На правах рукописи

Новиков Сергей Николаевич

МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ТЕХНОЛОГИЙ СЕТЕВОГО УРОВНЯ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ

05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени доктора технических наук

Новосибирск – 2016

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ, г. Новосибирск)

Научный консультант – доктор технических наук, профессор
Шувалов Вячеслав Петрович

Официальные оппоненты:

Белим Сергей Викторович, доктор физико-математических наук, профессор, зав. кафедрой информационной безопасности Омского государственного университета им. Ф.М. Достоевского

Захаров Александр Анатольевич, доктор технических наук, профессор, зав. кафедрой информационной безопасности Тюменского государственного университета

Сущенко Сергей Петрович, доктор технических наук, профессор, заведующий кафедрой прикладной информатики Национального исследовательского Томского государственного университета

Ведущая организация – Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный технический университет»

Защита состоится «_10_»____11_____2016 г. в «15:15» часов на заседании диссертационного совета Д 212.268.03 при Томском государственном университете систем управления и радиоэлектроники (ТУСУР) по адресу: 634050, г. Томск, пр. Ленина, 40, ауд 201.

С диссертацией можно ознакомиться в научной библиотеке ТУСУРа по адресу: г. Томск, ул. Красноармейская, 146, а также на официальном сайте ТУСУРа по адресу: https://tusur.ru/ru/nauka-i-innovatsii/podgotovka-kadrov-vysshey-nauchnoy-kvalifikatsii/ob-yavleniya-o-zaschitah-dissertatsiy/dissertatsiya-metodologiya-zaschity-informatsii-na-osnove-tehnologiy-setevogo-urovnya-multiservisnyh-setey-svyazi

Автореферат разослан «___»_____2016 г.

Ученый секретарь
диссертационного совета Д 212.268.03 Зыков Дмитрий Дмитриевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования и степень ее разработанности.

Отличительная особенность мультисервисных сетей связи (МСС) состоит в предоставлении пользователям в реальном масштабе времени неограниченного спектра приложений с гарантированным качеством обслуживания (Quality of Service, QoS) и защиты информации, реализация которой 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 Lou W., Fang Y. “A multipath routing approach for secure data delivery”, IEEE Military Communications Conference (MILCOM 2001), Mclean, VA, USA, Oct 2001, ведутся активные исследования возможности обеспечения конфиденциальности информации в мобильных сетях за счет механизмов сетевого уровня модели взаимосвязи открытых систем (МВОС) (работы Y. Zhang, И.А. Жукова, Ю.А. Кулакова, О.П. Мартыновой и других ученых). Данный подход имеет ряд преимуществ. Во-первых, чем масштабней сеть связи, тем больше ее ресурсов можно задействовать для обеспечения конфиденциальности 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 показатели параметров информационной безопасности. Система управления, проведя мониторинг свободных ресурсов МСС, реализует не только соединение, поддерживающее QoS для выбранного приложения, но и заявленный пользователем профиль защиты информации.

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 [16, 15, 18], математические модели и их программные реализации [20, 19, 22, 25], документы, поясняющие применение и техническое описание перечисленных алгоритмов и

программ
приняты: в гос. фонд алгоритмов и программ СССР [19, 24]; 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; 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.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение включает в себя: актуальность темы исследования, степень ее разработанности; цель и решаемые задачи; научную новизну; теоретическую и практическую значимость полученных результатов; методологию и методы исследования; положения, выносимые на защиту; степень достоверности и апробацию результатов.

Первая глава посвящена анализу современного состояния обеспечения конфиденциальности, целостности и доступности информации в МСС: приводятся основные термины и определения предметной области «Защита информации»; проводится анализ основных подходов по обеспечению конфиденциальности, целостности и доступности информации в МСС.

Анализ основных подходов по обеспечению базовых параметров защиты информации в МСС выявил следующие проблемы.

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

2. Применение стандартных подходов к защите информации в МСС ограничено. Это связано с увеличением времени задержки передачи информации, что является критичным для ряда 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 и алгоритмов, позволяющих решать задачи обеспечения базовых параметров защиты информации с поддержкой QoS приложений МСС.

Вторая глава диссертации посвящена исследованию и разработке методов защиты информации с использованием ресурсов МСС.

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 с симметричными алгоритмами шифрования криптостойкости требуется более длинный ключ. Во-вторых – зависимость времени шифрования $t_{\text{ш}}$ от длины ключа L_k имеет нелинейный характер и в общем случае определяется выражением $t_{\text{ш}} = A \cdot L_k^c + B$, где: A, B и c – постоянные, значения, которых определяются криптографическими алгоритмами.

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, что скажется на снижении QoS высокоскоростных приложений, функционирующих в реальном масштабе времени. С целью обеспечения конфиденциальности информации и поддержания QoS высокоскоростных приложений, исследуется возможность использования многократного вложения ассиметричных криптографических алгоритмов шифрования [3, 8, 9, 11, 17]:

$$y = E_{k_l^{(\text{о})}}\left\{..E_{k_i^{(\text{о})}}...[E_{k_1^{(\text{о})}}(M)]\right\}; M = D_{k_1^{(\text{с})}}\left\{..D_{k_i^{(\text{с})}}...[D_{k_l^{(\text{с})}}(y)]\right\}. \quad (1)$$

Здесь: $y = E_{k_i^{(\text{о})}}(M)$, $M = D_{k_i^{(\text{о})}}(y)$ – соответственно функции зашифрования M и расшифрования с использованием независимых ключей $k_i^{(\text{о})}$ и $k_i^{(\text{с})}; i = \overline{1,l}$; l – количество асимметричных шифрований.

Допустим, что длины всех открытых и секретных ключей одинаковы и равны между собой, т.е. $L_{k_i^{(\text{о})}} = L_{k_i^{(\text{с})}} = L_k; i = \overline{1,l}$. В данном случае время шифрования с учетом (1) (рисунок 1) определяется:

$$t_{\text{ш сос}} = l \cdot \left(A \cdot \frac{L_{k\,\text{сост}}}{l} \right)^c + B = \frac{A^c \cdot L_{k\,\text{сост}}^c}{l^{c-1}} + B, \quad (2)$$

при общей длине составного ключа:

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

Учитывая (1) и $f_0(L_{k\,\text{сост}})$ (рисунок 1), получим временной выигрыш от применения «составного» ключа по отношению к шифрованию одним «длинным» (при B=0):

$$\frac{t_{\text{ш}}}{t_{\text{ш сост}}} = \frac{A \cdot L_{k\,\text{сост}}^{c}}{l \cdot A \cdot \left(\frac{L_{k\,\text{сост}}}{l}\right)^{c}} = l^{c-1}. \qquad (3)$$

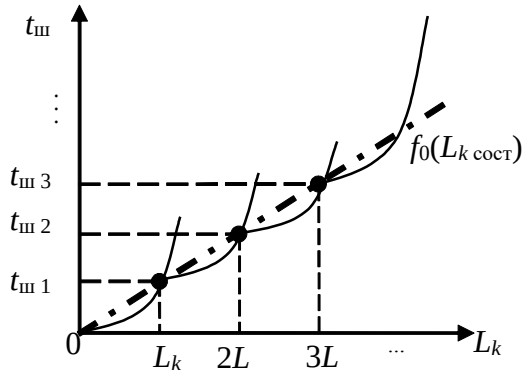


Рисунок 1 – Зависимости времени зашифрования от длины составного ключа

Результаты натурного эксперимента зашифрования алгоритмом *RSA* блока данных объемом 1 Кбайт при изменении длины ключа от 256 бит до 2048 бит и использовании составного 256-битного ключа подтвердили правильность теоретических предположений (1), (3) и представлены на рисунке 2.

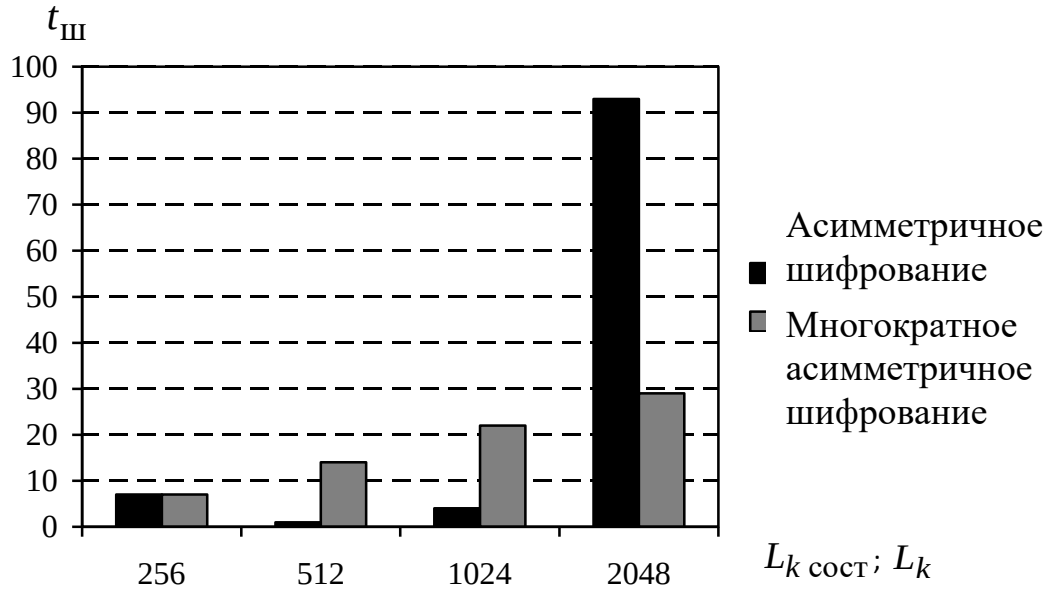


Рисунок 2 – Сравнение времени при асимметричном шифровании и при многократном асимметричном шифровании

Обеспечение целостности информации в МСС предлагается обеспечить за счет организации n параллельных соединений между узлом-источником (УИ), узлом-получателем (УП) и сводится к процессу принятия решения в УП по n одновременно принятым сообщениям $x = (x_1,...,x_i,...,x_n)$ [8, 10, 11, 15, 16]:

$$a_0 + \sum_{i=1}^{n} x_i \cdot a_i \begin{cases} \text{если} > 0, & \text{то принято } M_1; \\ \text{если} < 0, & \text{то принято } M_2, \end{cases} \qquad (4)$$

здесь

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

$P(M_1)$ и $P(M_2)$, соответственно, априорные вероятности появления сообщений M_1 либо M_2 в установленных параллельных соединениях между УИ и УП;

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

Функциональная схема решающего устройства (РУ) [8, 10, 15, 16] приведена на рисунке 3.

