ОТЗЫВ

официального оппонента ведущего научного сотрудника управления АСУ и связи Межрегионального общественного учредения «Институт инженерной физики» доктора технических ннаук, профессора Шиманова Сергея Николаевича на диссертацию и автореферат диссертации Метлинова Александра Дмитриевича, выполненной 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.

Проблема информационной безопасности и защиты информации в каналах связи, системах и сетях телекоммуникаций продолжает оставаться одной из центральных как в отечественной науке и промышленности, так и за рубежом. 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 канала связи, напрямую влияющая на возможность несанкционированного копирования, уничтожения, блокирования или искажения информации. Основные угрозы информационной безопасности направлены на перехват и имперсонацию сообщений, 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 *OSI* и имеют множество уязвимостей.

В связи с выше изложенным, диссертационная работа Метлинова А.Д., направленная на разработку новых моделей и алгоритмов повышения криптостойкости и производительности защищённого соединения на базе

симметричной ранцевой (рюкзачной) криптографической системы в сетях TCP/IP, является несомненно актуальной в научном плане и востребованной в практике.

Задачами, решаемыми в диссертационной работе, являются:

- анализ методов и средств обеспечения информационной безопасности и защиты информации в каналах связи телекоммуникационных сетей *TCP/IP*, выявление особенностей организации защищенного канала связи при помощи криптографического протокола *TLS*;

- разработка семейства моделей и алгоритмов повышения производительности и криптостойкости симметричных рюкзачных криптосистем в защищенных каналах связи сетей *TCP/IP*;

- модификация моделей симметричных рюкзачных криптосистем в защищенных каналах связи сетей *TCP/IP* семейством *CBC*-блочных алгоритмов шифрования и дешифрования информации;

- экспериментальное исследование предложенных средств и внедрение результатов работы.

В ходе проведения исследований по теме диссертационной работы автором получен ряд результатов, обладающих научной новизной, практической значимостью и выдвигаемых на защиту:

1. Разработаны математические модели и алгоритмы рюкзачной системы защиты, отличающейся от известных 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.

2. Предложена модификация симметричной рюкзачной криптосистемы с общей памятью семейством *CBC*-блочных алгоритмов шифрования и дешифрования информации, что еще в большей мере повышает криптостойкость.

3. Экспериментально выявлено, что между вероятностью успешной реализации L^3-атаки и плотностью укладки рюкзака при различных объемах исходного текста есть сильная статистическая зависимость (значение $|R| \sim 0.90$).

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 повысить эффективность защищенного канала связи сетей *TCP/IP*.

4. Практически реализовано семейство алгоритмов (шифрования, дешифрования и хеширования информации) для повышения быстродействия и криптостойкости симметричных рюкзачных криптосистем в защищенных каналах связи сетей *TCP/IP*.

Внедрение этих приложений на ряде предприятий позволило практически до нуля сократить количество инцидентов по несанкционированному доступу к информации, составляющей их коммерческую тайну и значительно сократить расходы по защите информации на предприятиях.

Основные результаты диссертации являются достоверными, что обусловлено корректностью постановки задач исследования, подтверждается с помощью исследований канала связи телекоммуникационных сетей *TCP/IP*, выполненных на экспериментальной установке, а также в ходе практического использования разработанных средств.

Научная новизна полученных в диссертации результатов заключается в развитии методологии обеспечения информационной безопасности и защиты информации в системах и сетях телекоммуникаций. Содержание основных положений и результаты диссертации докладывались на международных и всероссийских научно-технических конференциях.

Практическая значимость диссертационного исследования обусловлена разработкой информационного и программного обеспечения комплекса алгоритмов симметричной рюкзачной криптосистемы с общей памятью, включающее: 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). Особого внимания заслуживает, проведённое автором всестороннее тестирование криптостойкости и производительности разработанных алгоритмов и реализующих их программ на реальных TCP/IP соединениях.

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.

