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.

Прогресс в области применения различных информационных технологий в управлении современными предприятиями, обусловленный развитием вычислительных систем и программных средств, сопровождается повышением требований к безопасности и стабильности функционирования каналов связи телекоммуникационных сетей *TCP/IP* и устойчивости при попытках нарушения их информационной безопасности.

Диссертационное исследование посвящено изучению методологических аспектов актуальной проблемы повышения эффективности обеспечения информационной безопасности в каналах связи систем и сетей телекоммуникаций предприятий. Основные угрозы информационной безопасности направлены на перехват и имперсонацию сообщений (нарушение конфиденциальности и целостности передаваемых данных), нередки атаки на доступность узлов канала и их подмену. Каналы связи сетей *TCP/IP* не имеют встроенных средств защиты, существующие механизмы обеспечения информационной безопасности реализованы на сеансовом уровне сетевой модели *OSI* и имеют множество уязвимостей.

Внезапная успешная атака на канал связи или возникновение неизвестной ранее ситуации, которая может иметь отношение к информационной безопасности и сопряженное с этим нарушение требуемого функционирования телекоммуникационной сети могут нанести предприятию значительный материальный ущерб.

В силу этого тема диссертационной работы, затрагивающей проблему разработки новых моделей и алгоритмов повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*, является актуальной и имеет научную и практическую значимость.

Исходя из цели работы, автором формируется комплекс задач, предлагаются способы и методики их решения, даются научные выводы и рекомендации. Основные результаты исследования, имеющие научную и практическую ценность:

- разработаны математические модели рюкзачной системы защиты канала связи, отличающаяся наличием общей памяти, высоким уровнем плотности укладки рюкзака, использованием линейно-рекуррентных последовательностей;

- 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;

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

Замечания по автореферату:

1. Из текста автореферата не понятен тот факт, зависит ли криптостойкость и производительность протокола *TLS* от режима сцепления блоков.

2. Из содержания автореферата не понятно, как зависит криптостойкость протокола *TLS* от качества ГПСЧ, задающего вектор *E*.

Заключение:

1. Диссертационное исследование «Модели и алгоритмы повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*» является законченным, апробированным по решению актуальной научной задачи.

2. Работа соответствует требованиям ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций. Метлинов Александр Дмитриевич достоин присуждения ученой степени кандидата технических наук.

профессор кафедры
«Математики и информатики»
Московского университета
им. С.Ю. Витте (МУиВ),
к.ф.-м.н

Крисько О. В.

Подпись заверяю
Нач. отд. кадров МУиВ
ПОДПИСЬ

Тынянская Л. И.
Специалист
Службы персонала

ПЕЧАТЬ организации

7.05.2018 г.