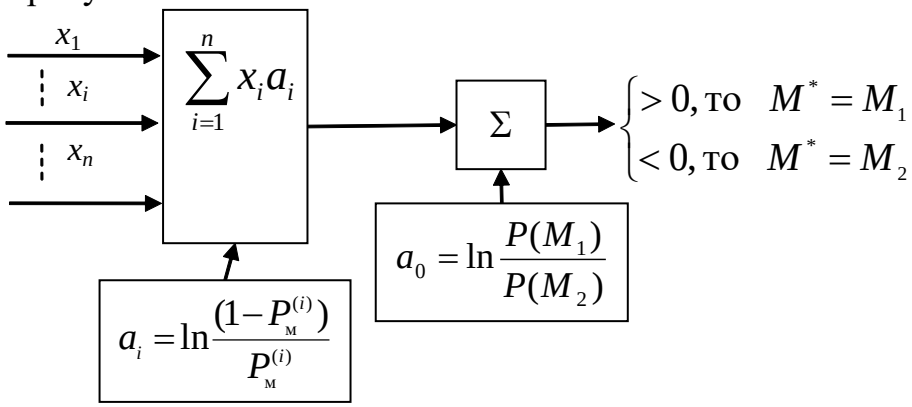


Рисунок 3 – Функциональная схема РУ

Вероятность целостности информации определяется:

$$P_{\text{ц РУ}} = 1 - \sum_{i=0}^{(n-1)/2} C_n^{(n+1+2\cdot i)/2} \cdot (1-P_{\text{м}})^{(n-1-2\cdot i)/2} \cdot P_{\text{м}}^{(n+1+2\cdot i)/2}, \qquad (5)$$

где $C_n^{(n+1+2\cdot i)/2}$ – число сочетаний $(n+1+2\cdot i)/2$ из n при условии, что $n \geq 3$ и нечетно; $P_{\text{м}} = P_{\text{м}}^{(i)}; i=\overline{1,n}$ и атаки нарушителей независимые.

На рисунке 4 приведены результаты оценки целостности информации, рассчитанные по формуле (5). Статистическое моделирование работы РУ (абсолютная погрешность $\Delta_a \leq 0{,}01$) подтверждает правильность теоретических расчетов (5).

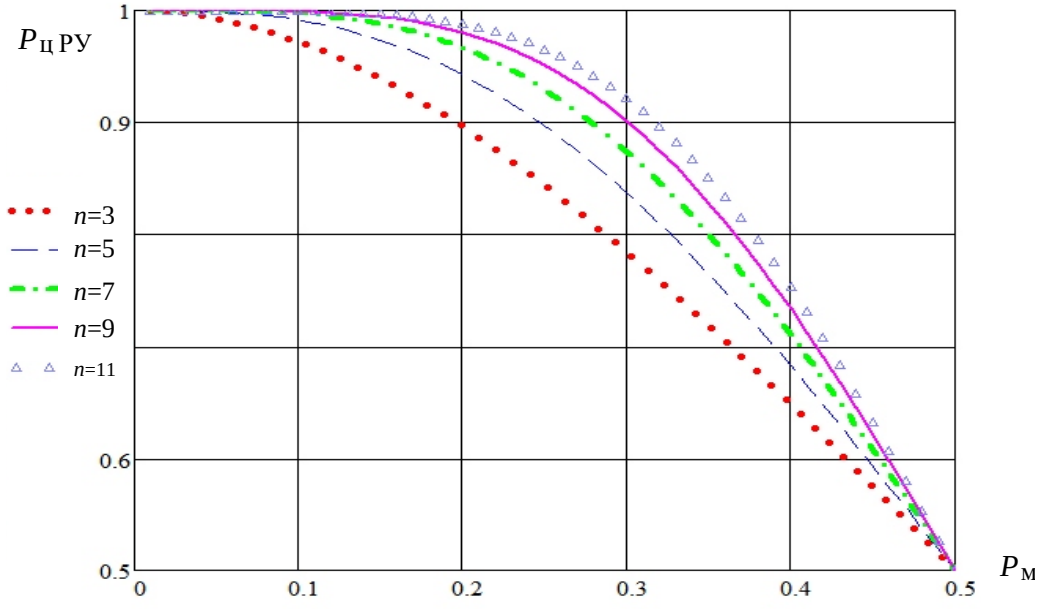


Рисунок 4 – Результаты теоретического расчета $P_{\text{ц РУ}} = f(P_{\text{м}})$ для различных значений n

В диссертации предложены показатели эффективности обеспечения доступности/целостности информации [8, 11, 18]. При организации n параллельных соединений между УИ и УП необходимо выбирать те маршруты, у которых:

$$\max\left\{\alpha_i = \left|\frac{\ln(1-p_i)}{c_i}\right|; i=\overline{1,n}\right\}, \quad (6)$$

где: c_i – стоимость i-го маршрута между УИ и УП для обеспечения доступности либо целостности информации;

p_i – вероятность обеспечения доступности либо целостности i-ого маршрута.

В заключении главы делается вывод – реализация разработанных методов защиты информации возможна за счет технологий сетевого уровня МВОС, что позволит обеспечить требуемый уровень информационной безопасности и QoS высокоскоростных приложений МСС, функционирующих в реальном масштабе времени.

В третьей главе: приводятся основные термины и определения предметной области «Маршрутизация»; разрабатывается обобщенная функциональная модель маршрутизации в МСС [25, 32, 33, 37]; приводится обзор методов маршрутизации в МСС; разрабатывается новая классификация методов маршрутизации в сетях связи; предлагаются новые методы маршрутизации в МСС [5, 25, 34, 37].

Обобщенная функциональная модель маршрутизации в МСС содержит два уровня − уровень формирования плана распределения информации (ПРИ) на сети (протоколы маршрутизации) и уровень выбора исходящий трактов передачи сообщений (ТПС) (протоколы сигнализации). Продуктом ПРИ являются таблицы маршрутизации (ТМ) для каждого приложения МСС $\left(\varepsilon=\overline{1,\mathrm{E}}\right)$. Уровень сигнализации, используя методы выбора исходящих трактов передачи сообщений (ТПС), по ТМ формирует: таблицы коммутации (ТК) для каждой заявки на установление соединения с требуемым QoS; структуру соединений защиты с целью обеспечения информационной безопасности.

Обзор методов маршрутизации (с учетом разработанной модели маршрутизации МСС) позволил разработать новую классификацию методов маршрутизации (рисунок 5) и тем самым: систематизировать и обобщить известные решения, реализованные в технологиях IP, ATM и MPLS. В результате, комбинируя методы формирования ПРИ и выбора исходящих ТПС, предложены новые методы маршрутизации, имеющие перспективу для использования в МСС.

«Логико-статистический» является комбинацией «Логического» и «Статистического» методов формирования ПРИ. В условиях отсутствия внешних деструктивных воздействий на элементы МСС формирование ПРИ осуществляется «Статистическим» методом. В условиях резкого изменения структуры МСС (по каким либо причинам) применяется «Логический» метод.

«Логико-лавинный» является комбинацией «Лавинного» и «Логического» методов и состоит в том, что для установления оптимального соединения из УИ организуется «Лавинный» поиск, но не во всех направлениях, а лишь в сторону УП. Волна поиска при этом распространяется в пределах некоторой зоны в виде

