

ОТЗЫВ

на автореферат диссертации Новикова Сергея Николаевича: «Методология защиты информации на основе технологий сетевого уровня мультисервисных сетей связи», представленной на соискание ученой степени доктора технических наук по специальностям: 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Известно, что обеспечение конфиденциальности информации в мобильных сетях за счет механизмов сетевого уровня модели взаимосвязи открытых систем (МВОС) всегда являлась приоритетным направлением для проектировщиков корпоративных сетевых структур различного назначения, особенно при резком возрастании масштабов сетевой структуры, например в военной области. Однако сложность решения этой проблемы обусловлена в предоставлении услуг по защите информации в реальном масштабе времени, что неизбежно приводит к финансовым, организационным и техническим издержкам. Поэтому работа Новикова С.Н., посвященная созданию методологической основы, применения технологий сетевого уровня мультисервисных сетей связи (МСС) для защиты информации является актуальной.

Автором разработаны методология, методы, инструментарий обеспечения конфиденциальности, целостности и доступности информации на базе протоколов сетевого уровня и исследованы их влияние на качество обслуживания приложений в условиях деструктивных воздействий.

Новизна работы заключается в разработке методов и алгоритмов многократного асимметричного шифрования с использованием параллельных методов маршрутизации на основе плана распределения информации для выбора исходящих трактов, для защиты которых от деструктивных воздействий используется «гибридная» маршрутизация, а также разработаны методики и математические модели позволяющие выявить наиболее эффективно функционирующие методы маршрутизации, при этом разработан оригинальный способ проверки графа на связность, уменьшающий алгоритмическую сложность решения задачи.

Практическая значимость работы заключается в разработке методов моделей и алгоритмов, позволяющих обеспечить конфиденциальность информации при меньшем времени ее шифрования, в повышении надежности функционирования МСС в условиях деструктивных воздействий.

В качестве недостатков следует отметить, что из автореферата неясно:

1. Каким образом вычисляются необходимое количество асимметричных шифрований и как это влияет на криптостойкость зашифрованных текстов;
2. Каким образом выбирается количество параллельных соединений, чтобы обеспечить заданную целостность информации;
3. Почему модель плана распределения информации на объем сетевых ресурсов выбрана в виде полинома и как определяется степень недоступности средних сетевых ресурсов.

Однако указанные недостатки не влияют на полученные автором результаты. Проведенное исследование соответствует требованиям Положения ВАК России, предъявляемым к докторским диссертациям. Автор диссертационной работы Новиков Сергей Николаевич заслуживает присвоения ученой степени доктора технических наук по специальностям: 05.13.19 – Методы и системы защиты информации, информационная безопасность,

350063, г. Краснодар, ул. Красина, д.4, тел. 8(861) 268-35-09, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко.

Профессор кафедры (математических основ криптологии и криптографической защиты информации)

доктор технических наук, профессор,
почетный работник высшего профессионального
образования Российской Федерации,
академик РАЕН



Ф.Г. Хисамов

Подпись профессора Хисамова Ф.Г. заверяю
начальник отдела кадров

144 1

Н. Енин