об отраслевой регистрации разработки № 2377 / С. Н. Новиков, А. А. Буров. – № 50200300153 ; заявл. 20.02.2003 ; опубл. 28.02.2003. – 1 с.

24. Программа оценки структурной надежности сетей связи / С. Н. Новиков, В. С. Гладкий, А. Н. Данилов ; Гос. ФАП СССР. – № 50870001283, 1987.

25. Электронное учебное пособие «Методы маршрутизации на цифровых

широкополосных сетях связи» : свидетельство об отраслевой регистрации разработки № 2413 / С. Н. Новиков. – № 50200300206 ; заявл. 12.03.2003 ; опубл. 26.03.2003. – 1 с.

Публикации, включенные в библиографические базы Web of Science, Scopus

26. Novikov, S. N. A Mathematical model of routing in B-ISDN with ATM technology / S. N. Novikov // 6th International conference on actual problems of electronic instrument engineering proceedings, APEIE – 2002. – Novosibirsk, 2002. – Vol. 1. – P. 173–175; (Accession Number: WOS: 000179482900043).

27. Novikov, S. N. Connections of the Information Security in Telecommunication System with Guarantee Quality of Service / S. N. Novikov, A. A. Kiselev // The IEEE Siberian Conference on Control and Communications, SIBCON-2003. – Tomsk, 2003. – P. 139–145.

28. Novikov, S. N. Formal Interpretation of Network Tasks of Model OSI / A. A. Kiselev, S. N. Novikov // The IEEE International Siberian Conference on Control and Communications (SIBCON-2005), Russia, Tomsk, 2005. – P. 16–22. – Режим доступа : http://www.scopus.com/inward/record.url?eid=2-s2.033847295334&partnerID=40&md5=4b2e7362f9159fe3a03700501601ddff); (Accession Number: WOS: 000236903500003).

29. Novikov, S. N. Information Security in Telecommunication Networks: Criteria and Protection profile / A. A. Kiselev, E. V. Safonov, S. N. Novikov // 5-th International Siberian Workshop on Electron Devices and Materials Proceedings, Erlagol, Altai – July 1-5, 2004. – P. 119–121. – Режим доступа : http:// www.scopus.com/inward /record.url?eid=2-s2.014244256468&partnerID=40&md5=0b8a6a538ff2bd335e14310f 4a2fbcd6 ; (Accession Number: WOS: 000224067100037).

30. Novikov, S. N. Modeling of the Routing Process Occurring in Communication Networks with Guaranteed Quality of Service / S. N. Novikov, A. A. Burov // The IEEE Siberian Conference on Control and Communications, SIBCON-2003. – Tomsk, 2003. – P. 32–35.

31. Novikov, S. N. The Analysis of Probability Time Characteristics of a Telecommunication Network / S. N. Novikov, A. A. Burov // The IEEE International Siberian Conference on Control and Communications (SIBCON-2005), Russia, Tomsk, 2005. – P. 26–29. – Режим доступа : http://www.scopus.com/inward/record.url?eid=2-s2.0-33847322657&partnerID=40&md5=c61188bdd8d11b1cfbc72aec998a1c85; (Accession Number: WOS:000236903500005).

Рецензируемые монографии

32. Маршрутизация и защита информации на сетевом уровне в мультисервисных сетях связи / С. Н. Новиков, А. А. Буров, А. А. Киселев, Е. В. Сафонов, О. И. Солонская ; Сиб. гос. ун-т телекоммуникаций и информатики. – М., 2004. – 221 с. – Деп. в ВИНИТИ 04.11.04, № 1732-В2004.

33. Новиков, С. Н. Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи / С. Н. Новиков, под ред. В. П. Шувалова. – М. : Горячая линия - Телеком, 2015. – 128 с.

Рецензируемые учебные пособия

34. Крук, Б. И. Телекоммуникационные системы и сети. В 3 т. Т.1. Современные технологии : учеб. пособие / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под ред. В. П. Шувалова. – 3-е изд., испр. и доп. – М. : Горячая линия-Телеком, 2003. – 647с. – Авт. гл. 9.5 : С. Н. Новиков.

35. Новиков, С. Н. Методы защиты информации : учеб. пособие / С. Н. Новиков, О. И. Солонская ; Сиб. гос. ун-т телекоммуникаций и информатики. – Новосибирск, 2009. – 120 с.

36. Новиков, С. Н. Методы оценки структурной надежности телекоммуникационных систем : учеб. пособие : метод. комплекс / С. Н. Новиков, Е. В. Сафонов ; Сиб. гос. ун-т телекоммуникаций и информатики. – Новосибирск, 2004. – 44 с.

37. Новиков, С. Н. Методы маршрутизации на цифровых широкополосных сетях связи.: учеб. пособие по специальности 200900-сети связи и системы коммутации / С. Н. Новиков. – Новосибирск : СибГУТИ.

Ч. 1.– 2001. – 83 с.

Ч. 2.– 2004.– 58 с.

Другие работы, в которых опубликованы результаты диссертации

38. Гладкий, В. С. Об одном методе маршрутизации на сети связи с коммутацией пакетов / В. С. Гладкий, С. Н. Новиков ; Моск. электротехн. ин-т связи. – 1984. – 15 с. – Деп. в ЦНТИ «Информсвязь» 28.11.1984, № 535.

39. Новиков, С. Н. Алгоритм оценки профиля защиты информации в телекоммуникационных сетях [Электронный ресурс] / С. Н. Новиков,
А. А. Киселев // Электрон. науч. журнал «Исследовано в России». – 8 с. – Режим доступа: http://zhurnal.ape.relarn.ru/articles/2005/197.pdf.

40. Новиков, С. Н. Алгоритм оценки профиля защиты информации в телекоммуникационных сетях / С. Н. Новиков, А. А. Киселев // Перспективы развития современных средств и систем телекоммуникаций : материалы Междунар. науч. - техн. семинара. – Екатеринбург, 2005. – С. 37–45.