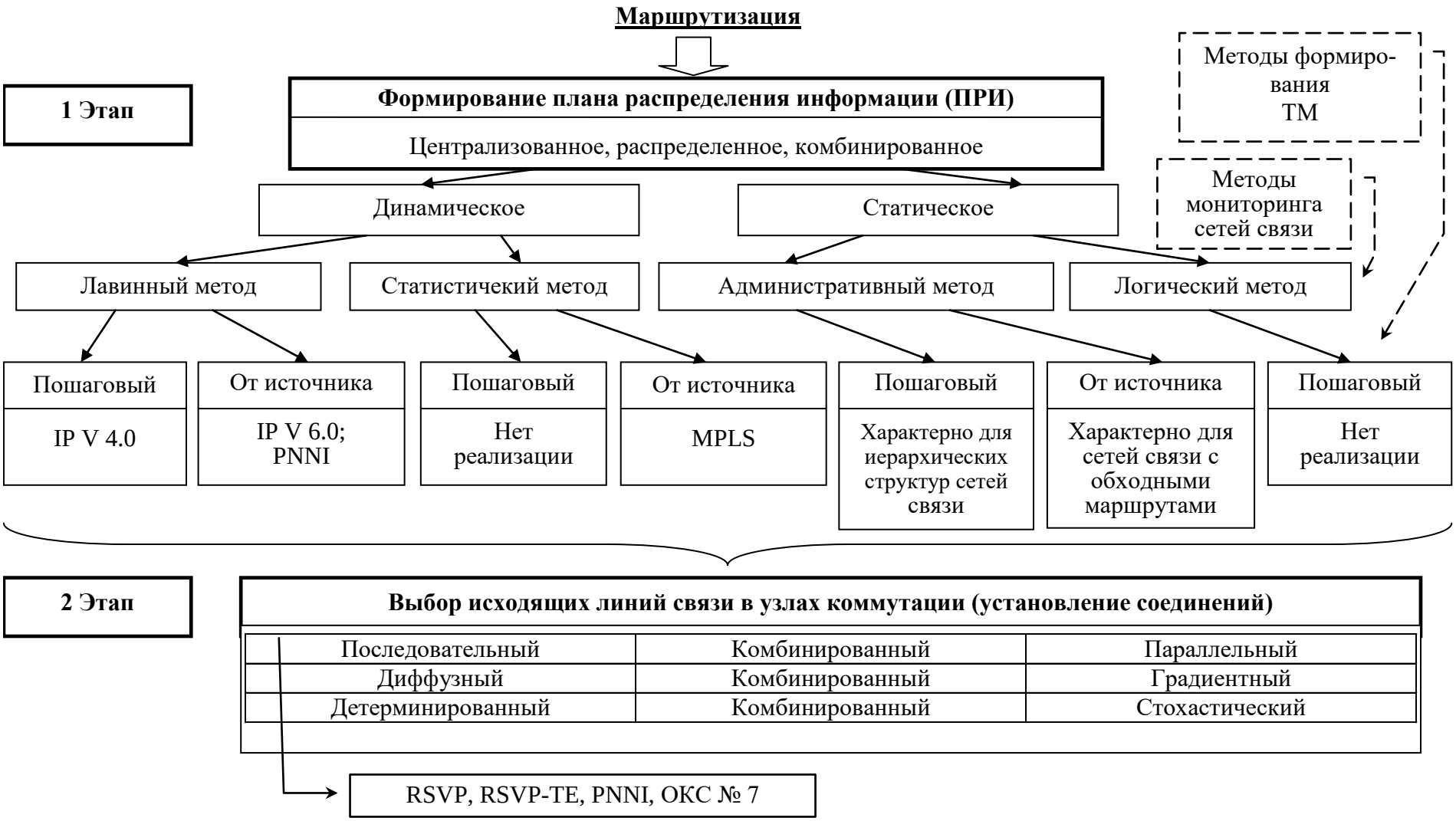


Рисунок 5 – Классификация методов маршрутизации в сетях связи

полосы, охватывающей УИ и УП. Ширина полосы зависит от приоритета пользователя, состояния элементов сети, требований приложений к QoS. Для пользователей низшей категории, количество выбранных ТПС может не превышать одного, тогда поиск превращается в "чисто" последовательный.

«Логико-лавинно-статистический» метод является обобщением «Логического», «Лавинного» и «Статистического». Применение одного из них зависит от условий функционирования МСС. В штатном режиме функционирования МСС формирование ПРИ осуществляется «Статистическим» методом. В случае выхода из строя элементов МСС (по каким либо причинам) применяется «Логико-лавинный» метод.

Четвертая глава посвящена разработке математических моделей маршрутизации МСС в условиях внешних деструктивных воздействий.

Представим структуру МСС в виде графа $G[A_S, M_S]$ с множеством: вершин $A_S = \{a_i\}; i = \overline{1,S}$, соответствующих узлам коммутации (УК); ребер $M_S = \{m_{ij}\}; i, j = \overline{1,S}; i \neq j$, соответствующих ТПС. Каждый ТПС обладает средней пропускной способностью $r_{ij}; i, j = \overline{1,S}; i \neq j$, которую будем называть ресурсом ТПС. Средний общий сетевой ресурс МСС определятся выражением:

$$R_{\text{о}} = \sum_{i,\, j=1; i \neq j}^{S} r_{ij} \text{ бит/с.}$$

I. Математическая *модель влияния методов формирования ПРИ на объем доступных сетевых ресурсов* [1, 6] состоит в представлении сетевых средних ресурсов, необходимых для формирования ТМ в каждом УК, в виде полинома:

$$R_{\text{тм}}^{(ROUT)} = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0; \qquad (7)$$

$a_i; i = \overline{0,n}$ – коэффициенты пропорциональности для каждого из методов формирования ПРИ; $0 \le x \le 1$ – переменная, которая определяет степень недоступности средних сетевых ресурсов вследствие внешних деструктивных воздействий на МСС.

При «Лавинном» методе формирования ПРИ каждый УК генерирует через равные интервалы времени Δt зонд-сигналы путем широковещательной рассылки *K* блоков данных размером *B*. В этом случае выражение (7) примет вид:

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

Относительный объем доступных средних сетевых ресурсов для передачи пользовательской информации будет определяться выражением:

$$R_{\text{п}}^{(\text{лав})} = (1 - x) - \frac{K \cdot B \cdot S}{\Delta t \cdot R_{\text{о}}} = 1 - x - y. \qquad (8)$$

При «Статистическом» методе корректировка ТМ происходит при попытке установления соединений. Следовательно, по аналогии с (8) имеем:

$$R_{\text{п}}^{(\text{стат})} = (1-x) - \frac{\left(a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0\right)}{R_{\text{о}}} = 1 - x - a'_0{}^{(\text{стат})} - \sum_{i=1}^{n} a'_i{}^{(\text{стат})};$$

$$a'_i = \frac{a_i}{R_{\text{о}}}.$$

При ограничении только одним членом полученного ряда (верхняя оценка) для «Статистического» метода формирования ПРИ получим:

$$R_{\text{п}}^{(\text{стат})} \le 1 - x - a'_1 \cdot x. \qquad (9)$$

На рисунке 6 приведены графики зависимостей (8) и (9) при изменении коэффициентов у и a'_1. Анализ данных зависимостей позволяет сделать следующие выводы. При выполнении условия $x = \frac{y}{a'_1}$ существует зона ($x \approx 0{,}2 \div 0{,}4$), в пределах которой оба метода формирования ПРИ используют одинаковые средние сетевые ресурсы. В случае, если $x < \frac{y}{a'_1}$ ($0 \le x \le (0{,}2 \div 0{,}4)$), то «Статистический» метод использует меньше сетевых ресурсов, чем «Лавинный». Если $x > (0{,}2 \div 0{,}4)$, то «Статистический» метод дает худшие результаты, по сравнению с «Лавинным».

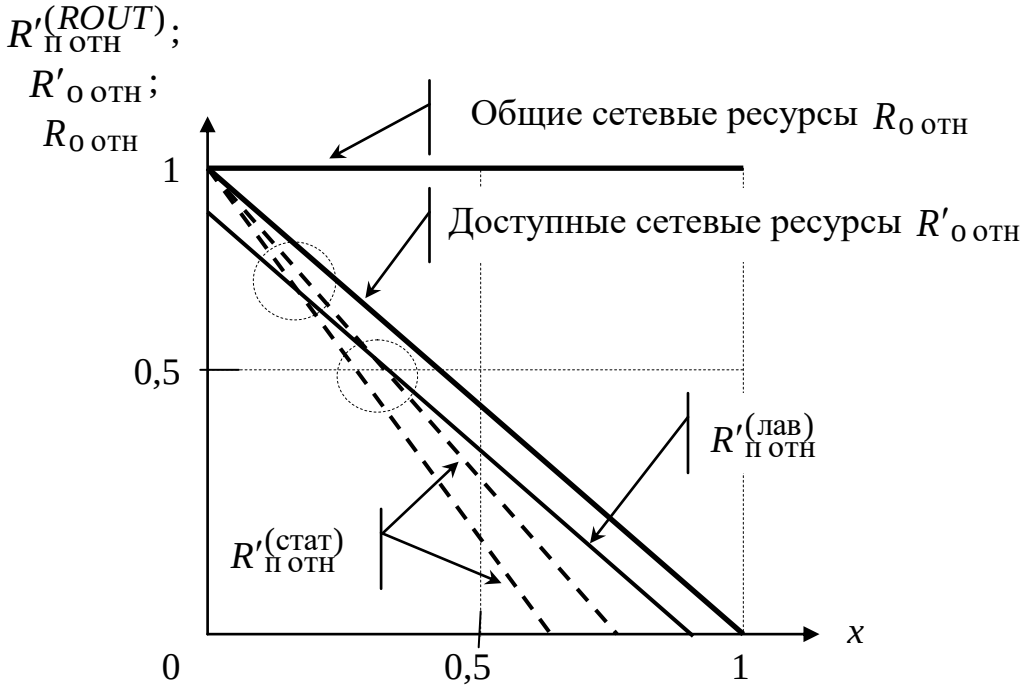


Рисунок 6 – Зависимости средних сетевых ресурсов от степени недоступности общих сетевых ресурсов МСС *x*

