На правах рукописи

Метлинов Александр Дмитриевич

МОДЕЛИ И АЛГОРИТМЫ ПОВЫШЕНИЯ КРИПТОСТОЙКОСТИ И ПРОИЗВОДИТЕЛЬНОСТИ ЗАЩИЩЕННОГО КАНАЛА СВЯЗИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ *TCP/IP*

Специальность: 05.12.13 – Системы, сети и устройства телекоммуникаций

Автореферат

диссертации на соискание ученой степени

кандидата технических наук

Владимир 2018

Работа выполнена на кафедре «Информатика и защита информации» в ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (ВлГУ)

Научный руководитель: **Монахов Михаил Юрьевич**
доктор технических наук, профессор, заведующий кафедрой информатики и защиты информации ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

Официальные оппоненты: **Шиманов Сергей Николаевич**
доктор технических наук, профессор, ведущий научный сотрудник по АСУ и связи МОУ «Институт инженерной физики» (ИИФ РФ), г. Серпухов.

Абрамов Константин Германович
кандидат технических наук, менеджер направления поддержки инфраструктуры ООО «ОМК - Информационные технологии», г. Владимир.

Ведущая организация: ФГБОУ ВО «Омский государственный технический университет», г. Омск.

Защита диссертации состоится 31 мая 2018 года в 14:00 часов в ауд. 301-3 на заседании диссертационного совета Д 212.025.04 при Владимирском государственном университете имени Александра Григорьевича и Николая Григорьевича Столетовых по адресу: 600000, г. Владимир, ул. Горького, 87, корп. 3, ВлГУ, ФРЭМТ, РТиРС.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» и на сайте http://diss.vlsu.ru.

Автореферат разослан «22» марта 2018 г.

Отзывы на автореферат в двух экземплярах, заверенные печатью, просим направлять по адресу: 600000, г. Владимир, ул. Горького, 87, ВлГУ, ФРЭМТ, РТиРС, ученому секретарю диссертационного совета Д 212.025.04

Ученый секретарь диссертационного совета,
доктор технических наук, профессор А. Г. Самойлов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность и степень разработанности темы. Содержание проблемы информационной безопасности (ИБ) и защиты информации (ЗИ) в системах и сетях телекоммуникаций интерпретируются следующим образом. По мере развития и усложнения моделей, алгоритмов и средств обработки и передачи информации в защищенных каналах связи (КС) телекоммуникационных сетей *TCP/IP* повышается уязвимость существующих протоколов безопасности КС, напрямую влияющая на возможность несанкционированного копирования, уничтожения, блокирования или искажения информации.

Основные угрозы ИБ направлены на перехват и имперсонацию сообщений (нарушение конфиденциальности и целостности передаваемых данных), нередки атаки на доступность узлов канала и их подмену. КС сетей *TCP/IP* не имеют встроенных средств защиты, существующие механизмы обеспечения ИБ реализованы на сеансовом уровне *OSI* и имеют множество уязвимостей.

Проблема ИБ и ЗИ в системах и сетях телекоммуникаций исследовалась в трудах ведущих российских ученых Герасименко В.А., Домарева В.В., Иванова М.А., Завгороднего В.И., Лукацкого А.В., Медведковского И.Д., Мурина Д.М., Никитина О.Р., Панасенко С., Соколова А.В., Черемушкина А.В., Шаньгина В.Ф., Хорева А.А. Значительный вклад в решение выделенной проблемы внесли зарубежные исследователи Адлеман Л., Блэкберн Р., Брикелл Э., Грэм Р., Гудман Р., Вастон А.С., Калиф М., Касахар М., Кимур М., Кобаяс К., Маколи Э., Минхуа Ц., Мерфи Ш.П., Нидеррайтер Х., Нгуен Ф., Нием В., Патерсон С., Ривест Р.Л., Хусейн А., Шамир А., Шеннон К., Шнайер Б., Шор Б., Штерн Ж.Г и другие.

Анализируя результаты исследований, можно сделать вывод, что наиболее перспективным подходом в обеспечении безопасности передаваемых сообщений является использование криптостойкого шифрования *TCP/IP*-потока. Это не позволяет злоумышленнику анализировать служебную информацию и уменьшает вероятность доступа к незашифрованным данным в узлах сети. Стандартный протокол *TLS* обеспечивает криптозащиту КС, но имеет недостаточную производительность и относительно низкую криптостойкость. Для повышения производительности и криптостойкости защищенного КС перспективным является использование средств симметричной рюкзачной криптографической системы.

