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".

Диссертация Метлинова А.Д. посвящена теоретическим и прикладным аспектам повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*, а также повышению безопасности телекоммуникационных сетей в целом.

По мере развития и усложнения моделей, алгоритмов и средств обработки и передачи информации в защищенных каналах связи телекоммуникационных сетей *TCP/IP* повышается уязвимость существующих протоколов безопасности каналов связи, напрямую влияющая на возможность несанкционированного копирования, уничтожения, блокирования или искажения информации. Основные причины возникновения угроз безопасности каналов связи – их низкая криптостойкость, сами каналы связи сетей *TCP/IP* не имеют встроенных средств защиты, существующие механизмы обеспечения информационной безопасности реализованы на сеансовом уровне модели *OSI* и имеют множество уязвимостей.

В связи с выше изложенным решение задачи повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях имеет научное и практическое значения.

В диссертации автором получены следующие результаты: разработаны математические модели рюкзачной системы защиты канала связи, отличающиеся, в частности, наличием общей памяти между узлом-отправителем и узлом-получателем и использованием линейно-рекуррентных последовательностей, позволяющие повысить криптостойкость и производительность канала связи; модифицирован протокол *TLS* путем введения в структуру данных полей для хранения общей памяти, а также добавления модулей шифрования и дешифрования, [illegible] этого протокола; разработаны алгоритмы передачи и приема сообщений в защищенном канале связи в телекоммуникационных сетях *TCP/IP*, построенном на основе рюкзачной системы защиты с общей памятью.

В качестве **замечания** следует отметить следующее: из текста автореферата не ясно, включена ли в алгоритмы шифрования и дешифрования модифицированной симметричной "рюкзачной" криптосистемы с общей памятью функция выравнивания по размеру ключа или шифруемого блока.

В целом считаю, что работа выполнена на высоком научно-техническом уровне, имеет практическую ценность и удовлетворяет всем требованиям ВАК РФ, предъявляемым к кандидатским диссертациям.

Работа может быть представлена к защите, а Метлинов А.Д. достоин присуждения ученой степени кандидата технических наук по специальности 05.12.13 – “Системы, сети и устройства телекоммуникаций”.

РЕЦЕНЗЕНТ

Д.т.н., профессор Александров Дмитрий Владимирович, профессор кафедры ИБМ-7 “Инновационное предпринимательство”

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)»

Адрес: 105005 Москва, 2-я Бауманская ул., д. 5, стр. 1
Тел.: +7(977)800-39-59; e-mail: dmalex-m2@yandex.ru

Специальность: 05.13.01 “Системный анализ, управление и обработка информации (промышленность)”

Подпись д.т.н., профессора Александрова Дмитрия Владимировича заверяю:

8.05.2018 г.

А Г. МАТВЕЕВ
ЗАМ. НАЧ. УПРАВЛЕНИЯ КАДРОВ
ТЕЛ. 8499-263 67 69