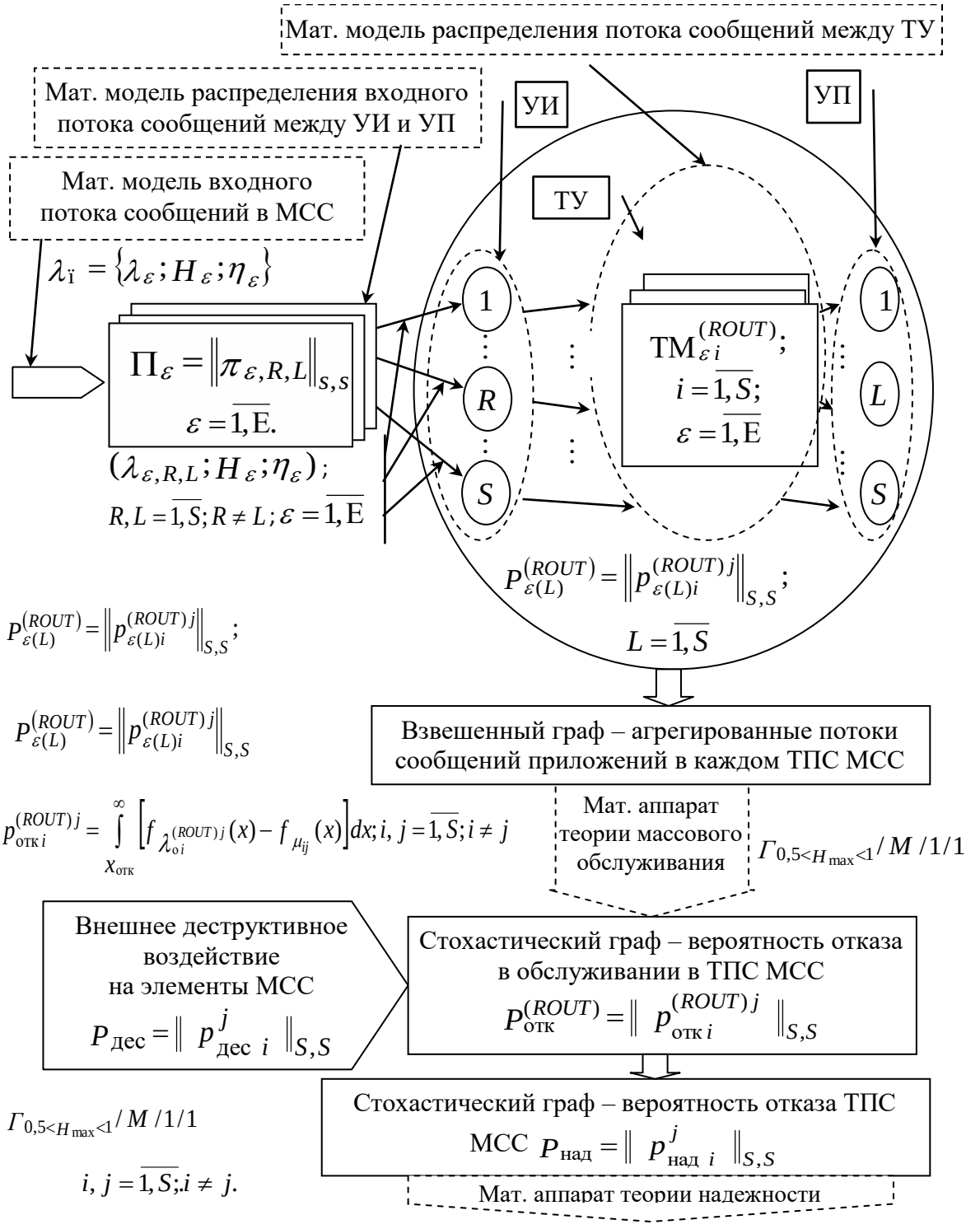


Рисунок 7 – Концепция математической модели маршрутизации в МСС

II. Математическая *модель маршрутизации в условиях входного самоподобного трафика и внешних деструктивных воздействий на элементы МСС* [6, 21, 25, 26, 30, 33, 37] представлена на рисунке 7.

Исходными данными являются.

1. Метод маршрутизации $ROUT$, который задается процедурой выбора исходящих ТПС на множестве S пошаговых ТМ для ε-го приложения:

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

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

χ_j – степень a_j-го УК. 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 выбран ν-й исходящий ТПС.

2. Пропускная способность ТПС МСС характеризуются $\mu_{ij}; i, j = \overline{1,S}; i \neq j$ – наибольшим количеством пакетов, передаваемых за единицу времени. Длительность обслуживания пакетов сообщений, поступающего асинхронного потока данных в ТПС между a_i и a_j УК, подчиняется экспоненциальному закону с параметром:

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

3. Поступающий в a_R-й УИ МСС информационный поток для последующей передачи в a_L-й УП характеризуется комбинацией параметров $(\lambda_{\varepsilon,R,L}; H_{\varepsilon}; \eta_{\varepsilon})$, где: H_{ε} – параметр Херста ε-го приложения; η_{ε} – средняя длина пакетов сообщений ε-го приложения.

Плотность распределения вероятностей последовательности промежутков между пакетами сообщений ε-го приложения, поступающими в a_R-й УИ для последующей передачи в a_L-й УП, определяется выражением:

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

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

Из свойства агрегирования самоподобных потоков

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

следует, что 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:

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

5. Внешнее деструктивное воздействие на МСС учитываются матрицей:

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

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

Критериями оценки функционирования МСС приняты:

$$\{\hat{P}_{\text{отк}}; \hat{p}^{(R,L)}_{\text{отк}}\} = f\{G[A_S, M_S]; \Pi_{\varepsilon}; \lambda_{\varepsilon}; H_{\varepsilon}; \mu; ROUT\}; R, L = \overline{1,L}; R \ne L; \varepsilon = \overline{1,\mathrm{E}}; \quad (10)$$

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

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

Входящий в МСС поток пакетов сообщений ε-го приложения в соответствии с матрицей тяготений Π_{ε} дезагрегируется на отдельные потоки, которые поступают в соответствующие УИ для последующей передачи в УП. Подчиняясь заранее определенному методу маршрутизации, потоки сообщений различных приложений распределяются по всем ТПС МСС. Далее, агрегируя распределенные потоки сообщений, определяется общий суммарный поток каждого ТПС МСС. Учитывая, что каждый 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 в обслуживании приложений МСС.

Внешнее деструктивное воздействие реализуется в заранее заданных вероятностях отказа ТПС МСС. Считается, что вероятности отказа обслуживания приложений МСС в каждом ТПС и вероятности отказа самих ТПС являются независимыми событиями. В этом случае 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 (10). Методика математического моделирования маршрутизации в МСС состоит в решении системы уравнений:

$$
\begin{cases}
P_{\varepsilon(L)}^{(ROUT)} = \left\| p_{\varepsilon(L)i}^{(ROUT)\,j} \right\|_{S,S} \; i,\, j = \overline{1,S}; \\
\lambda_{\text{o}\,i}^{(ROUT)\,j} = \sum_{L=1}^{S} \sum_{\varepsilon=1}^{\text{E}} \lambda_{\varepsilon} \cdot \pi_{\varepsilon,i,j} \cdot p_{\varepsilon(L)i}^{(ROUT)\,j}; i, j = \overline{1,S}; i \neq j; \\
p_{\text{отк}\;i}^{(ROUT)\,j} = \int\limits_{x_{\text{отк}}}^{\infty} \left[\dfrac{\lambda_{\text{o}\,i}^{(ROUT)} H_{\max\,j} \cdot x^{H_{\max}-1} \cdot e^{-\lambda_{\text{o}\,i}^{(ROUT)\,j \cdot x}}}{\int\limits_{0}^{\infty} x^{H_{\max}-1} \cdot e^{-x} dx} - \mu_{ij} e^{-\mu_{ij} \cdot x} \right] dx; i, j = \overline{1,S}; i \neq j \\
P_{\text{над}\;i}^{j} = (1 - p_{\text{отк}\;i}^{(ROUT)\,j}) \cdot (1 - p_{\text{дес}\;i}^{j}); i, j = \overline{1,S; i \neq j}; \\
\hat{p}_{\text{отк}}^{(R,L)} = 1 - \sum_{k=1}^{2^{\kappa}} Q_{RL}^{(k)} \cdot p_k = 1 - \sum_{k=1}^{2^{\kappa}} Q_{RL}^{(k)} \cdot \left(\prod_{\varphi=1}^{\kappa} p_{\varphi}^{\sigma_{\varphi}} \cdot q_{\varphi}^{1-\sigma_{\varphi}} \right); R, L = \overline{1,S}; \qquad (11) \\
\hat{P}_{\text{отк}} = 1 - \sum_{k=1}^{2^{\kappa}} Q_{o}^{(k)} \cdot p_k = 1 - \sum_{k=1}^{2^{\kappa}} Q_{o}^{(k)} \prod_{\varphi=1}^{\kappa} p_{\varphi}^{\sigma_{\varphi}} \cdot q_{\varphi}^{1-\sigma_{\varphi}}. \qquad (12)
\end{cases}
$$

В диссертации для определения (11), (12) используется метод статистического моделирования [12, 20, 22, 24, 33, 36]. 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 по правилу:

$$
\begin{cases}
\text{Если } X_{\varphi} \geq p_{\varphi} \Rightarrow \text{элемент графа считается выведенным из строя;} \\
\text{Если } X_{\varphi} < p_{\varphi} \Rightarrow \text{элемент графа находится в исправном состоянии.}
\end{cases} \qquad (13)
$$

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 искомой оценкой.

Абсолютная погрешность результата вычисления определяется формулой:

$$\Delta_a = N_o^{-0,5} \cdot \sigma \cdot t_{\beta}; \qquad (14)$$

Δ_a – абсолютное значение ошибки (половина доверительного интервала);

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

$\sigma^2 = \hat{P}_{\text{отк}} \cdot (1 - \hat{P}_{\text{отк}})$ 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 $(1+\beta)^{-1}$.

В диссертации разработан метод проверки графа на связность меньшей сложности [7, 19, 23, 33, 36]. Анализируемый граф «разбивают» на подграфы. Каждый подграф проверяют на связность параллельным «стягиванием» смежных вершин, к первоначально выбранной, до тех пор, пока подграф не представится в виде 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).

Показано, что при оптимальном числе разбиений графа на $N_{\text{опт}} = \sqrt{S}$ подграфов алгоритмическая сложность разработанного метода в $\sqrt{S}$ раз меньше по сравнению с известными методами проверки графа на связность. Данный результат подтвержден экспериментально [7, 19, 23]. На рисунке 8 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.

