УТВЕРЖДАЮ
Первый проректор,
проректор по НиИР ВлГУ
д.ф-м.н., профессор
_____ В.Г. Прокошев
«__» _____ 2018 года

ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (ВлГУ), Министерство образования и науки Российской Федерации

Диссертация Метлинова Александра Дмитриевича «Модели и алгоритмы повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*» выполнена на кафедре «Информатика и защита информации» института информационных технологий и радиоэлектроники, ВлГУ.

В период подготовки диссертации Метлинов Александр Дмитриевич являлся аспирантом очной формы обучения кафедры «Информатика и защита информации» Федерального государственного бюджетного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» с 2013 по 2017 год. В 2017 году окончил аспирантуру с предоставлением диссертации на кафедру. В настоящее время является главным специалистом по защите информации на частном коммерческом предприятии «Дивания» (Владимирская область, поселок Льнозавод).

В 2013 году Метлинов Александр Дмитриевич с отличием окончил ВлГУ по специальности «Комплексная защита объектов информатизации».

Метлинов Александр Дмитриевич сдал все кандидатские экзамены в ВлГУ: история и философия науки – отлично; иностранный язык – отлично; специальная дисциплина 05.12.13 – Системы, сети и устройства телекоммуникаций – отлично.

Научный руководитель - Монахов Михаил Юрьевич, доктор технических наук, профессор, заведующий кафедрой «Информатика и защита информации» Федерального государственного бюджетного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых».

По итогам обсуждения на кафедральном заседании принято следующее заключение:

Оценка выполненной автором диссертационной работы

Диссертационная работа посвящена актуальной в теоретическом и практическом плане теме проблемы информационной безопасности и защиты информации в системах и сетях телекоммуникаций.

В данной работе показано, что 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. По итогам анализа сделан вывод, что 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.

В диссертационной работе разработано семейство алгоритмов симметричных рюкзачных криптосистем, которые отличаются наличием общей памяти между

узлом-отправителем и узлом-получателем, высоким уровнем плотности укладки рюкзака, а также отказом от супервозрастающих базисов в пользу линейно - рекуррентных последовательностей. Предложена модификация симметричной рюкзачной криптосистемы с общей памятью семейством *CBC*-блочных алгоритмов шифрования и дешифрования информации, что еще в большей мере повышает криптостойкость. Экспериментально выявлено, что между вероятностью успешной реализации L^3-атаки и плотностью укладки рюкзака при различных объемах исходного текста есть сильная статистическая зависимость. Показано, что внедрение разработанной криптосистемы в фазы работы стандартного протокола *TLS* (аутентификации клиента и сервера, создания кода аутентификации сообщений и работы симметричных блочных алгоритмов шифрования и дешифрования сообщений) позволяет существенно повысить эффективность защищенного КС сетей *TCP/IP*.

Личное участие автора в получении результатов, изложенных в диссертационной работе

Все результаты, изложенные в диссертации, получены автором лично или при его непосредственном участии. Постановка цели и задач, обсуждение планов исследований и результатов выполнены совместно с научным руководителем.

Разработанные Метлиновым А.Д. теоретические положения, а также результаты практического исследования являются плодами самостоятельного исследования и вносят вклад в решение актуальных вопросов проблемы информационной безопасности и защиты информации в системах и сетях телекоммуникаций.

Степень достоверности результатов проведенных исследований

Основные результаты, полученные в диссертационной работе, являются обоснованными либо на доказательном, либо на экспериментальном уровне. 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.

Новизна и практическая значимость результатов исследования

Научная новизна заключается в следующем:

- 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.