41. Новиков, С. Н. Анализ маршрутизации в B-ISDN с технологией ATM / С.Н. Новиков // Труды Международного Форума по проблемам науки, техники и образования / под ред. В. П. Савиных, В. В. Вишневского. – М. : Академия наук о земле, 2001. – Т. 2. – С. 146–148.

42. Новиков, С. Н. Анализ современного состояния проблемы обеспечения комплексной защиты пользовательской информации в мультисервисных сетях связи / С. Н. Новиков // Надежность функционирования и информационная безопасность телекоммуникационных систем железнодорожного транспорта : межвуз. темат. сб. науч. тр. / Омский гос. ун-т путей сообщения. – Омск, 2013. – С. 18–24.

43. Новиков, С. Н. Задача анализа методов маршрутизации / С. Н. Новиков, А. А. Буров // Инновационная экономика и промышленная политика региона (ЭКОПРОМ-2009) : тр. VII Междунар. науч.-практ. конф., 30 сент. – 3 окт. 2009г.– СПб.: Изд-во Политехн. ун-та, 2009. – Т. 2. – С. 396–401.

44. Новиков, С. Н. Защита информации в телекоммуникационных сетях на

базе АТМ / С. Н. Новиков, Е. В. Сафонов // Актуальные проблемы электронного приборостроения. АПЭП – 2002 : материалы Междунар. конф. – Новосибирск, 2002. – Т. 4. – С. 108–112.

45. Новиков, С. Н. Защита пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи / С. Н. Новиков // Надежность функционирования и информационная безопасность телекоммуникационных систем железнодорожного транспорта : межвуз. темат. сб. науч. тр. / Омский гос. ун-т путей сообщения. – Омск, 2013. – С. 179–189.

46. Новиков, С. Н. Имитационное моделирование мультисервисной сети связи в условиях внешних, деструктивных воздействий / С. Н. Новиков,
Д. А. Тахтараков // Современныеипроблемы телекоммуникаций : материалы Российской науч. - техн. конференции. – Новосибирск, 2015. – С. 602–608.

47. Новиков, С. Н. К вопросу оценки структурной надежности сети связи / С. Н. Новиков, С. Н. Гончаров // Методы управления технической диагностикой и восстановлением работоспособности элементов сетей связи : Респ. науч. - техн. конф. : тез. докл. – Ташкент. – 1988. – С. 46.

48. Новиков, С. Н. Классификация методов маршрутизации на сетях связи / С. Н. Новиков // Современные информационные технологии. СИТ – 2000 : материалы IV Междунар. науч. - техн. конф. – Новосибирск, 2000. – С. 49–50.

49. Новиков, С. Н. Критерий выбора ресурсов для обеспечения доступности информации в сетях связи / С. Н. Новиков, О. И. Солонская // Проблемы информатики. – 2009. – № 4 (спец. вып.). – С. 37–40.

50. Новиков, С. Н. Логически-игровой метод формирования плана распределения информации / С. Н. Новиков // Перспективы развития современных средств и систем телекоммуникаций : материалы Междунар. семинара. – Омск, 2001. – С. 42–45.

51. Новиков, С. Н. Локально-волновой метод маршрутизации /
С. Н. Новиков // Информатика и проблемы телекоммуникаций : материалы Рос. науч. - техн. конф. – Новосибирск, 2000. – С. 35.

52. Новиков, С. Н. Маршрутизация в Ш-ЦСИО / С. Н. Новиков //

Информатика и проблемы телекоммуникаций : материалы Междунар. науч. - техн. конф. – Новосибирск, 2001. – С. 13–15.

53. Новиков, С. Н. Математическая модель маршрутизации на широкополосных цифровых сетях интегрального обслуживания / С. Н. Новиков // Перспективы развития современных средств и систем телекоммуникаций : материалы Междунар. семинара. – Новосибирск, 2000. – С. 64–68.

54. Новиков, С. Н. Обеспечение информационной безопасности на сетевом уровне модели взаимодействия открытых систем в мультисервисных сетях / С. Н. Новиков, О. И. Солонская // Проблемы функционирования информационных сетей : материалы X междунар. конф. – Новосибирск, 2008. – С. 81–86.

55. Новиков, С. Н. Обеспечение конфиденциальности передаваемой информации на сетевом уровне / С. Н. Новиков, О. И. Солонская // Инновационная экономика и промышленная политика региона (ЭКОПРОМ-2009) : тр. междунар. науч.-практ. конф. – СПб. : Изд-во Политехн. ун-та, 2009. – Т. 2. – С. 406–411.

56. Новиков, С. Н. Подход уменьшения дисперсии оценки структурной надежности сложных систем методом Монте-Карло / С. Н. Новиков // Современные проблемы телекоммуникаций : материалы Рос. науч.–техн. конф. – Новосибирск, 2013. – С. 309–310.

57. Новиков, С. Н. Современные технологии защиты информации на сетях связи / С. Н. Новиков // Труды Международного Форума по проблемам науки, техники и образования / под ред. В. П. Савиных, В. В. Вишневского. – М. : Академия наук о земле, 2002. – Т. 2. – С. 162–164.

58. Новиков, С. Н. Способ и устройство проверки графа сети на связность / С. Н. Новиков // Перспективы развития современных средств и систем телекоммуникаций : материалы Междунар. науч. - техн. семинара. – Томск, 2003. – С. 51–54.

59. Новиков, С. Н. Функциональная схема маршрутизатора Ш-ЦСИО /

С. Н. Новиков // Информатика и проблемы телекоммуникаций : материалы Междунар. науч.-техн. конф. – Новосибирск, 2001. – С. 26–29.