Таким образом, исследования, направленные на разработку новых моделей и алгоритмов повышения криптостойкости и производительности защищенного КС на базе симметричной рюкзачной криптографической системы в

сетях *TCP/IP*, актуальны и имеют практическое значение в решении проблемы обеспечения ИБ сетей телекоммуникаций предприятий.

Объект исследования – защищенный КС в телекоммуникационных сетях *TCP/IP*.

Предмет исследования - методы и средства криптографической защиты информации в КС сетей *TCP/IP*.

Цели и задачи работы. Целью работы является повышение криптостойкости и производительности защищенного КС в телекоммуникационных сетях *TCP/IP*. В соответствии с целью были поставлены и решены следующие научные задачи:

- анализ методов и средств обеспечения ИБ и ЗИ в КС телекоммуникационных сетей *TCP/IP,* выявление особенностей организации защищенного КС при помощи криптографического протокола *TLS*;
- разработка семейства моделей и алгоритмов повышения производительности и криптостойкости симметричных рюкзачных криптосистем в защищенных КС сетей *TCP/IP*;
- модификация моделей симметричных рюкзачных криптосистем в защищенных КС сетей *TCP/IP* семейством *CBC*-блочных алгоритмов шифрования и дешифрования информации;
- экспериментальное исследование предложенных средств и внедрение результатов работы.

Научная новизна. Получены следующие научные результаты:

- разработаны математические модели рюкзачной системы защиты КС, отличающаяся наличием общей памяти (ОП) между узлом-отправителем и узлом-получателем, высоким уровнем плотности укладки рюкзака, использованием линейно-рекуррентных последовательностей, позволяющие повысить криптостойкость и производительность КС (п.5 и п.10 паспорта 05.12.13);
- модифицирован протокол *TLS* путем введения в структуру данных полей для хранения ОП, а также добавления модулей шифрования и дешифрования, реализующих рюкзачную систему защиты, что позволяет повысить его (протокола) функциональные свойства (п.5 и п.10 паспорта 05.12.13);
- разработаны алгоритмы передачи и приема сообщений в защищенном КС в телекоммуникационных сетях *TCP/IP*, построенном на базе рюкзачной системы защиты с ОП (п.5 и п.10 паспорта 05.12.13).

Практическая значимость работы. Разработано информационное и программное обеспечение комплекса алгоритмов симметричной рюкзачной криптосистемы с ОП, включающее: программный комплекс *CBC*-блочной симметричной рюкзачной криптологической системы для вариации с плотно-

стью 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). 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 КС сетей *TCP/IP*: канал работает в среднем на 7-9% быстрее, чем использующий *DH_AES* в стандартном *TLS* и на 25-28% быстрее, чем рюкзачная криптосистема, в основе которой лежит супервозрастающий базис независимо от типа и объема исходных данных. Разработанная криптосистема с общей памятью при минимальном размере рюкзачного базиса в 64 бита имеет плотность укладки в пределах $0.9907 \leq \rho \leq 0.9989$, что удовлетворяет современным требованиям криптостойкости.

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.

Методология и методы исследования. В данном исследовании были использованы методы криптографии, линейной и нелинейной алгебры, теории сложности алгоритмов, математического анализа, математической статистики и теории вероятности.

Положения, выносимые на защиту:

- математические модели рюкзачной системы защиты КС;
- модификация протокола *TLS*;
- алгоритмы передачи и приема сообщений в защищенном КС в телекоммуникационных сетях *TCP/IP*;
- результаты экспериментального исследования и внедрения предложенных моделей и алгоритмов.

Степень достоверности результатов исследований. 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 собственного и стандартного программного обеспечения.

Апробация работы. Материалы диссертационной работы докладывались и обсуждались на IX и XI Международной научной конференции «Перспективные технологии в средствах передачи информации» (Владимир 2013,

2015); I, II и III Международной научно-практической конференции «Информационная безопасность в свете Стратегии Казахстан - 2050» (Астана 2013, 2014 и 2015); XXXIII и XXXVI Всероссийской НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (Серпухов 2014 и 2017); V Всероссийской научно-технической конференции ИКВО НИУ ИТМО «Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур» (Санкт-Петербург 2014); V международной научной конференции «Современные методы и проблемы теории операторов и гармонического анализа и их приложения V» (Ростов-на-Дону 2015) и других. Выигран конкурс «УМНИК-2015».

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

Личный вклад. 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.