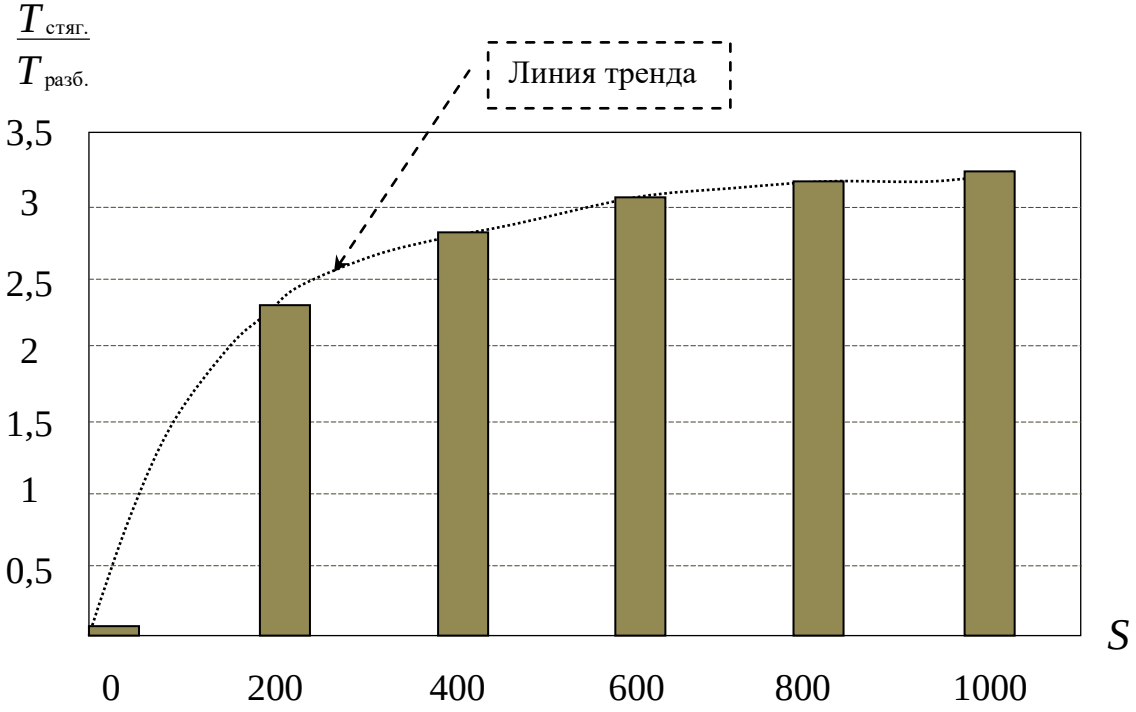


Рисунок 8 – Гистограмма относительного временного выигрыша проверки графа сети на связность методом «Разбиения» по отношению к методу «Стягивания»

I. *Методика определения ПРИ на однородной ячеистой сети связи большой размерности* [33] разработана для случая, когда структура сети связи приобретает некоторую регулярность, что характерно для ячеистых сетей связи. Суть методики состоит в том, что структура сети связи с квадратной ячейкой вкладывается в прямоугольную систему координат. Каждому УК присваивается адрес с координатами $\{i, j\}$. Для выбора более предпочтительного направления к УП из транзитных УК (включая УИ) достаточно сопоставить между собой

координаты данного узла с УП и продолжить поиск маршрута по направлению координаты *X* или *Y*, имеющей большее значение, соответствующих коэффициентов:

$$n_x = \frac{P_x \cdot q_x}{P_x \cdot q_x + P_y \cdot q_y};\ n_y = \frac{P_y \cdot q_y}{P_x \cdot q_x + P_y \cdot q_y}, \tag{15}$$

где

$$P_x = \frac{i}{i+j};\ P_y = \frac{j}{i+j};\ q_x = \frac{\Omega_X}{\Omega_X + \Omega_y};\ q_x = \frac{\Omega_y}{\Omega_X + \Omega_y};$$

Ω_x, Ω_y – вероятностно-временные параметры, определяющие QoS МСС в направлении *X* и *Y*, соответственно.

Данный подход позволяет реализовать некоторые, наиболее характерные методы маршрутизации (рисунок 5): «Градиентный вероятносто-детерминированный последовательный с логическим методом формирования ПРИ» (ГВДПЛ); «Диффузный без возвращения назад вероятносто-детерминированный последовательный с логическим методом формирования плана распределения информации» (ДБВНВДПЛ); «Диффузный вероятносто-детерминированный последовательный с логическим методом формирования плана распределения информации» (ДВДПЛ); «Локально-лавинный с детерминированным выбором зоны поиска маршрута и логическим методом формирования плана распределения информации» (ЛВДЛ).

II. *Упрощенная имитационная модель маршрутизации* [33] в качестве критерия сравнения методов маршрутизации использует способность МСС пропустить максимальную нагрузку между парами УИ и УП, выраженную, соответственно, в виде коэффициента пропускной способности в среднем по сети:

$$W = \frac{\tilde{\Xi}}{\Xi_{\max}}; \tag{16}$$

$\tilde{\Xi}$ – среднее количество установленных соединений за $N_{\text{о}}$ испытаний методом статистического моделирования; $\Xi_{\max}$ – максимально возможное количество соединений на сети:

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

$R_{\text{о}}$ – общий средний сетевой ресурс МСС; $L_{\text{ср}}$ – средняя длина маршрута между УИ и УП.

Исходными данными являются: матрица виртуальных каналов связи (ВКС) $K = \left\| k_{i,j} \right\|_{S,S}$ в фиксированный момент времени *t*; метод маршрутизации *ROUT*; количество заявок N, поступающих от пользователей в сеть в фиксированный момент времени *t*; матрица тяготений $\Pi_\varepsilon = \left\| \pi_{\varepsilon,R,L} \right\|_{S,S}$; матрица вероятностей внешних деструктивных воздействий на элементы сети $P_{\text{дес}} = \left\| \ p^{j}_{\text{дес}\ i} \ \right\|_{S,S}$.

Порядок определения (20) следующий. В соответствии с матрицей тяготений рассчитывается $L_{\text{ср}}$. Суммированием всех ВКС преобразованной сети $K = \left\| k_{i,j} \right\|_{S,S}$ (с учетом заданной матрицы $P_{\text{дес}} = \left\| \ p^{j}_{\text{дес}\ i} \ \right\|_{S,S}$) определяется средний общий сетевой ресурс МСС ($R_{\text{о}}$). Для выполнения преобразования сети $K = \left\| k_{i,j} \right\|_{S,S}$ (с учетом заданной матрицы $P_{\text{дес}} = \left\| \ p^{j}_{\text{дес}\ i} \ \right\|_{S,S}$) используется аналогичный алгоритм вывода из строя элементов сети (13). Вычисляется $\Xi_{\max}$.

Далее выполняют $N_{\text{о}}$ испытаний. Каждое испытание состоит из следующих процедур. Имитируется внешнее деструктивное воздействие на элементы МСС. Для этого, используя алгоритм (13) выполняется вывод из строя элементов матрицы $K = \left\| k_{i,j} \right\|_{S,S}$. Затем на преобразованной матрице $K = \left\| k_{i,j} \right\|_{S,S}$ выполняют N действий: поиск маршрутов; в случае нахождения маршрута осуществляется занятие соответствующих ВКС; подсчет количества установленных маршрутов. Для этого случайным образом в соответствии с матрицей тяготений 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 остаётся занятым до конца испытания. То есть, соответствующие ВКС в преобразованной матрице $K = \left\| k_{i,j} \right\|_{S,S}$ считаются занятыми. По окончанию N действий определяется $\Xi(I); I = \overline{1, N_{\text{о}}}$ количество установленных соединений в данном испытании. После $N_{\text{о}}$ испытаний рассчитывается среднее число установленных соединений:

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

В итоге вычисляются искомые значения (16). Таким образом, если при равных вероятностях отказа в одновременном установлении N соединений ($\hat{P}_{\text{отк}}$), два различных метода маршрутизации получили разные W, то предпочтительным считается тот, у которого коэффициент пропускной способности выше.

Пятая глава посвящена анализу результатов моделирования методов маршрутизации для разработанных в четвертой главе моделей.

I. *Имитационное моделирование МСС в условиях ограниченных сетевых ресурсов* [33] выполнено с использованием специализированного программного продукта Opnet Modeler v 14.0. Структура МСС представлена на рисунке 9. Каждая локальная сеть организована на базе технологии Fast Ethernet: на транспортном уровне поддерживается протоколами TCP и UDP; содержит 10 компьютеров; генерирует трафик видеоконференции со скоростью 1350 кбит/с.