60. Новиков, С. Н. Численный метод анализа маршрутизации на сетях связи с КК / С. Н. Новиков // Методы управления технической диагностикой и восстановлением работоспособности элементов сетей связи : Респ. науч. - техн. конф. : тез. докл. – Ташкент, 1988. – С. 121–122.

61. Способ обеспечения конфиденциальности передаваемой информации : заявка № 2012153588 Рос. Федерация / С. Н. Новиков, О. И. Солонская. – Опубл. 20.06.2014, Бюл. № 17.

62. Способ проверки графа на связность: заявка № 200011037/09 Рос. Федерация / С. Н. Новиков. – Заявл. 20.04.2000 ; опубл. 23.07.2002.

63. Novikov, S. N. Routing Methods General Analysis / S.N. Novikov, A.A. Burov // Leipzig Univrsity of Applied Sciences. Science Days. – Germany, Leipzig, 2009. – 8 p.

Отчеты НИР, имеющие государственную регистрацию в ВНТИЦ

64. Исследование и разработка методов маршрутизации и защиты информации на Ш-ЦСИО : отчет о НИР / Сиб. гос. ун-т телекоммуникаций и информатики ; рук. Новиков С. Н. ; исполн.: Буров А. А., Киселев А. А., Новиков С. Н., Сафонов Е. В., Солонская О. И. – Новосибирск, 2005. – № ГР 0120050144911. – Инв. № Б 02200501349.

65. Исследование и разработка методов маршрутизации на широкополосных цифровых сетях интегрального обслуживания (Ш-ЦСИО) : отчет о НИР / Сиб. гос. ун-т телекоммуникаций и информатики ; рук. Новиков С. Н. ; исполн.: Новиков С. Н., Сафонов Е. В., Гольник А. А. – Новосибирск, 2002. – № ГР 01200111639. – Инв. № 02200300138

66. Разработка методики анализа функционирования широкополосной цифровой сети интегрального обслуживания (Ш-ЦСИО) : отчет о НИР / Сиб. гос. ун-т телекоммуникаций и информатики ; рук. Новиков С. Н. – Новосибирск, 2003. – № ГР 01200304433.

Приложение Б Документы, подтверждающие реализацию результатов диссертационной работы
(справочное)

Приложение Б.1 Акты о внедрении и использовании результатов диссертации

Общество с ограниченной ответственностью
«Системы информационной безопасности»
ИНН 5405414231 КПП 540501001 ОКПО 66225083
р/с 40702810553970000394 в ЗАПАДНО-СИБИРСКОМ ФИЛИАЛЕ ПАО "РОСБАНК", Г.НОВОСИБИРСКК/с 30101810050030000779 БИК 045003779
г. Новосибирск, ул. Добролюбова, д. 16, корп. 2, оф. 206, тел.: 8 (383) 201-85-75,info@sib-nsk.net
г. Абакан, ул. Крылова, д. 47а, оф. 607, тел.: 8 (3902) 34-76-90, abakan@sib-nsk.net
г. Иркутск, ул. Лапина, д. 8, оф. 13, тел.: 8 (395) 264-01-63, irkutsk@sib-nsk.net
г. Владивосток, ул. Тигровая, д. 29, оф. 11, тел.: 8 (423) 250-26-42, prim@sib-nsk.net

Утверждаю
Директор ООО «СИБ»
_____ А.А. Помешкин
«15» октября 2015 г.

А К Т

внедрения результатов диссертационной работы

Новикова Сергея Николаевича,

представленной на соискание ученой степени доктора технических наук,

в разработках защищенных телекоммуникационных систем связи

Комиссия в составе:

председатель директор ООО «СИБ» Помешкин А.А.;

члены комиссии: заместитель директора ООО «СИБ», к.т.н. Гончаров С.А.

начальник аттестационно-аналитического отдела ООО «СИБ» Ковтонюк А. С

составили настоящий акт в том, что результаты диссертационной работы Новикова С.Н., представленной на соискание доктора технических наук, внедрены при проектировании защищенной системы видео конференцсвязи в Правительстве Республики Тыва, а именно:

методология обеспечения комплексной защиты пользовательской информации на базе протоколов сетевого уровня мультисервисных сетей связи включающая:

– подход обеспечения конфиденциальности информации использующий многократное асимметричное шифрование ключами меньшей длины, что позволило уменьшить время шифрования и задержки передачи пользовательской информации в l^{c-1} раз, где l – количество асимметричного шифрования, c – постоянная, значения которой определяется криптографическими алгоритмами шифрования;

– критерий, позволяющий выбирать оптимальные сетевые ресурсы (соединения) с точки зрения обеспечения целостности и доступности передаваемой информации в мультисервисных сетях связи при минимальной стоимости;

– способ и алгоритм, его реализующий, обеспечения целостности информации, использующий параллельные (многопутевые) методы маршрутизации и учитывающий вероятностно-стоимостные параметры маршрутов, что позволило уменьшить время задержки передачи пользовательской информации;

– алгоритм обеспечения доступности информации в мультисервисных сетях связи, состоящий в том, что параллельные соединения устанавливаются в соответствии с разработанным критерием выбора сетевых ресурсов (соединений), позволяющий выбирать оптимальные соединения с точки зрения обеспечения доступности передаваемой информации в мультисервисных сетях связи при минимальной стоимости

а так же документы, описывающие применение и техническое описание перечисленных алгоритмов

внедрены в разработке защищенной системы видео конференцсвязи в Правительстве Республики Тыва

Использование перечисленных алгоритмов и программ позволило выбрать оптимальные варианты реализации защищенной системы видео конференцсвязи в Правительстве Республики Тыва

Директор ООО «СИБ» Помешкин А.А.

Заместитель директора ООО «СИБ» к.т.н Гончаров С.А.

Начальник аттестационно-аналитического отдела

ООО «СИБ» Ковтонюк А. С

«15» января 2015 г.

