**ОТЗЫВ**

официального оппонента о диссертационной работе Новикова Сергея Николаевича «Методология защиты информации на основе технологий сетевого уровня мультисервисных сетей связи», представленной на соискание учёной степени доктора технических наук по специальности: 05.13.19 – Методы и системы защиты информации, информационная безопасность.

**Актуальность темы диссертации**

Диссертационная работа Новикова С.Н. посвящена вопросам защиты информации в мультисервисных сетях связи на сетевом уровне. При реализации мультисервисных сетей связи ставится задача предоставления гарантированного качества обслуживания и безопасности данных. Использование механизмов сетевого уровня обеспечивает широкие возможности внедрения средств защиты информации. На сегодняшний день существует ряд работ, доказывающих перспективность данного направления. Однако достаточно большой спектр задач, связанных с защитой информации на сетевом уровне в мультисервисных сетях остается не исследованным. В связи с вышеизложенным, цель диссертационной работы является актуальной.

**Общая характеристика содержания диссертации**

Диссертация состоит из введения, шести глав, заключения, списка литературы и приложений. Общее количество страниц – 235.

В первой главе осуществлен анализ современного состояния вопросов защиты информации в мультисервисных сетях связи. Отдельно рассмотрены основные подходы к обеспечению конфиденциальности, доступности и целостности информации.

Вторая глава посвящена разработке методов обеспечения конфиденциальности, доступности и целостности информации на основе ресурсов мультисервисных сетей связи. Для обеспечения конфиденциальности в диссертации предложен и протестирован метод многократного асимметричного шифрования с использованием более коротких ключей. Доступность и целостность обеспечивается формированием параллельных независимых соединений в соответствии с критерием выбора сетевых ресурсов.

В третьей главе разработана классификация методов маршрутизации, учитывающая независимые процедуры: формирование плана распределения информации, выбор исходящих линий и др. Предложены перспективные методы маршрутизации в мультисервисных сетях связи.

В четвёртой главе осуществлено моделирование маршрутизации в мультисервисных сетях связи в условиях внешних деструктивных воздействий.

Пятая глава посвящена анализу результатов моделирования деструктивного воздействия на элементы мультисервисной сети связи.

В шестой главе предложены подходы к обеспечению защиты информации на основе возможностей, предоставляемых мультисервисными сетями связи.

**Обоснованность и достоверность основных выводов и положений**

Основные положения и выводы работы являются обоснованными, они базируются на вероятностных методах моделирования компьютерных сетей, имитационном

моделировании и тестировании предложенных алгоритмов после реализации в программных комплексах.

**Публикации по теме диссертации**

Результаты диссертационной работы опубликованы в 66 научных работах, в том числе 14 статей в журналах из списка, рекомендованного ВАК. Автореферат достаточно полно отражает основное содержание диссертации.

**Новизна исследований и полученных результатов и выводов, сформулированных в диссертации**

Научная новизна результатов диссертации состоит в получении ряда новых результатов, совокупность которых дает существенный вклад в развитие методов защиты информации в мультисервисных сетях.

Из новых результатов можно выделить следующие, представляющие наибольший интерес:

1. Новая методология обеспечения конфиденциальности информации в мультисервисных сетях.
2. «Гибридный» метод маршрутизации, снижающий объем передаваемой служебной информации в условиях внешних деструктивных воздействий.
3. Инструментарий (методики, математические модели, алгоритмы, программные продукты) для анализа методов маршрутизации в условиях внешних деструктивных воздействий.

**Научная значимость полученных автором диссертации результатов**

Результаты, полученные в диссертации, вносят существенный вклад в развитие технологии защиты информации в сетях связи. Результаты могут быть использованы при проектировании, анализе и реализации защищенных мультисервисных сетей.

**Замечания по работе**

1. При исследовании возможностей многократного асимметричного шифрования в разделе 2.1 рассматриваются вопросы только уменьшения времени шифрования. Однако такая процедура может приводить к снижению стойкости криптосистемы. Более разумным было бы ввести некую целевую функцию, учитывающую два фактора – время шифрования и стойкость криптосистемы. В этом случае проблема выбора длины ключа сводится к задаче оптимизации, позволяющей получить более взвешенное решение.

2. В четвертой главе на основе математического моделирования получена система уравнений, описывающая маршрутизацию в мультисервисных сетях (стр. 104). Однако в диссертации не проведено достаточно полного исследования свойств данной системы уравнений с целью определения условия существования решений. Данное исследование может привести к новым достаточно интересным следствиям и рекомендациям по проектированию мультисервисных сетей связи.

3. В выводе 3 к главе 5 (стр. 153) утверждается, что результат анализа функционирования мультисевисной сети связи в условиях внешних деструктивных

воздействий подтвержден на различных структурах мультисервисных сетей связи. Однако в самой диссертации приведено подробное описание только одной структуры сети и эксперимента на ней (раздел 5.2). Полное описание выбора анализируемых структур сетей сделало бы этот вывод более обоснованным.

4. В главе 6 при использовании алгоритмов асимметричного шифрования (стр. 168) предлагается простая передача открытого ключа по линиям связи. Однако, как хорошо известно, такая схема не устойчива к атаке «человек посредине». Необходимо использовать более стойкие криптографические протоколы.

**Заключение**

В целом, несмотря на указанные замечания, представленная диссертация является законченной научно-квалификационной работой, которая может рассматриваться как научное достижение, состоящее в существенном вкладе в развитие технологии защиты информации в сетях связи.

Диссертация Новикова С.Н. удовлетворяет требованиям Положения ВАК, предъявляемым к докторским диссертациям, а её автор – Новиков Сергей Николаевич присуждения ему учёной степени доктора технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Заведующий кафедрой информационной
безопасности ОмГУ им. Ф.М. Достоевского,
д.ф.-м.н., профессор С.В. Белим

03.10.16

Рабочий почтовый адрес:
644077, г. Омск, пр. Мира 55а
Рабочий телефон: (3812)268422
e-mail: belimsv@omsu.ru

Подпись работника Белим С.В.
Ученый секретарь Ученого совета
университета Л.И.Ковалевская