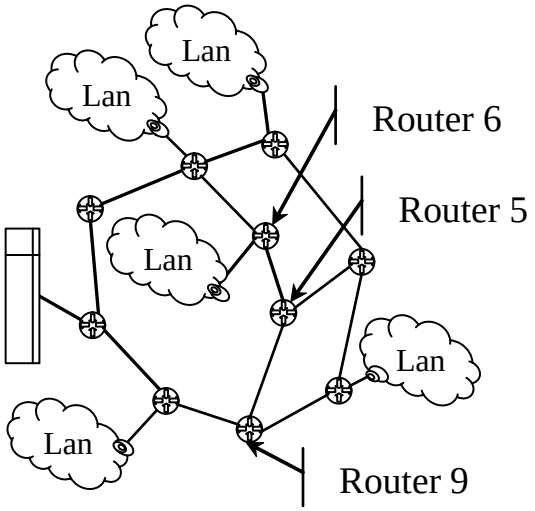
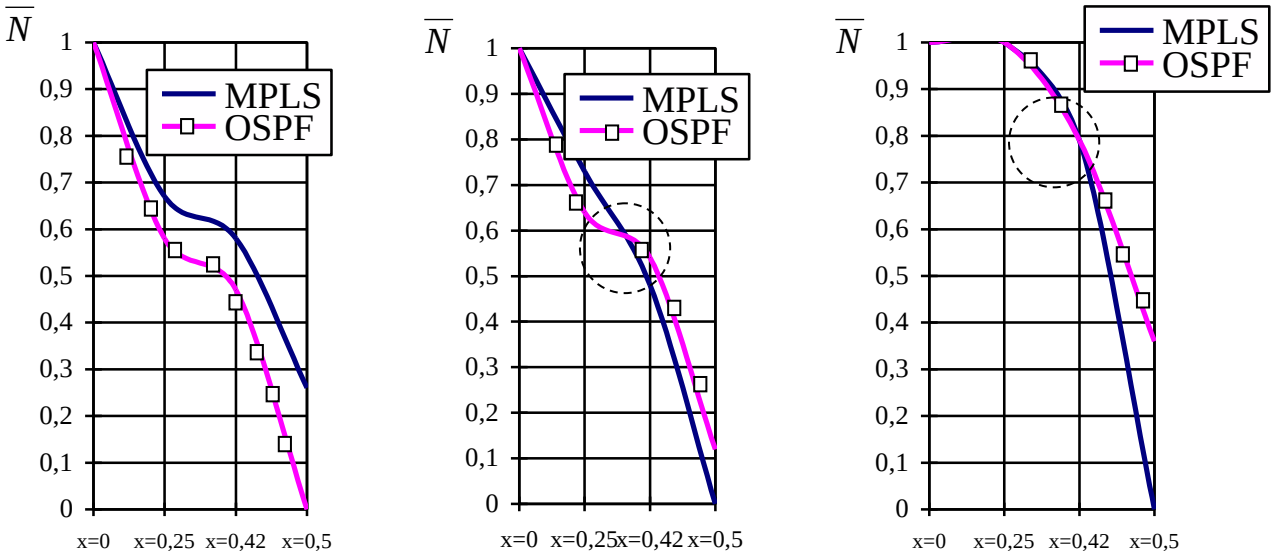


Рисунок 9 – Структура анализируемой МСС

Маршрутизаторы в каждом испытании поддерживают только OSPF или MPLS и между собой 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. Пошаговое уменьшение пропускной способности сетевого кабеля от 1000 Мбит/с до 10 Мбит/с сокращает общие сетевые ресурсы $R_o = 12 \cdot r$ МСС..

Одно испытание состоит в тридцати минутной имитации функционирования анализируемой МСС. С нулевой до пятой минуты МСС функционирует в штатном режиме. На пятой минуте маршрутизатор Router9 выходит из строя. В таком состоянии МСС продолжает функционировать до десятой минуты. На десятой и пятнадцатой минутах, соответственно, выходят из строя Router5 и Router6. Данный процесс имитирует внешние деструктивные воздействия на МСС. На рисунке 10 представлены нормированные результаты имитационного моделирования.



А) r = 1000 Мбит/с Б) r = 100 Мбит/с В) r = 10 Мбит/с

Рисунок 10 – Нормированные результаты моделирования

Здесь: x – степень недоступности общих сетевых ресурсов анализируемой сети; $\overline{N}$ – нормированное количество потерянных пакетов за единицу времени

$$x_i = \frac{R_o - R_o^{(i)}}{R_o}; i = \overline{1,4}. \ \overline{N} = 1 - \frac{N_{\text{потерь}}}{N_{\text{потерь (max)}}^{(j)}}; j = \overline{1,3};$$

$N_{\text{потерь}}$ – количество потерянных пакетов за единицу времени в одном испытании имитационного моделирования; $N_{\text{потерь (max)}}^{(j)}; j = \overline{1,3}$ – максимальное значение

$N_{\text{потерь}}$ в каждом из трех испытаний имитационного моделирования; $R_{\text{о}}^{(i)}; i=\overline{1,4}$ – общий сетевой ресурс анализируемой МСС в одном имитационном испытании на соответствующем интервале времени, который определяется:

$$\begin{cases} R_{\text{о}}^{(1)}=12\cdot r & \text{интервал моделирования с 0 до 5 минуты;} \\ R_{\text{о}}^{(2)}=9\cdot r & \text{интервал моделирования с 5 до 10 минуты;} \\ R_{\text{о}}^{(3)}=7\cdot r & \text{интервал моделирования с 10 до 15 минуты;} \\ R_{\text{о}}^{(4)}=6\cdot r & \text{интервал моделирования с 15 до 30 минуты.} \end{cases}$$

Результаты моделирования подтверждают полученные ранее результаты (рисунок 6), и позволяют утверждать, что в условиях внешнего деструктивного воздействия, при котором примерно 30% сетевых ресурсов МСС выходит из строя, целесообразно применять «Лавинные» методы формирования ПРИ.

II. *Математическое моделирование маршрутизации в условиях входного самоподобного трафика и внешних деструктивных воздействий на элементы МСС* [30, 33] проведно на однородной ячеистой структуре, содержащей двенадцать УК. 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 потока данных в ТПС между a_i и a_j УК подчиняется экспоненциальному закону с параметром $w=\frac{1}{\mu}$. Пакеты ε–го приложения $(\varepsilon=\overline{1,3})$ поступают в МСС с интенсивностью $\lambda=\lambda_\varepsilon; \varepsilon=\overline{1,\text{E}}$, величина которой принимает одно их значений: $\lambda_1=10\cdot 10^6$; $\lambda_2=50\cdot 10^6$. $H=H_\varepsilon=0{,}5$; $\varepsilon=\overline{1,\text{E}}$ – параметр Херста ε-го приложения.

Анализируемые методы маршрутизации: «Последовательный детерминированный с лавинным методом формирования ПРИ»; «Параллельный детерминированный с лавинным методом формирования ПРИ»; «Последовательный детерминированный со статистическим методом формирования ПРИ»; «Параллельный детерминированный со статистическим методом формирования ПРИ».

Вероятность поступления потока данных ε-го приложения в a_R-й УИ для его последующей передачи a_L-му УП определяется матрицей тяготений Π_ε. Элементы матрицы тяготений равны между собой и имеют равновероятный характер. Внешнее деструктивное воздействие на элементы МСС описывается матрицей $P_{\text{дес}}$. При моделировании принято, что вероятности $p_{\text{дес}}=p^{j}_{\text{дес}\ i}; i, j=\overline{1,S}$, значение которых изменялось от 0 до 0,6 с шагом $\Delta p_{\text{дес}}=0{,}05$. Погрешность измерений в исследованиях определялась по формуле (14) и не превышает одного процента.

Результаты моделирования показали, что при $\lambda_1=10\cdot 10^6$ характер влияния методов маршрутизации на интегральную оценку (12) в целом одинаковое.

Графики зависимостей вероятности отказа в обслуживании в целом по МСС (интегральная оценка (12)) при $\lambda_2 = 50 \cdot 10^6$ представлены на рисунке 11.

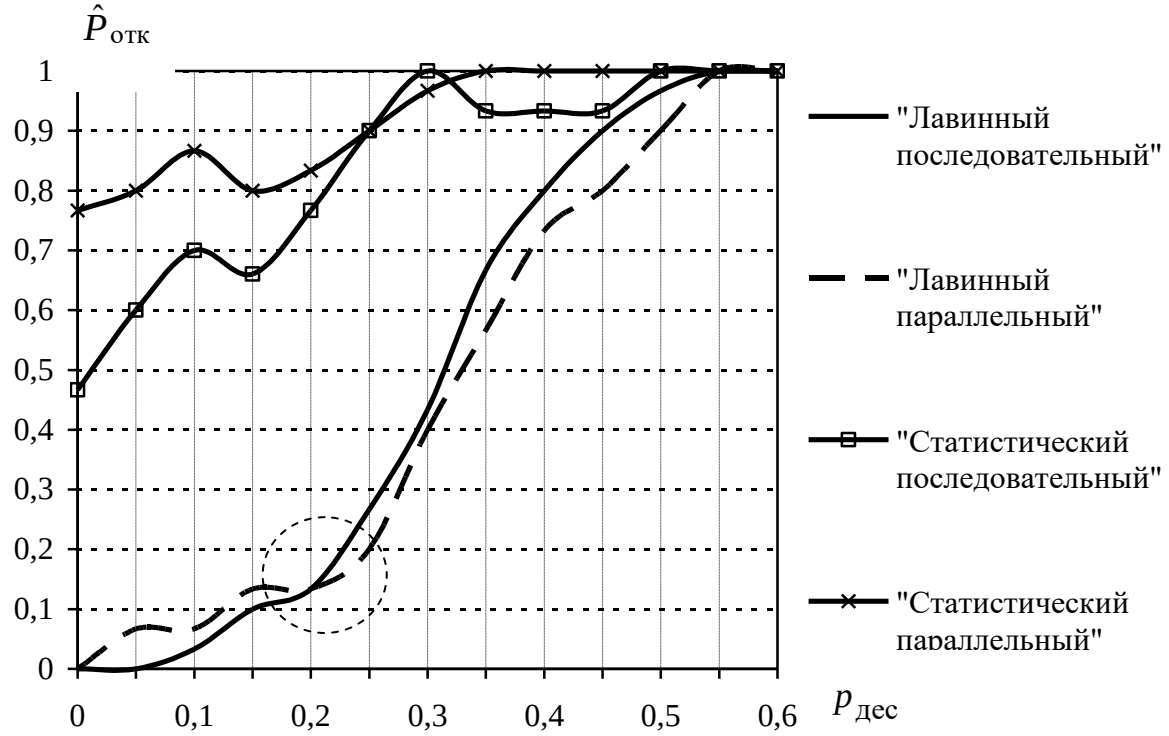


Рисунок 11 – Зависимости вероятности отказа в обслуживании в целом по МСС

В результате можно заключить, что увеличение интенсивности поступления пакетов в МСС до $\lambda_2 = 50 \cdot 10^6$ приводит к значительному повышению вероятности отказа в обслуживании в целом по МСС. Причем «Лавинные» методы имеют существенное преимущество по сравнению со «Статистическими».