Development and manufacture of telecommunication products

Eltex Enterprise Ltd
630020, Russia, Novosibirsk
Okruzhnaya street 29v
tel.: (383)274-10-01, fax: (383)274-48-48
e-mail: eltex@eltex.nsk.ru

УТВЕРЖДАЮ

Директор ООО «Предприятие «Элтекс»

_____ А.Н. Черников

«10» 08 2015 г.

А К Т

о внедрении результатов диссертационной работы

на соискание ученой степени д.т.н.

Новикова Сергея Николаевича

Научно-техническая комиссия в составе: технического директора Малова В.К., начальника лаборатории Мохова А.Е. и заместителя начальника сервисного центра ШПД Макаренко И.М., подготовила настоящий акт о внедрении основных научных результатов диссертационной работы Новикова С.Н., представленной на соискание ученой степени д.т.н., в процесс проектирования и разработки сетевого коммутационного оборудования (коммутаторов и маршрутизаторов) предприятия ООО «Предприятие «Элтекс», а именно:

1) методика обеспечения целостности пользовательской информации за счет сетевых ресурсов мультисервисной сети связи, основанная на разработках:

– Способ обеспечения целостности передаваемой информации : пат. 2513725 Рос. Федерация / С. Н. Новиков, О. И. Солонская. – Опубл. 20.04.14, Бюл. № 11.;

– Алгоритм обеспечения целостности пользовательской информации в сетях с гарантированным качеством обслуживания на сетевом уровне : свидетельство об отраслевой регистрации разработки № 15062 / С. Н. Новиков, О. И. Солонская. – № 50200901147 ; заявл. 23.11.2009 ; опубл. 02.12.2009. – 1 с.;

2) методика обеспечения доступности пользовательской информации за счет сетевых ресурсов мультисервисной сети связи, основанная на разработке

Development and manufacture of telecommunication products

Eltex Enterprise Ltd
630020, Russia, Novosibirsk
Okruzhnaya street 29v
tel.: (383)274-10-01, fax: (383)274-48-48
e-mail: eltex@eltex.nsk.ru

– Алгоритм, позволяющий обеспечить требуемый пользователем уровень доступности информации : свидетельство об отраслевой регистрации разработки № 16227 / С. Н. Новиков, О. И. Солонская. – № 50201001615 ; заявл. 29.09.2010 ; опубл. 05.10.2010. 1 с.;

3) методика обеспечения конфиденциальности пользовательской информации за счет сетевых ресурсов мультисервисной сети связи

– Алгоритм, позволяющий обеспечить требуемый пользователем уровень конфиденциальности информации в мультисервисных сетях связи : свидетельство об отраслевой регистрации разработки № 16462 / С. Н. Новиков, О. И. Солонская. – № 50201050230 ; заявл. 06.12.2010 ; опубл. 08.12.2010. – 1 с.;

4) методика комплексной защиты пользовательской информации за счет сетевых ресурсов мультисервисных сетей связи.

Реализация разработанных автором диссертации вышеуказанных методик позволила:

– сократить время на проведение НИР и ОКР по защите пользовательской информации в сетях специального назначения;

– расширить возможности ООО «Предприятие «Элтекс» по производству сетевого оборудования (маршрутизаторов, коммутаторов) для сетей специального назначения;

– участвовать в конкурсных проектах разработки сетевого оборудования (маршрутизаторов, коммутаторов) для сетей специального назначения.

Данные методики позволяют обеспечить комплексную защиту пользовательской информации в мультисервисных сетях связи специального назначения без снижения QoS высокоскоростных приложений, функционирующих в реальном масштабе времени (критичных к задержкам).

Технический директор ООО «Предприятие «Элтекс» Малов В.К.

Начальник лаборатории ООО «Предприятие «Элтекс» Мохов А.Е.

Заместитель начальника сервисного центра ЦППД
ООО «Предприятие «Элтекс» Макаренко И.М.

«УТВЕРЖДАЮ»
Управляющий делами Губернатора
Иркутской области
и Правительства Иркутской области

_____ А.Г. Суханов
«21» 08 2012 год

А К Т

об использовании результатов диссертационной работы

Новикова Сергея Николаевича

на соискание ученой степени д.н.т.

в разработке защищенных телекоммуникационных систем связи

КСПД (корпоративной сети передачи данных) управления делами

Губернатора Иркутской области и Правительства Иркутской области.

Мы, нижеподписавшиеся:
начальник управления информационного и документационного обеспечения Губернатора Иркутской области и Правительства Иркутской области Виноградов С.А.,
начальник отдела инженерного обеспечения систем связи, охраны и контроля доступа управления делами Губернатора Иркутской области и Правительства Иркутской области Косарев Э.Ю.,
ведущий инженер отдела инженерного обеспечения систем связи, охраны и контроля доступа управления делами Губернатора Иркутской области и Правительства Иркутской области Модный Ю.Ю.

Составили настоящий акт о том, что результаты диссертационной работы Новикова С.Н. использованы при обеспечении безопасности каналов связи ОГВ (органов государственной власти) имеющих доступ к КСПД, а именно:

- программный продукт – программа для ЭВМ «Интерфейс «Пользователь ЭВМ» для анализа живучести телекоммуникационных систем»;
- программный продукт – «Анализ методов маршрутизации в широкополосных цифровых сетях интегрального обслуживания (Ш-ЦСИО)»;
- алгоритм обеспечения целостности пользовательской информации в сетях с гарантированным качеством обслуживания на сетевом уровне;
- алгоритм, позволяющий обеспечить требуемый пользователем уровень доступности информации;
- алгоритм, позволяющий обеспечить требуемый пользователем уровень конфиденциальности информации в мультисервисных сетях связи, а также документы, описывающие применение и техническое описание перечисленных алгоритмов и программ.

Использованы в разработке защищенных телекоммуникационных систем связи КСПД (корпоративной сети передачи данных) управления делами Губернатора Иркутской области и Правительства Иркутской области.

