ОТЗЫВ

официального оппонента к.т.н., Абрамова Константина Германовича 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 работы

Диссертационная работа направлена на решение научно-технической задачи повышения криптостойкости и производительности защищенного канала связи на базе симметричной рюкзачной криптографической системы в сетях *TCP/IP* за счет использования средств симметричной рюкзачной криптографической системы.

Современная распределенная ИТ-инфраструктура предприятий, большое количество задач в организациях, связанных с передачей конфиденциальной информации за пределы корпоративной сети, требуют обеспечения безопасности при использовании незащищенных каналов связи. В качестве среды передачи данных сегодня в большинстве случаев выступает глобальная сеть Интернет, которая подвержена множеству угроз, в том числе связанных с несанкционированным подключением к каналам связи и осуществлением перехвата и модификации передаваемой информации.

В 21 веке – информационном веке последствия от несанкционированного получения доступа к информации могут иметь катастрофический масштаб: от финансовых потерь в больших размерах до банкротства организации. Поэтому вопросы информационной безопасности и в частности защиты каналов связи является актуальной потребностью для большинства компаний.

В сегодняшних условиях даже злоумышленник с низким уровнем

знаний может воспользоваться множеством существующих общедоступных инструментов для получения несанкционированного доступа к трафику в каналах связи телекоммуникационных сетей *TCP/IP*, в связи с этим проблемы конфиденциальности и целостности информации стоят особенно остро.

Из выше сказанного можно сделать 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.

Содержание работы в целом соответствует названию и обозначенной проблематике. В диссертацию входят: введение, обзорная глава, в которой анализируются методы обеспечения информационной безопасности в каналах связи телекоммуникационных сетей *TCP/IP*, рассматриваются их основные элементы и структура, возможности, недостатки и уязвимости; глава, в которой представлена математическая модель рюкзачной системы защиты канала связи, описываются алгоритмы передачи и приема сообщений; глава, в которой приводятся результаты исследования предложенных средств организации защищенного канала связи, рассматриваются характеристики их производительности и криптостойкости, приведены результаты *NIST*-тестирования; глава, в которой предлагается практическая реализация алгоритмов, приведенных в предыдущих главах по экспериментальному исследованию разработанных средств организации защищенного канала связи в телекоммуникационных сетях *TCP/IP*, показываются их основные возможности и функционал; список сокращений и обозначений, заключение и приложения.

Новизна исследования и полученных результатов: 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 работу 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.

Степень обоснованности и достоверности научных положений, выводов и заключений, сформулированных в диссертации. Основные результаты, полученные в работе, являются обоснованными либо на доказательном, либо на экспериментальном уровне. Достоверность практических результатов достигается за счет большого количества экспериментов при решении задач и использования разработанного и существующего программного обеспечения.

Выводы и рекомендации, отражающие теоретическое и прикладное значение диссертационной работы, не вызывают сомнений в их правильности и обоснованности. Новизна и достоверность научных положений и выводов, сформулированных в диссертации, подтверждены апробацией на всероссийских и международных научных конференциях, исследованиями.

Опубликование основных результатов диссертации в научной печати.

Автором опубликовано 14 работ, 4 в изданиях из перечня ВАК. Получено 3 свидетельства о государственной регистрации программ для ЭВМ.

Ценность для науки и практики.

Ценность для науки определяется перечисленными выше научными

результатами, направленными на повышение криптостойкости и производительности защищенного канала связи на базе симметричной рюкзачной криптографической системы в сетях *TCP/IP*. Основная ценность - 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, а также алгоритмы передачи и приема сообщений в защищенном канале связи в телекоммуникационных сетях *TCP/IP*, построенном на базе рюкзачной системы защиты с общей памятью.

Внедрение этих алгоритмов позволяет безопасно хранить и передавать конфиденциальные данные предприятия, снижать материальные затраты на активные средства по защите, организовывать безопасный удаленный доступ к конфиденциальным данным. Развитие тематики в диссертационном исследовании имеет существенное теоретическое и практическое значение для проектирования защищенных каналов связи, систем и средств защиты информации в телекоммуникационных системах и сетях.

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 для развития симметричных рюкзачных криптосистем.

Замечания по диссертационному исследованию:

- Исследование направлено на нейтрализацию угроз конфиденциальности и целостности, но говорить о том, что «незначительное количество атак относится к атакам на доступность узлов канала и их подмену» (стр. 10) не корректно.
- В некоторых частях работы приведена информация из старых

источников, которая на сегодняшний день уже неактуальна. Например, на стр. 17 указано, что используются ключи размерами 40, 56 и 128 бит.

- На стр. 28 в выводах написано, что «каналы связи сетей *TCP/IP* не имеют встроенных средств защиты передаваемых сообщений. Механизмы обеспечения информационной безопасности реализованы на сеансовом уровне сетевой модели *OSI*...» Почему не был рассмотрен набор протоколов *IPSec*, который архитектурно встроен в протокол *IPv6*?
- Не ясно, как получилось значение снижения количества инцидентов по взлому серверов на 95%? Каковы исходные данные?
- Почему для сравнения по скорости работы и криптостойкости из всех алгоритмов стандартного шифронабора *TLS* выбраны алгоритмы *DH* и *AES*?
- Предложенная автором модификация протокола *TLS* с помощью симметричной рюкзачной криптосистемы с общей памятью использует блочный режим работы. В фазе начальной аутентификации двух узлов присутствует возможность выбора работы протокола *TLS* в поточном режиме. Что произойдет, если будет выбран этот режим работы?
- В работе использовано много ненаучных формулировок: «и т.п.», «весьма», «скорее всего». Использованы устаревшие термины, например, «ЭЦП».

Указанные недостатки существенным образом не снижают достоинств работы, которая в целом заслуживает положительной оценки.

Заключение

Работа представляет собой законченное научное исследование, включающее постановку проблемы, теоретические исследования и новые научные и практические результаты. Основные положения и выводы, сформулированные в работе, теоретически обоснованы, проверены в ходе экспериментальных исследований, достаточно отражены в научных публикациях и апробированы. Диссертационная работа соответствует

паспорту заявленной специальности.

Автореферат правильно отражает основное содержание диссертации. Диссертация Метлинова Александра Дмитриевича соответствует требованиям ВАК РФ и п.5 и п.10 паспорта специальности, предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Официальный оппонент
Абрамов Константин Германович, кандидат технических наук, менеджер направления поддержки инфраструктуры Общества с ограниченной ответственностью «ОМК – Информационные технологии»,
601213, г. Владимир, ул. Ноябрьская д. 121а
телефон +7 (980) 752-50-32
дата: 26.04.2018

К.Г. Абрамов

Подпись к.т.н.,
Абрамова К.Г. заверяю:

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ ОМК Информационные технологии г.Владимир ИНН 5247051889 ОГРН

Руководитель практики 1С
Кузин П.П.
дов. №5000-Д-54/17
от 03.10.2017