УТВЕРЖДАЮ
Проректор по научной работе
федерального государственного
образовательного учреждения
высшего образования «Омский
государственный технический
университет» (ОмГТУ)
к.т.н., доцент
Б.Д. Женатов
«___» _____ 2018 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертацию и 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.

Актуальность темы диссертационной работы

В настоящее время невозможно представить жизнь современного общества без повсеместного применения информационных технологий. Сегодня компьютерные каналы связи, системы и сети телекоммуникаций, реализуют современные информационные технологии, обеспечивая хранение информации, ее обработку, доставку и представление потребителям. Уровень технологического развития перечисленных каналов и их защищенность во многом определяют степень информатизации экономики страны, ее место в протекающих мировых информационных процессах, престиж страны, ее готовность противостоять вызовам в области обороны и безопасности.

Диссертационная работа посвящена ***актуальной в теоретическом и практическом плане*** проблеме информационной безопасности и защиты информации в каналах связи систем и сетей телекоммуникаций. Применение новых информационных и телекоммуникационных технологий, а также различного программного обеспечения в каналах связи телекоммуникационных сетей *TCP/IP* порождает новые вызовы информационной безопасности.

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. Каналы связи сетей *TCP/IP* не имеют встроенных средств защиты, существующие механизмы обеспечения информационной безопасности реализованы на сеансовом уровне *OSI* и имеют множество уязвимостей.

Несанкционированный доступ каналам связи, а, следовательно, к информационным ресурсам предприятия, блокирование его средств телекоммуникаций или их несанкционированное использование могут в результате нанести предприятию значительный материальный ущерб, вплоть до остановки его производства. Перечисленные инциденты информационной безопасности также негативно влияют на имидж организации, что может значительно сказаться на доверии клиентов, вплоть до сокращения клиентской базы предприятия.

Широкомасштабная стандартизация и унификация средств вычислительной техники, телекоммуникаций и программного обеспечения в значительной степени расширяют возможности несанкционированного воздействия на каналах связи телекоммуникационных сетей *TCP/IP*.

Таким образом, исследования, направленные на разработку новых моделей и алгоритмов повышения криптостойкости и производительности защищенного канала связи на базе симметричной рюкзачной криптографической системы в сетях *TCP/IP*, ***актуальны и имеют практическое значение*** в решении проблемы обеспечения информационной безопасности сетей телекоммуникаций предприятий.

Новизна исследования и полученных результатов, выводов и рекомендаций, сформулированных в диссертации:

Диссертация состоит из введения, четырех глав, заключения, списка использованных источников, списка сокращений, списка обозначений и приложений. Содержание диссертации изложено в логически последовательной форме. Стиль изложения в целом четкий и ясный. Диссертация оформлена в соответствии с требованиями ВАК.

Анализ диссертационной работы, автореферата и научных трудов автора позволил сделать вывод о том, что научная новизна диссертационной работы обоснована и в ней получены автором лично или при его непосредственном участии следующие результаты.

- 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.

- 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.

Положения, выносимые на защиту:

- математические модели рюкзачной системы защиты канала связи;

- модификация протокола *TLS*;

- алгоритмы передачи и приема сообщений в защищенном канале связи в телекоммуникационных сетях *TCP/IP*;

- результаты экспериментального исследования и внедрения предложенных моделей и алгоритмов.

Обоснованность и достоверность научных положений, основных выводов и результатов диссертации обеспечивается за счет анализа состояний исследования в данной области, согласованности теоретических выводов с результатами экспериментальных исследований. Достоверность практических результатов достигается за счет большого количества экспериментов при решении задач и использования собственного и стандартного программного обеспечения. Теоретической основой для данной диссертационной работы послужили фундаментальные работы отечественных и зарубежных ученых в области информационной безопасности и защиты информации в системах и сетях телекоммуникаций.

Основные результаты работы, полученные автором, прошли апробацию на международных и всероссийских научных конференциях. Достоверность научных положений, выводов и практических рекомендаций, полученных в диссертационной работе, подтверждается корректным обоснованием постановок задач, точной формулировкой, результатами экспериментальных исследований, а также их внедрением на практике.

Значимость для науки и практики результатов, полученных автором диссертации:

Основным научным достижением автора является разработка новых моделей и алгоритмов повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*. Полученные научные результаты вносят существенный вклад в развитие механизмов обеспечения информационной безопасности систем и сетей телекоммуникаций.

Сделанные теоретические выводы подтверждены экспериментальной проверкой с использованием разработанных программных средств в процессе диссертационного исследования. Результаты исследований внедрены в ООО «Русский мастер», Владимирская область, поселок Льнозавод; в ООО «ДИВАНиЯ», Владимирская область, поселок Льнозавод, а также в ИП Щерба А.Ю., город Владимир. Теоретические и практические результаты диссертационной работы получили поддержку грантов Фонда содействия инновациям и РФФИ.

Замечания по диссертационной работе:

- В первой главе автором для повышения криптостойкости и производительности протокола *TLS* предлагается использовать [стр. 25] *CBC*-блочный вариант симметричной рюкзачной криптосистемы с общей памятью. Не указано какой именно режим сцепления блоков используется и зависит ли криптостойкость и производительность протокола *TLS* от режима сцепления блоков?

- Что имеется ввиду автором под «жадным алгоритмом» и какова его алгоритмическая сложность?

- Каким образом автором получается значение вероятности успешной реализации L^3-атаки в спроектированной криптосистеме [формула 3.1, стр. 60] при вычислении величины криптостойкости?

- В схемах работы алгоритмов приема и передачи сообщений, шифрования и дешифрования информации на основе предложенной модификации протокола *TLS* [стр. 42-49] не дана оценка сложности работы всех алгоритмов, а также не приведена оценка скорости работы алгоритмов приема и передачи сообщений, в то время как оценка скорости работы алгоритмов шифрования и дешифрования информации в канале связи присутствует.

Заключение и выводы:

Диссертация представляет собой законченную научно - исследовательскую работу на актуальную тему. Выполненные исследования и полученные результаты развивают методику обеспечения информационной безопасности каналов связи, систем и сетей телекоммуникаций. Название диссертации, автореферат и публикации в полной мере отражают содержание работы.

Диссертационная работа «Модели и алгоритмы повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*» соответствует паспорту научной специальности 05.12.13 – Системы, сети и устройства телекоммуникаций, именно п.5 и п.10, а также «Положению о присуждении ученых степеней», утвержденному постановление Правительства Российской Федерации от 24 сентября 2013 г. №842. Диссертация Метлинова

Александра Дмитриевича «Модели и алгоритмы повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*» рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций. Ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Отзыв утвержден на плановом заседании кафедры «Комплексная защита информации» Федерального государственного бюджетного образовательного учреждения высшего образования «Омский государственный технический университет». Протокол заседания № 6 от «17» апреля 2018 года.

Отзыв составил:

Заведующий кафедрой
«Комплексная защита информации»,
кандидат технических наук, доцент, ОмГТУ П.С. Ложников

Наименование организации в соответствии с уставом: федеральное государственное бюджетное образовательное учреждение высшего образования «Омский государственный технический университет» (ОмГТУ).
Адрес: 644050, Сибирский федеральный округ, Омская область, г. Омск, Пр. Мира, д.11
Тел.: (3812) 65-34-07, (3812) 62-87-07,
Адрес эл. почты: info@omgtu.ru