Замечания и недостатки:

1. К сожалению ни в диссертационной работе, ни в автореферате не сформулирована в общем виде решаемая научная задача.

2. В первой главе диссертации из схемы работы стандартной реализации протокола *TLS* [рисунок 1.5, стр. 23] не совсем ясно какую именно уязвимость данного протокола имеет ввиду автор.

3. В приведенной структуре данных, взятой автором реализации протокола *TLS*, среди прочего содержится флаг для поточного режима работы протокола. Как поведет себя протокол, с предложенной блочной модификацией, если будет выбран этот флаг?

4. В работе в явном виде не приведены оценки оперативности процедуры формирования общей памяти между узлом-отправителем и узлом-получателем [шаг 2 алгоритма стр. 45] и трудоёмкости [шага 5 алгоритма стр.45]. Как эти значения могут сказаться на результатах скоростного тестирования [п.п. 3.3 стр.78]?

5. Почему из результатов *NIST*-тестирования [таблица 3.6, стр. 76], а именно из полученной схожести результатов работы спроектированного канала связи на основе симметричной рюкзачной криптосистемы с общей памятью со случайной последовательностью делается утверждение о высоком уровне криптостойкости?

6. Автор работы не указал причины, по которым так значительно снизилось время аутентификации пользователей при внедрении нового комплекса программного обеспечения на одном из предприятий Владимирской области.

7. Имеют место редакционные неточности. Так значения графиков по оси ординат не соответствуют значениям, по которым они построены [рис. 3.2-3.4, табл.

3.2-3.4, стр.62-65]. В блок схемах [рис. 2.8, 2.9 стр. 52,53] вместо операции сложения по модулю два указано обычное сложение.

В целом, однако, отмеченные недостатки не носят принципиального характера и не наносят существенного ущерба значимости результатам диссертационной работы, выполненной на высоком научном уровне.

Отличительными особенностями работы являются логическая последовательность поставленных задач и направленность на решение важной практической технической задачи – повышения уровня безопасности каналов связи телекоммуникационных сетей предприятий и организаций.

Основные выводы и положения диссертации достаточно широко опубликованы в научных изданиях и докладывались на представительных научно-технических конференциях, где получили одобрение научной общественности, признающей авторитет автора в разработке вопросов, положенных в основу диссертационной работы. Требование ВАК о наличии публикаций в изданиях из перечня ВАК выполнено.

Диссертация написана хорошим литературным языком и аккуратно оформлена. Содержание автореферата соответствует основным положениям диссертации и позволяет сформировать обоснованное представление по всей работе в целом, а содержание диссертации соответствует паспорту специальности 05.12.13 – Системы, сети и устройства телекоммуникаций, конкретно 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.

ВЫВОДЫ:

1. Представленная диссертация является законченной научной квалификационной работой, содержащей научно-обоснованные разработки новых моделей и алгоритмов повышения криптостойкости и производительности защищённого соединения на базе симметричной рюкзачной криптографической системы в сетях TCP/IP.

2. По актуальности темы исследований, научной новизне и практической значимости результатов, их апробации, опубликованию и реализации полученных результатов диссертация удовлетворяет требованиям п.п. 9-14 «Положения о присуждении учёных степеней», а её автор, Метлинов Александр Дмитриевич заслуживает присуждения ему учёной степени кандидата технических наук.

Официальный оппонент
Шиманов Сергей Николаевич, доктор технических
наук, профессор, ведущий научный сотрудник управления
АСУ и связи Межрегиональное общественное учреждение
«Института инженерной физики» (МОУ «ИИФ», iifrf.ru),
142210, Россия, Московская обл., г. Серпухов, Б. Ударный пер. д.1а.
телефон +7 (915) 037-61-00, e-mail: shimi_sn@mail.ru

С.Н. Шиманов

25.04.2018 года

Подпись доктора технических наук, профессора
Шиманова С.Н. заверяю: Начальник отдела кадров МОУ «ИИФ»

В.В. Евченко