Межрегиональное общественное учреждение
"Институт инженерной физики"
(Научное, образовательное и производственное учреждение)
(МОУ "ИИФ")
Большой Ударный пер., д. 1а, г. Серпухов, Московская обл., 142210
тел. 8(4967)353193; 8(4967)351371; 8-499-400-05-75; факс: 354420; e-mail: info@iifmail.ru; www.iifrf.ru
ОКПО 42232569, ОГРН 1035000009417, ИНН/КПП 5043014134/504301001

16.05.2018 № 7/1605/ии

на № _____ от _____

Ученому секретарю диссертационного совета Д 212.025.04

600000, Владимир, ул. Горького, 87, ВлГУ, ФРЭМТ

УТВЕРЖДАЮ
Генеральный директор –
Первый Вице-президент Института
доктор технических наук, доцент

Д.В. Смирнов
«__» _____ 2018 г.

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»

На современном этапе развития телекоммуникационных систем и средств связи особенно остро встала проблема обеспечения их безопасности, с точки зрения, информации, циркулирующей в таких системах. Основные угрозы информационной безопасности в таких системах направлены на перехват с целью нарушения конфиденциальности и целостности передаваемых данных, а также на компрометацию передаваемой информации, нанося при этом непоправимый ущерб как компаниям, так и государству. При этом злоумышленники используют уязвимости, имеющиеся в протоколах защищенных каналов связи (КС) сетей TCP/IP, которых становится с каждым годом больше, вследствие усложнения моделей, алгоритмов и средств обработки информации.

Наиболее эффективным способом обеспечения безопасности информации в телекоммуникационных системах и средствах связи является применение криптостойкого шифрования TCP/IP-потока. Однако стандартный протокол TLS, обеспечивающий криптозащиту обладает двумя главными недостатками:

– низкая производительность (при больших объемах передаваемой информации);

– относительно низкая криптостойкость.

В связи с этим, автор предлагает использовать для повышения производительности и криптостойкости TCP/IP-потока защищенного КС программно-аппаратное решение на основе средств симметричной рюкзачной криптографической системы.

Исходя из изложенного, диссертация Метлинова А.Д., направленная на решение научной задачи по разработке новых моделей и алгоритмов повышения криптостойкости и производительности защищенных каналов связи на базе симметричной рюкзачной криптографической системы с общей памятью в сетях TCP/IP, является актуальной и востребованной временем.

В работе решены следующие задачи, обладающие научной новизной и практической значимостью:

– разработаны математические модели рюкзачной системы защиты КС; отличающиеся наличием общей памяти (ОП) между узлом отправителем и узлом-получателем, высоким уровнем плотности укладки шифруемого потока, использованием линейно-рекуррентных последовательностей, позволяющие повысить криптостойкость и производительность КС;

– модифицирован протокол TLS путем введения в структуру данных полей для хранения ОП, а также добавления модулей шифрования и дешифрования, реализующих рюкзачную систему защиты, что позволило повысит функциональные свойства протокола TLS;

– разработаны алгоритмы передачи и приема сообщений в защищенном КС в телекоммуникационных сетях TCP/IP, построенном на базе рюкзачной системы защиты с ОП.

Достоинством работы является доведение теоретических результатов до практической реализации и внедрения разработанной криптосистемы в фазы работы протокола TLS (аутентификация клиента и сервера, создание кода аутентификации сообщений и работы симметричных блочных алгоритмов шифрования и дешифрования), что позволило повысить быстродействие в среднем на 7-9 процентов в сравнении с методом DH_AES в стандартном TLS и на 25-28 процентов в сравнении со стандартным методом на основе рюкзачной системы без ОП.

Обоснованность результатов, достигнутых соискателем, основывается на внедрении полученных практических результатов на предприятиях города Владимира и Владимирской области: ООО «Русский мастер», ООО «ДИВАНиЯ», ИП Щерба А.Ю., а также получением трех свидетельств на программы.

Основные положения работы прошли достаточную апробацию на научно-технических конференциях высокого уровня и в научной печати. Требование о наличии публикаций в журналах из Перечня ВАК в работе выполнено.

Недостатками диссертации, судя по автореферату, являются:

– на рисунках 1 и 2 автореферата приведены схемы работы защищенного канала связи на основе стандартной процедуры протокола TLS, из которых неясно, что и где модифицирует автор для достижения полученных научных и практических результатов;

– не совсем корректная формулировка достоверности полученных результатов.

Однако, указанные замечания не снижают ценности диссертации, ее практической и научной значимости.

Таким образом, диссертация Метлинова Александра Дмитриевича на тему: «Модели и алгоритмы повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях TCP/IP» является законченной научно-квалификационной работой, в которой решена новая научная задача по разработке моделей и алгоритмов повышения криптостойкости и производительности защищенных каналов связи на базе симметричной рюкзачной криптографической системы с общей памятью в сетях TCP/IP, позволяющих значительно повысить быстродействие и криптостойкость передаваемых данных по защищенному каналу связи, и полностью удовлетворяет требованиям п.п. 9, 10, 11 и 13 «Положения о присуждении ученых степеней».

Считаем, что Метлинов А.Д. заслуживает присуждения ученой степени кандидата технических наук по специальности 05.12.13 «Системы, сети и устройства телекоммуникаций».

Отзыв составили:

Начальник управления АСУ и связи
Кандидат технических наук — В.А. Прасолов

Старший научный сотрудник управления АСУ и связи
кандидат технических наук — К. В. Карпочкин