III. Анализ результатов *моделирования маршрутизации на упрощенной имитационной модели сети связи* [33]. При определении ПРИ использовалась методика для однородной ячеистой сети связи большой размерности (15). В качестве исходных данных было принято: $X_{\max} = 10$; $Y_{\max} = 5$; $S = X_{\max} \cdot Y_{\max} = 50$; $k_{i,j} = 8; i, j = \overline{1,50}$; $p_{\text{дес}} = p^{j}_{\text{дес}\ i}; i, j = \overline{1,S}$ изменялось от 0 до 0,8 с шагом $\Delta p_{\text{дес}} = 0{,}2;$ равновероятный выбор УИ и УП, то есть значения элементов матрицы тяготений $\pi_{i,j} = \dfrac{1}{S^2}; i, j = \overline{1,S}$; $N_{\text{о}} = 1000$.

На рисунке 12 представлены результаты статистического моделирования ($\Delta_a \le 0{,}08$) для следующих методов маршрутизации: «Градиентный вероятносто-детерминированный последовательный с логическим методом формирования ПРИ» (ГВДПЛ); «Диффузный без возвращения назад вероятносто-детерминированный последовательный с логическим методом формирования ПРИ» (ДБВВДПЛ); «Диффузный вероятносто-детерминированный последовательный с логическим методом формирования ПРИ» (ДВДПЛ);

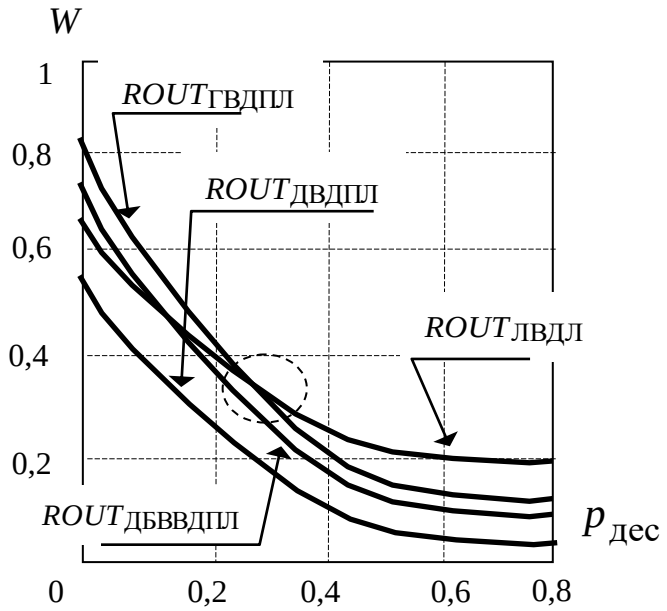


Рисунок 12 – Зависимость $W = f(P_{\text{дес}})$ для различных методов маршрутизации

«Локально-лавинный с детерминированным выбором зоны поиска маршрута и логическим методом формирования ПРИ» (ЛВДЛ).

Исследования (с использованием различных математических и имитационных моделей) методов маршрутизации в условиях внешних деструктивных воздействий на элементы МСС позволяют сделать следующие выводы.

1. Целесообразность применения того или иного метода маршрутизации зависит от конкретных масштабов внешнего деструктивного воздействия.

2. В условиях практического 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. При условии выхода из строя более 20 % ÷ 30 % сетевых ресурсов МСС «Лавинные параллельные» методы маршрутизации по сравнению со «Статистическими» показывают лучшие результаты. Данный результат независимо подтвержден на различных структурах МСС 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 МСС предусматривать не менее 30 % резерва сетевых ресурсов.

Разработанные в предыдущих главах: методы обеспечения базовых параметров защиты информации (конфиденциальность, доступность и целостность); методы маршрутизации и проведенные исследования методов маршрутизации в условиях внешних деструктивных воздействий на элементы МСС позволяют создать методики защиты информации за счет технологий сетевого уровня модели взаимосвязи открытых систем без снижения качества обслуживания приложений МСС, чему, и посвящена **шестая глава диссертации**.

Пользователю со стороны МСС (оператора МСС) предоставляется не только выбор приложения 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 МСС, реализует не только соединение, поддерживающее QoS для выбранного приложения, но и заявленный пользователем профиль в виде структуры соединений защиты информации.

Концепция методики защиты информации в МСС (рисунки 13, 14) включает в себя последовательное применение разработанных методик обеспечения доступности, конфиденциальности и целостности [33].

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 для каждого приложения МСС $\left(\varepsilon = \overline{1,\text{E}}\right)$ ТМ (например, от источника) (оператор 02):

$$M_{\varepsilon}{}^{(j)} = \left(\overline{\mu_{(\varepsilon)1}^{(j)}},...,\overline{\mu_{(\varepsilon)i}^{(j)}},...,\overline{\mu_{(\varepsilon)j-1}^{(j)}},\overline{\mu_{(\varepsilon)j+1}^{(j)}},...,\overline{\mu_{(\varepsilon)S}^{(j)}}\right), \varepsilon = \overline{1,\text{E}},$$

где

$$\overline{\mu_{(\varepsilon)i}^{(j)}} = \left(\langle \mu_{(\varepsilon)i1}^{(j)} \rangle,...,\langle \mu_{(\varepsilon)i\nu}^{(j)} \rangle,...\langle \mu_{(\varepsilon)im_j}^{(j)} \rangle\right), i, j = \overline{1,S}; i \neq j, \varepsilon = \overline{1,\text{E}};$$

$\overline{\mu_{(\varepsilon)i}^{(j)}}$ – 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) выполняются следующие процедуры.

1. Расчет для каждого маршрута $\left\langle \mu_{(\varepsilon)i\nu}^{(j)} \right\rangle$ выражения:

$$\overline{\alpha}_i = \left| \frac{\ln(1-p_i)}{c_i} \right|; i = \overline{1,m_j}.$$

Здесь в качестве переменных c_i и p_i можно использовать следующие значения. Для c_i – вместо стоимости $\left\langle \mu_{(\varepsilon)i\nu}^{(j)} \right\rangle$-го маршрута можно использовать количество транзитных УК между УИ и УП. В качестве p_i можно использовать:

– надежность $\left\langle \mu_{(\varepsilon)i\nu}^{(j)} \right\rangle$-го маршрута, выраженную в вероятностных величинах;

– $(1-p_{\text{ош}\,i})$, где $p_{\text{ош}\,i}$ – вероятность ошибочного приема на символ, пакет, сообщение и т.п. $\left\langle \mu^{(j)}_{(\varepsilon)i\nu} \right\rangle$-го маршрута;

– $(1-p_{\text{м}\,i})$, где $p_{\text{м}\,i}$ – вероятность модификации сообщения $\left\langle \mu^{(j)}_{(\varepsilon)i\nu} \right\rangle$-го маршрута.