Использование перечисленных алгоритмов и программ позволяет выбрать оптимальные варианты реализации защищенных телекоммуникационных систем связи в органах государственной власти Правительства Иркутской области.

ПОДПИСИ:

1. Начальник управления информационного и документационного обеспечения Губернатора Иркутской области и Правительства Иркутской области

   _____С.А. Виноградов
2. Начальник отдела инженерного обеспечения систем связи, охраны и контроля доступа управления делами Губернатора Иркутской области и Правительства Иркутской области

   _____Э.Ю. Косарев
3. Ведущий инженер отдела инженерного обеспечения систем связи, охраны и контроля доступа управления делами Губернатора Иркутской области и Правительства Иркутской области

   _____Ю.Ю. Модный

ООО «ЦИБ-Сервис»

656052, Алтайский край, г. Барнаул, ул. Северо-Западная, 159, оф. 05
ИНН 2225113092 КПП 222101001 ОГРН 1102225011020
Расчетный счет 40702810304000007374 в банке АКБ «Зернобанк» (ЗАО)
Корреспондентский счет 30101810600000000754 БИК 040173754
Тел. +7(3852) 200-460, 200-464 Факс. +7(3852) 200-460

УТВЕРЖДАЮ

Директор

_____ **С.Г.Семенов**

«08» 07 2012 г.

А К Т

внедрения результатов диссертационной работы
Новикова Сергея Николаевича
на соискание ученой степени д.т.н.
при разработке защищенных телекоммуникационных систем связи

Комиссия, назначенная приказом № 12-п от 08.07.2012, в составе директора Семенова С.Г. и руководителя отдела по защите информации Соболя Д.Б. составила настоящий акт в том, что результаты диссертационной работы Новикова С.Н.:

- пакет прикладных программ функционирования сети в экстремальных условиях (ППППФСЭУ), включающий - «Интерфейс «Пользователь – ЭВМ» для анализа живучести телекоммуникационных систем»; «Анализ методов маршрутизации в широкополосных цифровых сетях интегрального обслуживания»;
- документы, описывающие применение, содержание и техническое описание ППППФСЭУ

внедрены при разработке защищенных телекоммуникационных систем связи

Использование перечисленных алгоритмов и программ позволило выбрать оптимальные варианты реализации защищенных телекоммуникационных систем связи. Так же данные разработки использовались при проектировании защищённой сети учреждений среднего образования и дошкольного обучения г. Барнаула.

Директор _____ С.Г.Семенов

Руководитель отдела по защите информации _____ Д.Б.Соболь

«08» 07 2012 г.

«Утверждаю»
И.о. ректора ФГОБУ ВПО «СибГУТИ»
_____В.Г. Беленький
«07» июля 2015 г.

АКТ

внедрения результатов диссертационной работы
Новикова Сергея Николаевича,
представленной на соискание ученой степени доктора технических наук
в учебный процесс ФГОБУ ВПО «СибГУТИ»

Мы, нижеподписавшиеся: и.о. проректора по учебной работе ФГОБУ ВПО «СибГУТИ», д.т.н., доцент Мамойленко С.Н.; декан факультета АЭС ФГОБУ ВПО «СибГУТИ», д.т.н., профессор Мелентьев О.Г.; к.т.н., доцент кафедры «Безопасность и управление в телекоммуникациях» ФГОБУ ВПО «СибГУТИ» Солонская О.И. составили настоящий акт в том, что результаты научно-исследовательской квалификационной работы Новикова С.Н., представленной на соискание ученой степени доктора технических наук, внедрены в учебный процесс ФГОБУ ВПО «СибГУТИ», а именно:

1) обобщенная, функциональная модель маршрутизации в мультисервисных сетях связи (МСС); классификация методов маршрутизации для сетей связи; методы маршрутизации; математическая и имитационная модели анализа функционирования МСС с учетом методов маршрутизации; теория и принципы оценки живучести и структурной надежности сетей связи,

разработанные в диссертации, используются при проведении всех видов занятий для студентов специальности «Информационная безопасность телекоммуникационных систем» к.т.н., доцентом О.И. Солонской по курсу «Телекоммуникационные технологии с гарантированным качеством обслуживания» и старшим преподавателем В.О. Жариковой по курсу «Моделирование систем» и включены в учебные пособия:

– Новиков, С. Н. Методы маршрутизации на цифровых широкополосных сетях связи. Ч. 1 : учеб. пособие / С. Н. Новиков ; Сиб. гос. ун-т телекоммуникаций и информатики. – Новосибирск, 2000. – 84 с. (Рекомендовано УМО);

– Крук, Б. И. Телекоммуникационные системы и сети. В 3 т. Т.1. Современные технологии : учеб. пособие / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под ред. В. П. Шувалова. – 3-е изд., испр. и доп. – М. : Горячая линия-Телеком, 2003. – 647с. – Авт. гл. 9.5 : С. Н. Новиков. (Рекомендовано УМО);

– Новиков, С. Н. Методы оценки структурной надежности телекоммуникационных систем : учеб. пособие : метод. комплекс / С. Н. Новиков, Е. В. Сафонов ; Сиб. гос. ун-т телекоммуникаций и информатики. – Новосибирск, 2004. – 44 с. (Рекомендовано УМО),

а так же использованы при подготовке учебно-методических комплексов проекта Европейской Комиссии TEMPUS JEP_26032_2005, в рамках которых выпущены учебные пособия для студентов магистратуры направления «Телекоммуникации»:

1

– Новиков С.Н. Телекоммуникационные технологии. Ч. 1: Учебное пособие / ГОУ ВПО «СибГУТИ». – Новосибирск, 2009 г. – 84 с.;

– Новиков С.Н. Телекоммуникационные технологии. Ч. 2: Учебное пособие / ГОУ ВПО «СибГУТИ». – Новосибирск, 2009 г. – 60 с.;

