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.

Даже после внедрения защитных мер и средств в каналы связи телекоммуникационных сетей *TCP/IP* предприятия всегда остаются их уязвимые места, которые могут сделать обеспечение его информационной безопасности неэффективным. Кроме того, всегда могут появляться новые, ранее не идентифицированные уязвимые места. 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.

Предлагаемая автором диссертационная работа представляет собой комплекс научных и практических решений задачи разработки новых моделей и алгоритмов повышения криптостойкости и производительности защищенного канала связи на базе симметричной рюкзачной криптографической системы в сетях *TCP/IP* для повышения эффективности обеспечения информационной безопасности в каналах связи, системах и сетях телекоммуникаций предприятий.

Выделю следующие положения научной новизны диссертационной работы:

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.

Практическая значимость работы заключается в разработке информационного и программного обеспечения комплекса алгоритмов симметричной рюкзачной криптосистемы с общей памятью. Внедренные актуальные версии на предприятиях данного программного

комплекса показали, что разработки автора позволяют безопасно хранить данные предприятия, составляющие коммерческую тайну, а также безопасно их передавать между подразделениями, снизить материальные затраты на активные средства по защите и т.п.

Результаты исследований апробированы на международных и всероссийских конференциях и, судя по публикациям, имеют достаточно общий характер, что позволяет распространить их на широкий круг различных каналов связи телекоммуникационных сетей *TCP/IP* предприятий.

Замечание: По тексту автореферата не понятен тот факт, зависит ли (рис.4 и рис.5) выигрыш в скорости от статистических характеристик (размера) или типа файла.

Несмотря на замечание, диссертационное исследование «Модели и алгоритмы повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*», представляет собой самостоятельно выполненное, законченное исследование по решению актуальной научной задачи, соответствует требованиям ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций, а ее автор Метлинов Александр Дмитриевич заслуживает присуждения ученой степени кандидата технических наук.

Рецензент:
Доцент кафедры физики
Факультет авиационных систем и
комплексов, Московского технического
университета гражданской авиации
(МГТУ ГА),
канд.ф.- м. наук Скоробогатова Т.В.
10.05.2018.

Подпись доцента Скоробогатовой Т.В.
заверяю:

Ученый секретарь Ученого совета
Федерального государственного
бюджетного образовательного
учреждения высшего образования
«Московский государственный
технический университет
гражданской авиации» (МГТУ ГА) Манолова О.Н.