Структура и объем диссертационной работы. Диссертация состоит из введения, четырех глав, заключения, списка обозначений и сокращений, списка определений, списка использованных источников из 74 наименований, 6 приложений и содержит 166 страниц, из них 117 страниц основного текста, иллюстрированного 45 рисунками, содержит 11 таблиц.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** формулируется цель и задачи исследования, обосновывается актуальность, научная новизна работы, теоретическая и практическая значимость результатов.

В **главе 1** «*Защищенный канал связи телекоммуникационных сетей TCP/IP. Анализ объекта исследования*» приводятся объект и предмет исследования. Анализируются методы обеспечения ИБ в КС телекоммуникационных сетей *TCP/IP*, рассматриваются их основные элементы и структура, возможности, недостатки и уязвимости.

Объектом диссертационного исследования является защищенный канал связи (КС) в телекоммуникационных сетях *TCP/IP*. Канал связи (англ. *channel, data line*) — это система технических средств и среда распространения сигналов для передачи данных (информации) от отправителя к получателю (рисунок 1).

Рисунок 1 – Структурная схема канала связи сети *TCP/IP*

Особенности КС в телекоммуникационных сетях *TCP/IP*: основные угрозы и атаки в КС направлены на перехват передаваемых сообщений, КС не имеет встроенных средств защиты, механизмы обеспечения ИБ реализованы на сеансовом уровне сети и имеют множество проблем. Например, для *TLS* (рисунок 2).

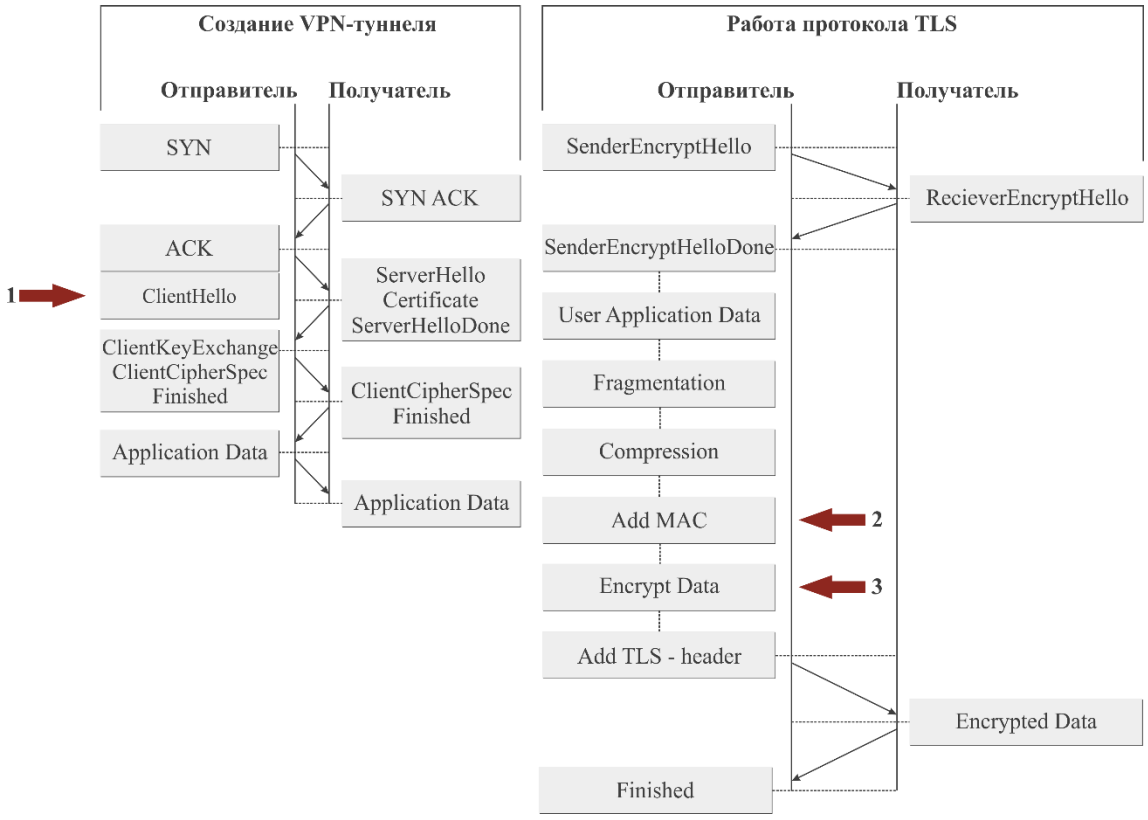

Рисунок 2 – Схема работы *TLS*

Проблема 1. Из-за большой вариации используемых алгоритмов ассиметричной криптографии с разными длинами ключей возможно осуществление *MITM*-атаки: все передаваемые данные будут скомпрометированы. Для генерации сеансовых ключей (при аутентификации сервера и клиента) на этапе создания *VPN*-туннеля вместо медленного *RSA* предлагается использовать симметричный вариант рюкзачной криптосистемы с *pre-shared key* в виде общей памяти, для генерации *Master Secret* использовать уникальную для пары (клиент, сервер) хеш-функцию.