– Новиков С.Н. Методы защиты информации: Учебное пособие/С.Н.Новиков, О.И. Солонская / ГОУ ВПО «СибГУТИ». – Новосибирск, 2009 г. – 120 с.;

2) методики и критерии, позволяющие выбирать оптимальные соединения с точки зрения обеспечения целостности и доступности передаваемой информации в МСС при минимальной стоимости; методики и алгоритмы обеспечения: целостности пользовательской информации в сетях с гарантированным качеством обслуживания на сетевом уровне; требуемых пользователем уровней доступности и конфиденциальности информации в МСС,

разработанные в диссертации, используются при проведении всех видов занятий для студентов специальности «Информационная безопасность телекоммуникационных систем» к.т.н., доцентом О.И. Солонской для студентов по курсу «Защита и мониторинг мультисервисных сетей связи»;

3) теория и принципы защиты пользовательской информации с использованием ресурсов МСС,

а так же программные продукты: «Интерфейс «Пользователь – ЭВМ» для анализа живучести телекоммуникационных систем»; «Анализ методов маршрутизации в широкополосных цифровых сетях интегрального обслуживания (Ш-ЦСИО)»,

разработанные в диссертации, используются автором диссертации (Новиковым С.Н.) при проведении всех видов занятий для студентов специальности «Информационная безопасность телекоммуникационных систем» по курсам «Основы проектирования защищенных телекоммуникационных систем», «Основы технической эксплуатации защищенных телекоммуникационных систем», «Живучесть телекоммуникационных систем», а так же в авторском курсе «Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи» для аспирантов ФГОБУ ВПО «СибГУТИ» направления10.06.01 «Информационная безопасность» научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» и опубликованы в монографии автора диссертации

(Новиков, С. Н. Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи / С. Н. Новиков, под ред. В. П. Шувалова. – М. : Горячая линия - Телеком, 2015. – 128 с.).

И.о. проректора по учебной работе
ФГОБУ ВПО «СибГУТИ», д.т.н., доцент Мамойленко С.Н.

Декан факультета АЭС ФГОБУ ВПО «СибГУТИ»,
Д.т.н., профессор Мелентьев О.Г.

К.т.н., доцент Солонская О.И.

«07» июля 2015 г.

ПАО «ГАЗПРОМ»

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ГАЗПРОМ ТРАНСГАЗ ТОМСК»

(ООО «Газпром трансгаз Томск»)

А К Т

использования результатов диссертационной работы
Новикова Сергея Николаевича, представленной
на соискание ученой степени доктора технических наук

Комиссия, в составе: заместителя начальника службы связи Шабаловского А.А., начальника лаборатории связи Куликова Л.О. и начальника отдела развития Глотова В.М. составила настоящий акт в том, что следующие результаты диссертационной работы Новикова С.Н., представленной на соискание ученой степени доктора технических наук, использованы при проектировании систем управления сетями связи ООО «Газпром трансгаз Томск»:

1) программная реализация разработанной математической модели маршрутизации в условиях внешних деструктивных воздействий на элементы сети связи с гарантированным качеством обслуживания;

2) инструкция пользователя программной реализации математической модели маршрутизации в условиях внешних деструктивных воздействий на элементы сети связи с гарантированным качеством обслуживания, основанные на разработках:

– Анализ методов маршрутизации в широкополосных цифровых сетях интегрального обслуживания (Ш-ЦСИО): извещение о государственной регистрации в Отраслевом фонде алгоритмов и программ / С. Н. Новиков, А. А. Буров. – № 50200401220; зарегистрировано 18.10.2004. – 1 с.;

– Метод проверки телекоммуникационной системы на связность: свидетельство об отраслевой регистрации разработки № 2377 / С. Н. Новиков, А. А. Буров. – № 50200300153; заявл. 20.02.2003; опубл. 28.02.2003. – 1 с.

– Анализ живучести сетей: извещение о государственной регистрации в Отраслевом фонде алгоритмов и программ / С. Н. Новиков, А. Н. Гольник. – № 50200100095; зарегистрировано 02.04.2001. – 1 с.;

– Интерфейс "Пользователь - ЭВМ" для анализа живучести телекоммуникационных систем : извещение о государственной регистрации в Отраслевом фонде алгоритмов и программ / С. Н. Новиков, Е. В. Сафонов. – №50200100421; зарегистрировано 24.10.2001. – 1 с.

Реализация разработанных и внедренных автором диссертации вышеуказанных продуктов позволила в период с 2003г. по 2005г: выбрать оптимальные варианты построения сетей связи; оценивать степень живучести сетей связи с гарантированным обслуживанием при сокращении сроков проектирования систем управления сетью связи.

Начальник службы связи
ООО «Газпром трансгаз Томск» **А.А. Кривенцов**

Заместитель начальника службы связи
ООО «Газпром трансгаз Томск» **А.А. Шабаловский**

Начальник отдела развития
службы связи ООО «Газпром трансгаз Томск» **В.М. Глотов**

Начальник лаборатории связи
службы связи ООО «Газпром трансгаз Томск» **Л.О. Куликов**

«15» 12 2015 г.

Приложение Б.2 Свидетельства о регистрации электронных ресурсов

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Государственный координационный центр информационных технологий

117933, Москва, В-49
Ленинский пр., 6
Телефон: 123-90-23

13.04.2001 № 38

На №

Сибирский государственный университет телекоммуникаций и информатики
Проректору по научной работе, профессору
Ю.Д.Козляеву

Сообщаю Вам, что представленное Вами в Отраслевой фонд алгоритмов и программ (ОФАП) программное средство зарегистрировано в Информационно-библиотечном фонде Российской Федерации с ***присвоением следующего номера государственной регистрации:***

"Анализ живучести сетей связи", авторы Новиков С.Н., Гольник А.Н.
Регистрационный номер – **50200100095.**

В соответствии с пунктом 17 Положения о порядке присуждения научным и научно-педагогическим работникам ученых степеней и присвоения научным работникам ученых званий, утвержденного постановлением Правительства Российской Федерации от 24 октября 1994 года № 1185, алгоритмы и программы, включенные в Информационно-библиотечный фонд Российской Федерации, приравниваются к опубликованным работам, отражающим научные результаты диссертации.