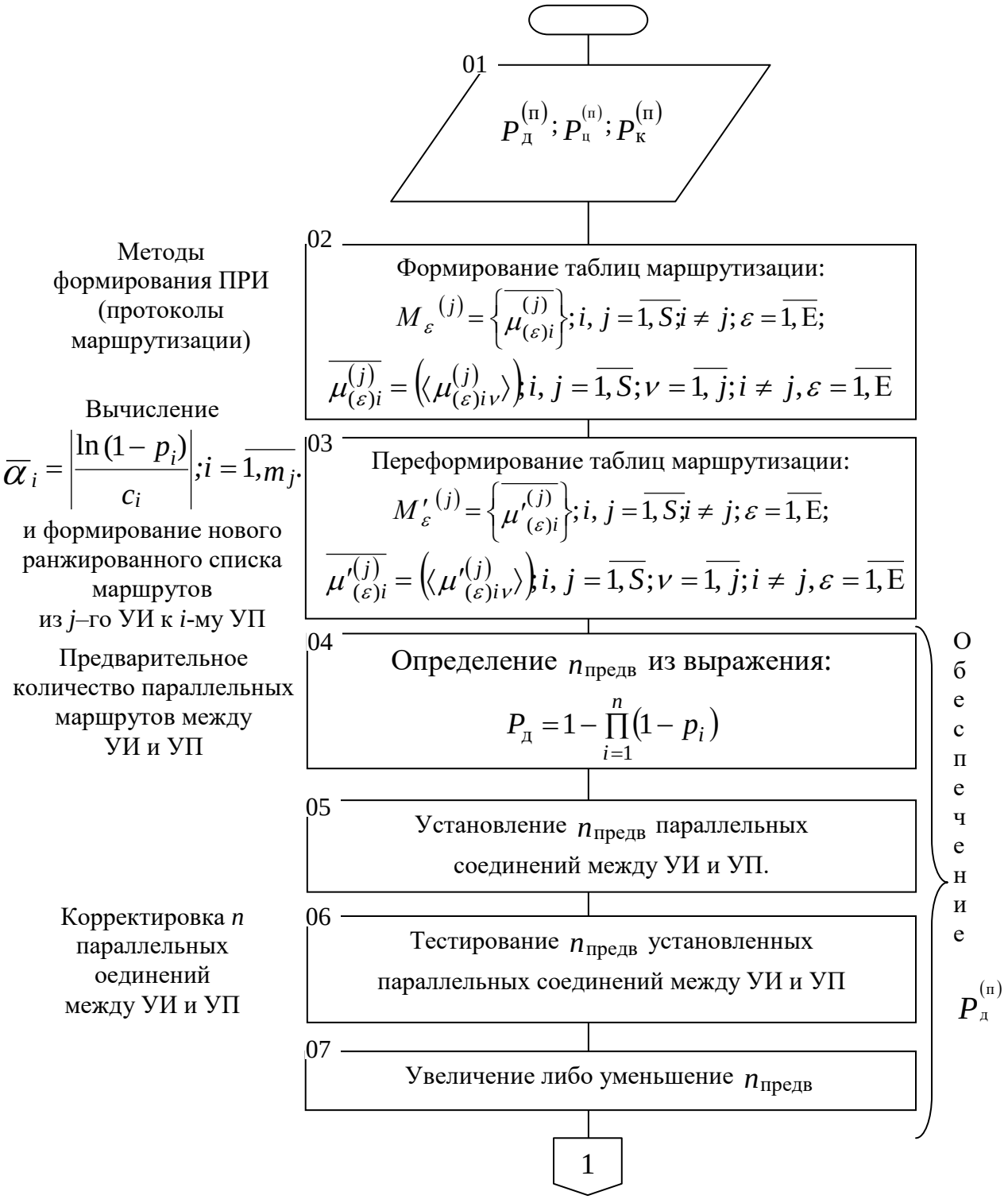


Рисунок 13 – Концепция методики обеспечения защиты информации

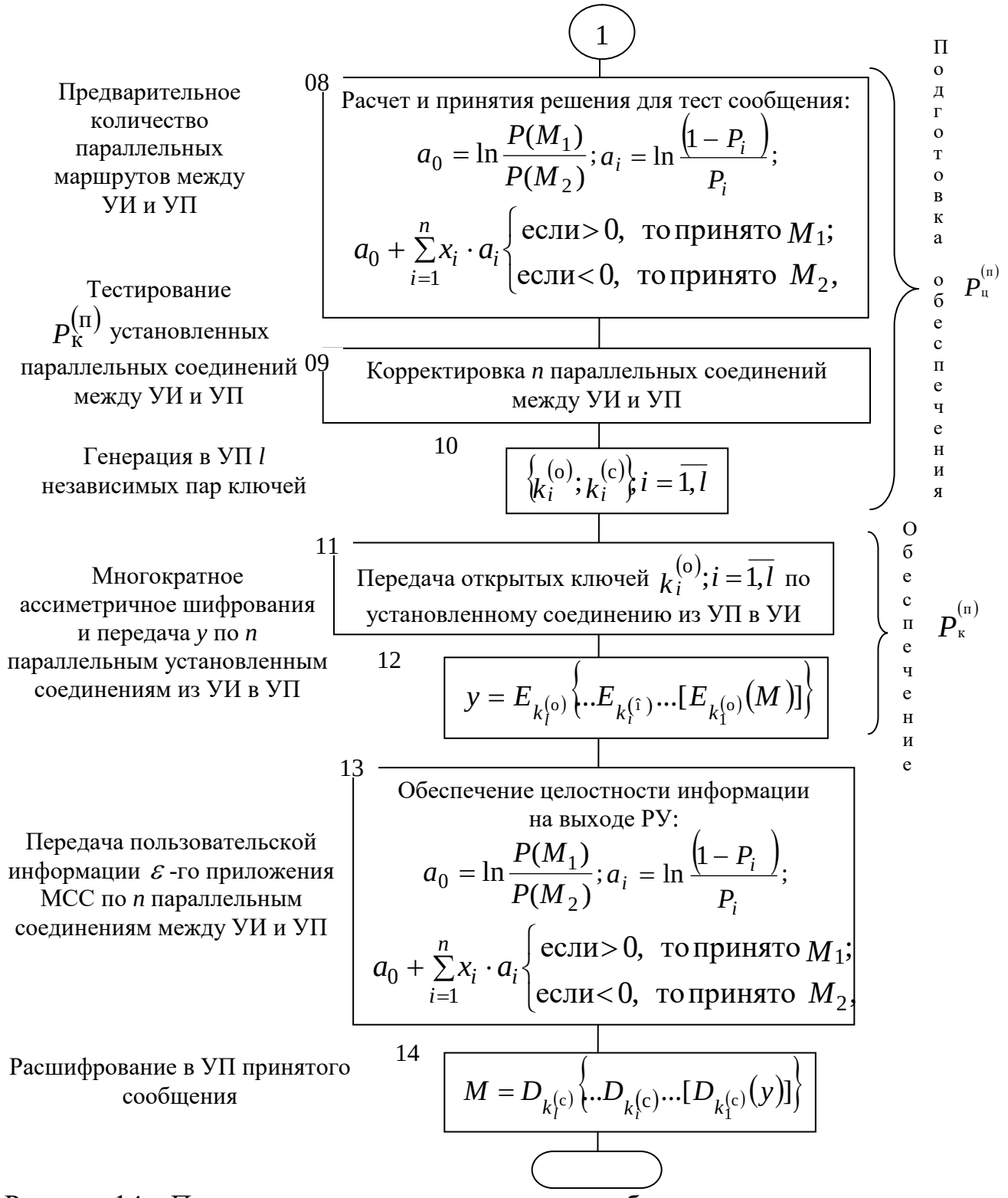


Рисунок 14 – Продолжение концепции методики обеспечения защиты информации

2. Перестановка маршрутов в новый ранжированный убывающий по предпочтительности список. Более предпочтительным является тот маршрут, у которого $\overline{\alpha}_i; i = \overline{1,m_j}$ больше.

В результате для каждого ε-го приложения МСС формируются ТМ:

$$M'^{(j)}_{\varepsilon} = \left(\overline{\mu'^{(j)}_{(\varepsilon)1}},\ldots,\overline{\mu'^{(j)}_{(\varepsilon)i}},\ldots,\overline{\mu'^{(j)}_{(\varepsilon)j-1}},\overline{\mu'^{(j)}_{(\varepsilon)j+1}},\ldots,\overline{\mu'^{(j)}_{(\varepsilon)S}}\right), \varepsilon = \overline{1,\mathrm{E}};$$

$$\overline{\mu'^{(j)}_{(\varepsilon)i}} = \left(\langle \mu'^{(j)}_{(\varepsilon)i1}\rangle,\ldots,\langle \mu'^{(j)}_{(\varepsilon)iv}\rangle,\ldots\langle \mu'^{(j)}_{(\varepsilon)im_j}\rangle\right), i,\ j = \overline{1,S}; i \neq j, \varepsilon = \overline{1,\mathrm{E}}.$$

Операторы 04 ÷ 07 определяют и устанавливают *n* параллельных соединений между УИ и УП для обеспечения доступности ($P_{\text{д}}^{(\text{п})}$) информации в МСС.

Определение количества параллельных соединений состоит из двух этапов – предварительного (операторы 04 ÷ 06) и окончательного (оператор 07).

На предварительном этапе, применяя:

$$P_{\text{д}} = 1 - \prod_{i=1}^{n}(1 - p_i),$$

определяется $n_{\text{предв}}$ (оператор 04). Далее система управления МСС, используя протоколы сигнализации, устанавливает между УИ и УП $n_{\text{предв}}$ параллельных соединений (оператор 05). Окончательное определение величины *n* состоит в:

– в тестировании установленных $n_{\text{предв}}$ соединений (оператор 06);

– корректировке *n* (увеличении либо уменьшении $n_{\text{предв}}$) (оператор 07).

Таким образом, 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 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 информации. РУ, которое расположено в УП, выполняет:

– процедуру восстановления принятого тест-сигнала по правилу:

$$a_0 + \sum_{i=1}^{n} x_i \cdot a_i \begin{cases} \text{если} > 0, & \text{то принято } M_1; \\ \text{если} < 0, & \text{то принято } M_2; \end{cases} \qquad a_0 = \ln\frac{P(M_1)}{P(M_2)};\ a_i = \ln\frac{\left(1 - P_i\right)}{P_i};$$

– сравнение принятого тест-сигнала с переданным.

В случае недостаточного значения величины $P_{\text{д}}^{(\text{п})}$ принимается решение о добавлении дополнительных параллельных соединений между УИ и УП.

По окончанию 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 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) $\{k_i^{(о)}; k_i^{(с)}\}; i=\overline{1,l}$. Далее открытые ключи $k_i^{(о)}; i=\overline{1,l}$ 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 ($P_{д}^{(п)}, P_{к}^{(п)}, P_{ц}^{(п)}$).

В УИ выполняется процедура многократно ассиметричного шифрования (оператор 12) $y = E_{k_l^{(о)}}\{..E_{k_i^{(о)}}...[E_{k_1^{(о)}}(M)]\}$. Зашифрованное сообщение y передается по n параллельным установленным соединениям из УИ в УП. Принятое в УП сообщение обрабатывается РУ (оператор 13) по правилу:

$$a_0 + \sum_{i=1}^{n} x_i \cdot a_i \begin{cases} \text{если} > 0, \ \text{то принято} \ M_1; \\ \text{если} < 0, \ \text{то принято} \ M_2; \end{cases} \quad a_0 = \ln \frac{P(M_1)}{P(M_2)}; \ a_i = \ln \frac{\left(1 - P_i\right)}{P_i}.$$

Тем самым реализуется целостность информации. Далее сообщение y расшифровывается (оператор 14) $M = D_{k_l^{(с)}}\{..D_{k_i^{(с)}}...[D_{k_1^{(с)}}(y)]\}$.

Таким образом 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.

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 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;

– методики 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;

– 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).

Полный список опубликованных автором 66 работ приведен в диссертации.

Список наиболее значимых научных работ автора по теме диссертации

Статьи в ведущих рецензируемых журналах, 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 и 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.

НОВИКОВ Сергей Николаевич

МЕТОДОЛОГИЯ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЬСКОЙ ИНФОРМАЦИИ НА ОСНОВЕ ТЕХНОЛОГИЙ СЕТЕВОГО УРОВНЯ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ

Автореферат диссертации
На соискание ученой степени доктора технических наук

Пописано в печать
Формат бумаги 62х84/16, отпечатано на ризографе, шрифт № 10,
Изд. л. ___, заказ № , тираж – 100 экз., _____.
_____