Проблема 2. *MAC* можно проверить только после дешифрования и, если значение оказалось некорректным, *TLS* должен сообщить об ошибке. Атакующий, манипулируя шифрованным текстом, может использовать дешифровывающий узел в качестве «криптографического оракула», который постепенно раскроет весь секретный текст. На этом основано несколько атак на *TLS*. Для решения этой проблемы предлагается использовать построение параметризованного по наличию ОП стандартного алгоритма хеширования. Свертка шифра порождает строго индивидуальную хэш-функцию для пары (отправитель, получатель), которая лишена вышеописанного недостатка.

Проблема 3. Низкая криптостойкость и производительность шифронабора *TLS* (например, *RC2, RC4, DES, 3DES*). Предлагается использовать алгоритмы преобразования информации с помощью *CBC*-блочного варианта симметричной рюкзачной криптосистемы с ОП.

Основными направлениями повышения эффективности использования протоколов ЗИ в КС сетей *TCP/IP* является повышение их производительности и криптостойкости. Под производительностью *TLS* понимается величина $IPS(TLS) = 1/(T_{auth} + T_{frag} + T_{cmps} + T_{MAC} + T_{enc})$, где T_{auth} - время работы алгоритма аутентификации клиента и сервера; T_{frag} – время работы алгоритма фрагментации сообщений; T_{cmps} - время работы алгоритма компрессии сообщений; T_{MAC} - время работы алгоритма создания кода аутентификации сообщений и T_{enc} – время работы симметричных блочных алгоритмов шифрования и дешифрования сообщений. Внедряя предложенную криптосистему в такие фазы работы протокола *TLS*, как фаза аутентификации клиента и сервера, фаза создания кода аутентификации сообщений и фаза работы симметричных блочных алгоритмов шифрования и дешифрования сообщений, мы тем самым уменьшаем величины T_{auth}, T_{MAC} и T_{enc} из-за чего увеличивается значение $IPS(TLS)$, то есть повышается производительность *TLS*.

Под характеристикой криптостойкости будем понимать величину $W = \frac{\rho(1-P)\omega}{\rho_{max}}$, где ρ – плотность укладки рюкзака; $\rho = y/(max_{1\le i\le y}\, log_2\, a_y)$, y

– количество элементов возрастающего базиса; a_y – максимальный элемент базиса; ρ_{max} – предельная плотность ($\rho_{max} \approx 1{,}45$); P - вероятность успешной реализации L^3-атаки; ω – показатель статистической защищенности, где $\omega = 1$, если криптосистема успешно прошла все стандартные *NIST*-тесты, иначе $\omega = 0$.

Основные проблемы рюкзачных криптосистем, которые существенным образом влияют на их криптостойкость: использование рюкзачных векторов (базисов) малой размерности, для которых задача о рюкзаке легко решаема даже вручную из-за очень низкого показателя плотности укладки; использование в качестве рюкзачных сверхрастущих векторов (супервозрастающих последовательностей), для которых возможно проведение L^3-атаки; атака Шамира на пару связанных между собой ключей – открытого и закрытого. Для решения этих проблем предлагается: (1) использовать общую память между отправителем и получателем сообщений в КС сетей *TCP/IP*; (2) отказаться от базисов малой размерности и супервозрастающих базисов в пользу линейно-рекуррентных последовательностей порядка m, где $m \geq 2$; (3) добиться $\rho \sim 1$, при котором затруднено проведение L^3-атаки.

В **главе 2** «*Разработка моделей и алгоритмов организации защищенного канала связи в сетях TCP/IP на базе симметричной рюкзачной криптосистемы*» представлена математическая модель рюкзачной системы защиты КС, описываются алгоритмы передачи и приема сообщений.