Приложение: 1.Сопроводительное письмо – на 1л. в 1 экз.,
2. Информационная карта алгоритмов и программ-на 1л. в 1 экз.

Директор Е.Г.Калинкевич

113
03 05.01

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Государственный координационный центр информационных технологий

117933, Москва, В-49
Ленинский пр., 6
Телефон: 123-90-23

20.11.01г. № 112

На №_____

СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ
РЕКТОРУ Бакалову В.П.

Сообщаю Вам, что представленное Вами в Отраслевой фонд алгоритмов и программ (ОФАП) программное средство зарегистрировано в Информационно-библиотечном фонде Российской Федерации с ***присвоением следующего номера государственной регистрации:***

1 Интерфейс "Пользователь –ЭВМ" для анализа живучести телекоммуникационных систем, авторы Новиков С.Н., Сафонов Е.В.
Регистрационный номер – **50200100421.**

В соответствии с пунктом 17 Положения о порядке присуждения научным и научно-педагогическим работникам ученых степеней и присвоения научным работникам ученых званий, утвержденного постановлением Правительства Российской Федерации от 24 октября 1994 года № 1185, алгоритмы и программы, включенные в Информационно-библиотечный фонд Российской Федерации, приравниваются к опубликованным работам, отражающим научные результаты диссертации.

Приложение: 1.Сопроводительное письмо – на 1л. в 1 экз.,
2. Информационная карта алгоритмов и программ - на 1 л. в 1 экз.

Директор Е.Г.Калинкевич

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСУДАРСТВЕННЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ОТРАСЛЕВОЙ ФОНД АЛГОРИТМОВ И ПРОГРАММ

СВИДЕТЕЛЬСТВО ОБ ОТРАСЛЕВОЙ РЕГИСТРАЦИИ РАЗРАБОТКИ

№ 2377

Настоящее свидетельство выдано на разработку:

«Метод проверки телекоммуникационной системы на связность»

зарегистрированную в Отраслевом фонде алгоритмов и программ.

Дата регистрации: **20 февраля 2003 года**

Авторы**: Новиков С.Н., Буров А.А.**

Организация-разработчик: **Сибирский государственный университет телекоммуникаций и информатики**

Директор Госкоорцентра _____ **Е.Г. Калинкевич**

Руководитель ОФАП _____ **А.И. Галкина**

Дата выдачи 27.03.2003.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСУДАРСТВЕННЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ОТРАСЛЕВОЙ ФОНД АЛГОРИТМОВ И ПРОГРАММ

СВИДЕТЕЛЬСТВО ОБ ОТРАСЛЕВОЙ РЕГИСТРАЦИИ РАЗРАБОТКИ

№ 2413

Настоящее свидетельство выдано на разработку:

Электронное учебное пособие «Методы маршрутизации на цифровых широкополосных сетях связи»

зарегистрированную в Отраслевом фонде алгоритмов и программ.

Дата регистрации: **12 марта 2003 года**

Автор: **Новиков С.Н.**

Организация-разработчик: **Сибирский государственный университет телекоммуникаций и информатики**

Директор _____ **Е.Г. Калинкевич**

Руководитель ОФАП _____ **А.И. Галкина**

Дата выдачи _____

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ
И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Государственный координационный
центр информационных технологий**

117933, Москва, В-49
Ленинский пр., 6
Телефон: 129-43-00, доб. 2-00

15.11.2004 № 988

На №_____

Сибирский государственный
университет телекоммуникаций и
информатики

630102, г. Новосибирск, ул. Кирова,
д. 86

ИЗВЕЩЕНИЕ

О ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ В «НАЦИОНАЛЬНОМ ИНФОРМАЦИОННОМ ФОНДЕ НЕОПУБЛИКОВАННЫХ ДОКУМЕНТОВ» РАЗРАБОТКИ, ПРЕДЪЯВЛЕННОЙ В ОТРАСЛЕВОЙ ФОНД АЛГОРИТМОВ И ПРОГРАММ:

Анализ методов маршрутизации в широкополосных цифровых сетях интегрального обслуживания (Ш-ЦСИО)

Авторы: **Новиков С.Н., Буров А.А.**

Организация-разработчик: **Сибирский государственный университет телекоммуникаций и информатики**

Номер государственной регистрации: **50200401220**

Дата регистрации: **18 октября 2004 года**

В соответствии с «Положением о порядке присуждения ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 30 января 2002 г. № 74, «... К опубликованным работам, отражающим основные результаты диссертации, приравниваются ***... программы для электронных вычислительных машин; базы данных; ... информационные карты на новые материалы, включенные в государственный банк данных ...****».*

Директор Е.Г. Калинкевич

ГОСУДАРСТВЕННАЯ АКАДЕМИЯ НАУК
РОССИЙСКАЯ АКАДЕМИЯ ОБРАЗОВАНИЯ
ИНСТИТУТ НАУЧНОЙ ИНФОРМАЦИИ И МОНИТОРИНГА
ОБЪЕДИНЕННЫЙ ФОНД ЭЛЕКТРОННЫХ РЕСУРСОВ "НАУКА И ОБРАЗОВАНИЕ"

СВИДЕТЕЛЬСТВО О РЕГИСТРАЦИИ ЭЛЕКТРОННОГО РЕСУРСА

№ 15062

Настоящее свидетельство выдано на электронный ресурс, отвечающий требованиям новизны и приоритетности:

Алгоритм обеспечения целостности пользовательской информации в сетях с гарантированным качеством обслуживания на сетевом уровне

Дата регистрация: **23 ноября 2009 года**

Авторы: **Новиков С.Н., Солонская О.И.**

Директор ИНИМ РАО,
чл.-корр. РАО, д.ю.н., проф. _____ В.Е. Усанов

Руководитель ОФЭРНиО, почетный
работник науки и техники РФ _____ А.И. Галкина

Дата выдачи 08.12.2009

ГОСУДАРСТВЕННАЯ АКАДЕМИЯ НАУК
РОССИЙСКАЯ АКАДЕМИЯ ОБРАЗОВАНИЯ
ИНСТИТУТ НАУЧНОЙ ИНФОРМАЦИИ И МОНИТОРИНГА
ОБЪЕДИНЕННЫЙ ФОНД ЭЛЕКТРОННЫХ РЕСУРСОВ "НАУКА И ОБРАЗОВАНИЕ"

СВИДЕТЕЛЬСТВО О РЕГИСТРАЦИИ ЭЛЕКТРОННОГО РЕСУРСА

№ 16227

Настоящее свидетельство выдано на электронный ресурс, отвечающий требованиям новизны и приоритетности:

Алгоритм, позволяющий обеспечить требуемый пользователем уровень доступности информации

Дата регистрации: **29 сентября 2010 года**

Авторы: **Новиков С.Н., Солонская О.И.**

Директор ИНИМ РАО,
чл.-корр. РАО, д.ю.н., проф. _____ В.Е. Усанов

Руководитель ОФЭРНиО, почетный
работник науки и техники РФ _____ А.И. Галкина

Дата выдачи 07.10.2010

ГОСУДАРСТВЕННАЯ АКАДЕМИЯ НАУК
РОССИЙСКАЯ АКАДЕМИЯ ОБРАЗОВАНИЯ
ИНСТИТУТ НАУЧНОЙ ИНФОРМАЦИИ И МОНИТОРИНГА
ОБЪЕДИНЕННЫЙ ФОНД ЭЛЕКТРОННЫХ РЕСУРСОВ "НАУКА И ОБРАЗОВАНИЕ"

СВИДЕТЕЛЬСТВО О РЕГИСТРАЦИИ ЭЛЕКТРОННОГО РЕСУРСА

№ 16462

Настоящее свидетельство выдано на электронный ресурс, отвечающий требованиям новизны и приоритетности:

Алгоритм, позволяющий обеспечить требуемый пользователем уровень конфиденциальности информации в мультисервисных сетях связи

Дата регистрации: **06 декабря 2010 года**

Авторы: **Солонская О.И., Новиков С.Н.**

Директор ИНИМ РАО,
чл.-корр. РАО, д.ю.н., проф. _____ В.Е. Усанов

Руководитель ОФЭРНиО, почетный
работник науки и техники РФ _____ А.И. Галкина

Дата выдачи 07.12.2010

Приложение Б.3 Патент авторского свидетельства

РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) 2 513 725 (13) **C2**

(51) МПК
G06F 11/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: 2012122695/08, 01.06.2012

(24) Дата начала отсчета срока действия патента:
01.06.2012

Приоритет(ы):
(22) Дата подачи заявки: 01.06.2012

(43) Дата публикации заявки: 10.12.2013 Бюл. № 34

(45) Опубликовано: 20.04.2014 Бюл. № 11

(56) Список документов, цитированных в отчете о поиске: RU 2444846 C1, 10.03.2012. RU 2414062 C2, 10.03.2011. RU 2393633 C1, 27.06.2010. US 2012/0134325 A1, 31.05.2012. US 2012/0051468 A1, 01.03.2012

Адрес для переписки:
630102, г.Новосибирск, ул. Кирова, 86, ФГОБУ ВПО "СибГУТИ", проректору по научной работе А.Н. Фионову

(72) Автор(ы):
Новиков Сергей Николаевич (RU),
Солонская Оксана Игоревна (RU)

(73) Патентообладатель(и):
Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Сибирский государственный университет телекоммуникаций и информатики" (ФГОБУ ВПО "СибГУТИ") (RU)

RU 2513725 C2

(54) СПОСОБ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ

(57) Реферат:

Изобретение относится к области исправления ошибок на приемной стороне в системах связи. Техническим результатом является повышение эффективности приема передаваемой информации при учете вероятности модификации передаваемой информации. Способ обеспечения целостности передаваемой информации состоит в том, что на приемной стороне принимают информацию по n параллельным каналам, вычисляют значение $\ln\frac{P(S_1)}{P(S_2)}+\sum_{i=0}^{n}x_i\cdot\ln\frac{\left(1-P_M^{(i)}\right)}{P_M^{(i)}}$, где $P(S_1)$ и $P(S_2)$ - априорные вероятности передаваемых символов (S_1=1; S_2=-1) - информации от источника; x_1, ..., x_i, ..., x_n значения принятых символов по каждому из n каналов; $P_M^{(i)}$ вероятность несанкционированного воздействия третьим лицом на передаваемые символы от источника в каждом i-м из n каналов; сравнивают вычисленное значение с нулем; если вычисленное значение больше нуля, то принимают решение, что передавался символ S_1, иначе передавался символ S_2. 9 ил., 1 табл.

RU 2513725 C2

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2513725

СПОСОБ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ

Патентообладатель(ли): ***Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Сибирский государственный университет телекоммуникаций и информатики" (ФГОБУ ВПО "СибГУТИ") (RU)***

Автор(ы): ***см. на обороте***

Заявка № **2012122695**

Приоритет изобретения **01 июня 2012 г.**

Зарегистрировано в Государственном реестре изобретений Российской Федерации ***20 февраля 2014 г.***

Срок действия патента истекает **01 июня 2032 г.**

Руководитель Федеральной службы по интеллектуальной собственности

Б.П. Симонов