ОТЗЫВ

на автореферат диссертации Метлинова Александра Дмитриевича на тему «Модели и алгоритмы повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*», представленной на соискание ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Целью представленной диссертации является повышение криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*. Это, безусловно, задача актуальная, которая, кроме теоретического, имеет явную практическую направленность в вопросах обеспечения безопасности каналов связи и телекоммуникационных систем и сетей в общем.

В соответствии с авторефератом, следующие результаты обладают научной новизной:

1. Разработаны математические модели рюкзачной системы защиты канала связи, отличающаяся наличием общей памяти между узлом-отправителем и узлом-получателем, высоким уровнем плотности укладки рюкзака, использованием линейно-рекуррентных последовательностей, позволяющие повысить криптостойкость и производительность канала связи.

2. Модифицирован протокол *TLS* путем введения в структуру данных полей для хранения общей памяти, а также добавления модулей шифрования и дешифрования, реализующих рюкзачную систему защиты, что позволяет повысить его (протокола) функциональные свойства.

3. Разработаны алгоритмы передачи и приема сообщений в защищенном канале связи в телекоммуникационных сетях *TCP/IP*, построенном на базе рюкзачной системы защиты с общей памятью.

4. Практически реализовано семейство алгоритмов (шифрования, дешифрования и хеширования информации) для повышения быстродействия и криптостойкости симметричных рюкзачных криптосистем в защищенных каналах связи сетей *TCP/IP*. Внедрение этих приложений на предприятия позволило практически до нуля сократить количество инцидентов по несанкционированному доступу к информации, составляющей их коммерческую тайну и значительно сократить расходы по защите информации на предприятиях.

Достоинством работы является ее практическая направленность. На основе предложенных моделей и алгоритмов разработано информационное и программное

обеспечение комплекса алгоритмов симметричной рюкзачной криптосистемы с ОП, включающее: программный комплекс *CBC*-блочной симметричной рюкзачной криптологи-ческой системы для вариации с плотностью укладки больше единицы при величине рюкзачного базиса 128 бит; программный тестовый комплекс для симметричной рюкзачной криптосистемы; программный модуль генератора общей памяти для симметричной рюкзачной криптосистемы.

На основе изучения материалов автореферата возникло замечание по существу работы: не совсем понятно, какой из режимов сцепления блоков применялся автором при проектировании защищенного канала связи на основе модификации протокола *TLS* и экспериментальном исследовании.

В целом диссертация представляет собой законченную работу, имеющую как теоретическую, так и практическую ценность в вопросах обеспечения безопасности каналов связи и телекоммуникационных систем и сетей в общем. Предложены модели и алгоритмы, отвечающие критерию научной новизны. Результаты диссертации опубликованы в центральной печати, прошли апробацию на научно-технических конференциях, внедрены в ряде предприятий.

Работа в целом удовлетворяет требованиям ВАК, предъявляемым к кандидатским диссертациям. Метлинов А.Д. заслуживает присвоения ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Груздева Людмила Михайловна, кандидат технических наук (05.12.13 – Системы, сети и устройства телекоммуникаций), доцент кафедры «Информационно-математические технологии и информационное право» федерального государственного бюджетного образовательного учреждения высшего образования «Российский университет транспорта (МИИТ)»,
адрес: 127994, г. Москва, ул. Образцова, д 9, стр. 9
тел.: 8 (495) 684-29-37
дата: 18.04.2018г.

Л.М. Груздева

Подпись руки Груздевой Л.М.
Заверяю
Начальник Отраслевого центра подготовки научно – педагогических кадров высшей квалификации С.Н. Коржин