Математические модели рюкзачной системы защиты КС

Параметры моделей: M – исходное сообщение (отрытый текст); $M = M_1 \,||\, \dots \,||\, M_n \,||\, M_N$, где N – количество блоков в открытом сообщении; $M_n = m_{n1} \,||\, \dots \,||\, m_{ng} \,||\, m_{nG}$ - побитовое представление каждого блока открытого сообщения, G – количество бит в одном блоке и $m_{ng} \in \{0,1\}$; k – криптографический ключ; S – передаваемое (зашифрованное) сообщение; $S = S_1 \,||\, \dots \,||\, S_n \,||\, S_N$, где N – количество блоков в закрытом сообщении; $S_n = s_{n1} \,||\, \dots \,||\, s_{ng} || s_{nG}$ - побитовое представление каждого блока закрытого сообщения, $s_{ng} \in \{0,1\}$; $F_k(M)$ и $F_k^{-1}(S)$ – алгоритмы прямого и обратного преобразования информации на ключе k; O – общая память между отправителем и получателем; $O = \{o_1, \dots, o_b, o_B\}$, где B – количество документов общей памяти, || - операция конкатенации.

Модель 1. Прямое преобразование $M \xrightarrow{F_k(M)} S$: $S_n = \left(\sum_{n=1}^{G} m_g * k_g(\Psi_0)\right)$; где $k_1(\Psi_0) = 1$, $k_2(\Psi_0) = 1 \oplus \Psi_0$, ..., $k_g(\Psi_0) = k_{g-1}(\Psi_0) \oplus k_{g-2}(\Psi_0)$, для $g > 2$, до тех пор, пока таких элементов $k_g(\Psi_0)$ не будет ровно G, $\oplus$ - операция сложения в

выбранном поле Галуа GF_p; Ψ_0 - серединный элемент отсортированной последовательности $\{\Psi\}$ не повторяющихся произведений элементов вектора O на элементы вектора $E = \{e_1, \dots, e_b, e_B\}$, $e_b \in \{0,1\}$, генерируемых случайным образом, вычисляемый в соответствии с алгоритмом, записанным ниже псевдокодом по рекомендации *IETF*:

```
init vector_O [1…B] // вектор O
init vector_E [1…B] // вектор E
init vector_K [1…G] // вектор K - криптографический ключ
init temp_vector_ Ψ [1…B*B] // временный вектор произведений Ψ
init vector_ Ψ [1…B*B] // вектор произведений Ψ

for (i=1; i <=B; i++) // вычисление всех возможных произведений O и E
        for (j=1; j <=B; j++)
                t_Ψ(j) = O(i) * E(j)

for (i=1; i <=B*B; i++) // удаление одинаковых элементов из вектора Ψ
        for (j=1; j <=B*B; j++)
                if (t_Ψ(i) != t_Ψ(j) )
                Ψ(j) = t_Ψ(j)

for (i=1; i <=B*B; i++) // сортировка вектора Ψ по возрастанию
        for (j= B*B; j > i; j--)
                if (Ψ(j − 1) > Ψ(j))
                temp = Ψ(j − 1)
                Ψ(j − 1) = Ψ(j)
                Ψ(j) = temp

Ψ0= Ψ size(Ψ) / 2 // выбор срединного элемента
G = size(Ψ);
K(1) = 1;

for (Ψ −2; Ψ <–G; Ψ ++) // формирование вектора K
        k(Ψ) = k(Ψ − 1) + k(Ψ − 2)

for (i=1; i <=G; i++) // прямое преобразование в КС для одного блока текста
        s(i) = m(i) * k(i)
```

Модель 2. Обратное преобразование $S \xrightarrow{F^{-1}(S)} M$: $M_n = m_{n1} || \dots || m_{ng} || m_{nG}$- побитовое представление каждого блока открытого сообщения; $m_{ng} = s_{ng} - k_g(\Psi_0)$, $m_{n(g-1)} = s_{n(g-1)} - k_{g-1}(\Psi_0)$, …, $m_{n1} = s_{n1} - k_1(\Psi_0)$ – дешифрование с помощью «жадного алгоритма»; если $s_{ng} < k_g(\Psi_0)$ – то $k_g(\Psi_0) = k_{g-1}(\Psi_0)$. Ψ_0 определяется аналогично модели 1.