Практическая значимость диссертационной работы Метлинова А.Д. состоит в разработке информационного и программного обеспечения комплекса алгоритмов симметричной рюкзачной криптосистемы с общей памятью, включающего: программный комплекс *CBC*-блочной симметричной рюкзачной криптологической системы для вариации с плотностью укладки больше единицы при величине рюкзачного базиса 128 бит (свидетельство о гос. регистрации программы для ЭВМ №2014614981); программный тестовый комплекс для симметричной рюкзачной криптосистемы (свидетельство №2014614937); программный модуль генератора общей памяти для симметричной рюкзачной криптосистемы (свидетельство №2015616165), а также во внедрении разработанной криптосистемы в фазы работы стандартного протокола *TLS* (аутентификации клиента и сервера, создания кода аутентификации сообщений и работы симметричных блочных алгоритмов шифрования и дешифрования сообщений), позволяющее повысить эффективность защищенного канала связи сетей *TCP/IP*.

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 фондов УМНИК и РФФИ, в дальнейшем могут использоваться в учебном процессе и совершенствовании симметричных рюкзачных криптосистем.

Ценность научных работ автора

Ценность научных работ Метлинова А.Д. состоит в том, что в них отражены обоснование и особенности проектирования защищенного канала связи на базе симметричной рюкзачной криптосистемы с плотностью укладки больше единицы. Приведен обзор существующих на сегодняшний день подходов к построению рюкзачных каналов связи телекоммуникационных систем, а также криптосистем и причин их уязвимостей. На основе протоколов с общей памятью предложена схема шифрования, использующая разложение числа в фибоначчиевых базисах и их обобщениях. Изучены статистические свойства симметричной рюкзачной криптосистемы. Спроектированы алгоритмы шифрования и дешифрования для полученной криптосистемы. Показаны особенности защищенного канала связи в телекоммуникационных сетях на основе модификации протокола *TLS* с помощью модели рюкзачной криптосистемы с общей памятью. Предложено в дополнение к существующим криптоалгоритмам использовать на всех этапах работы протокола *TLS* алгоритмы симметричной рюкзачной криптографии, *CBC*-блочного варианта симметричной рюкзачной криптосистемы и хеш-функции на его основе.

Полнота изложения материалов диссертации в работах, опубликованных автором

Все основные положения и результаты диссертационного исследования отражены в 14 работах, в том числе в 4 статьях, опубликованных в ведущих рецензируемых журналах, рекомендованных ВАК для публикации результатов научных исследований.

Соответствие содержания диссертации избранной специальности

Диссертация Метлинова Александра Дмитриевича «Модели и алгоритмы

повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*» по своему содержанию соответствует профилю специальности 05.12.13 – Системы, сети и устройства телекоммуникаций, пункту 5: Развитие и разработка новых методов дифференцированного доступа абонентов к ресурсам сетей, систем и устройств телекоммуникаций и пункту 10: Исследование и разработка новых методов защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций.

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.

Заключение принято на плановом заседании кафедры «Информатика и защита информации». Дата заседания кафедры 12.02.2018 года. Протокол заседания №6. Присутствовало на заседании – 13 человек: зав. каф., д.т.н., профессор Монахов М.Ю., к.т.н., доц. Монахов Ю.М., к.ф-м.н., доц. Александров А.В., к.п.н., доц. Артюшина Л.А., к.т.н., доц. Воронин А.А., к.т.н., доц. Таннинг Ж.Ф., к.п.н., доц. Троицкая Е.А., к.т.н., доц. Тельный А.В., к.т.н., доц. Полянский Д.А., к.т.н., доц. Мишин Д.В., доц. Спирина Т.В., к.т.н., ст. пр. Монахова М.М., тех. Яковлева Е.И.

Заведующий кафедрой «Информатика и защита информации»,
доктор технических наук, профессор, Федеральное
государственное бюджетное образовательное учреждение
высшего образования «Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»,
600000, г. Владимир, ул. Горького, 87, корпус 2, аудитория 406,
mmonakhov@vlsu.ru, +7 (4922) 479-746
12.02.2018 М.Ю. Монахов

Подпись зав. кафедрой, д.т.н.,
профессора Монахова М.Ю. заверяю:

12.02.2018
ЗАВЕРЯЮ
УЧЕНЫЙ СЕКРЕТАРЬ ВлГУ
КОПЫЛОВА Т. Г.