Модифицированная структура данных *TLS*

Приведен алгоритм формирования ОП, записанным ниже псевдокодом по рекомендации *IETF*. По сравнению со стандартным *TLS* расширяется его структура данных за счет добавления ОП между узлами-отправителями и узлами-получателями, а также внедрения нового модуля шифрования на основе разработанной рюкзачной схемы с ОП в стандартный шифронабор *TLS*.

```
        enum { server, client } ConnectionEnd; отправитель/получатель
        enum { null, rc4, rc2, des, 3des, des40, skc_sh } BulkCipherAlgorithm; алгоритм
симметричного шифрования
        enum { stream, block } CipherType; блочный/поточный режим
        enum { true, false } IsExportable;
        enum { null, md5, sha } MACAlgorithm; алгоритм хеширования
        enum { null(0), (255) } CompressionMethod; метод сжатия (null(0) по умолчанию)
        enum {sh_m1, sh_m2, …, sh_mn} SharedMemory; общая память
        struct {
          ConnectionEnd         entity;
          BulkCipherAlgorithm   bulk_cipher_algorithm;
          CipherType            cipher_type;
          uint8                 key_size;
          uint8                 key_material_length;
          IsExportable          is_exportable;
          MACAlgorithm          mac_algorithm;
          uint8                 hash_size;
          CompressionMethod     compression_algorithm;
          opaque                master_secret[48];
          opaque                client_random[32];
          opaque                server_random[32];
          opaque                shared_memory[64];
} SecurityParameters;
```

Алгоритмы передачи и приема сообщений в КС

Алгоритм передачи сообщений:

Шаг 1. Установить *TCP*-соединение по КС, задав *IP*-адрес и порт узла-получателя.

Шаг 2. Провести взаимную аутентификацию узла-отправителя и узла-получателя с помощью протокола Диффи – Хеллмана из стандартного шифронабора протокола безопасности *TLS*. При успешной аутентификации перейти к шагу 3, иначе конец алгоритма (закрыть соединение).

Шаг 3. Выполнить прямое преобразование сообщения $M \xrightarrow{F_k(M)} S$ в соответствии с математической моделью 1 рюкзачной системы защиты.

Шаг 4. Передать $E = \{e_1, \dots, e_b, e_B\}$ и $S = S_1 \,||\, \dots \,||\, S_n \,||\, S_N$ аутентифицированному узлу-получателю по установленному КС.

Шаг 5. Дождаться ответа от узла-получателя. Если ответа не поступило перейти к шагу 4. При повторном отсутствии ответа от узла-получателя закрыть установленное соединение. Конец алгоритма.

Алгоритм приема сообщений:

Шаг 1. Провести взаимную аутентификацию узла-отправителя и узла-получателя с помощью протокола Диффи – Хеллмана из стандартного шифронабора протокола безопасности *TLS*. При успешной аутентификации перейти к шагу 2, иначе конец алгоритма (закрыть соединение).

Шаг 2. Принять $E = \{e_1, \dots, e_b, e_B\}$ и $S = S_1 \,||\, \dots \,||\, S_n \,||\, S_N$ от узла-отправителя по установленному КС.

Шаг 3. Ответить узлу-отправителю об успешном принятии пересланных данных и перейти к шагу 4, иначе сообщить об ошибке и закрыть соединение.

Шаг 4. Выполнить обратное преобразование сообщения $M \xrightarrow{F_k(M)} S$ в соответствии с математической моделью 2 рюкзачной системы защиты КС. Конец алгоритма.

В **главе 3** «*Экспериментальное исследование защищенного канала связи на базе симметричной рюкзачной криптосистемы с общей памятью*» приводятся результаты исследования предложенных средств организации защищенного канала связи, рассматриваются характеристики их производительности и криптостойкости, приведены результаты *NIST*-тестирования.

Экспериментальное исследование зависимости криптостойкости (вероятности успешной реализации L^3-атаки) от плотности укладки рюкзака $P(\rho)$ показало (рисунок 3): предложенная криптосистема обладает плотностью укладки $\rho \geq 0.9408$, что в соответствии с рекомендациями Костера – Одлыжко затрудняет атаку. Криптосистема при минимальном размере рюкзачного базиса $G = 64$ бита имеет $0.9907 \leq \rho \leq 0.9989$, что удовлетворяет современным требованиям криптостойкости; с возрастанием ρ уменьшается $P(\rho)$: при $0.9907 \leq \rho \leq 0.9989$ $P(\rho) \approx 1 \dots 2$ %, при $1.1910 \leq \rho \leq 1.1991$ $P(\rho) \approx 0.4 \dots 0.9$ % и при $1.4415 \leq \rho \leq 1.4429$ $P(\rho) \approx 0.1 \dots 0.2$ %.

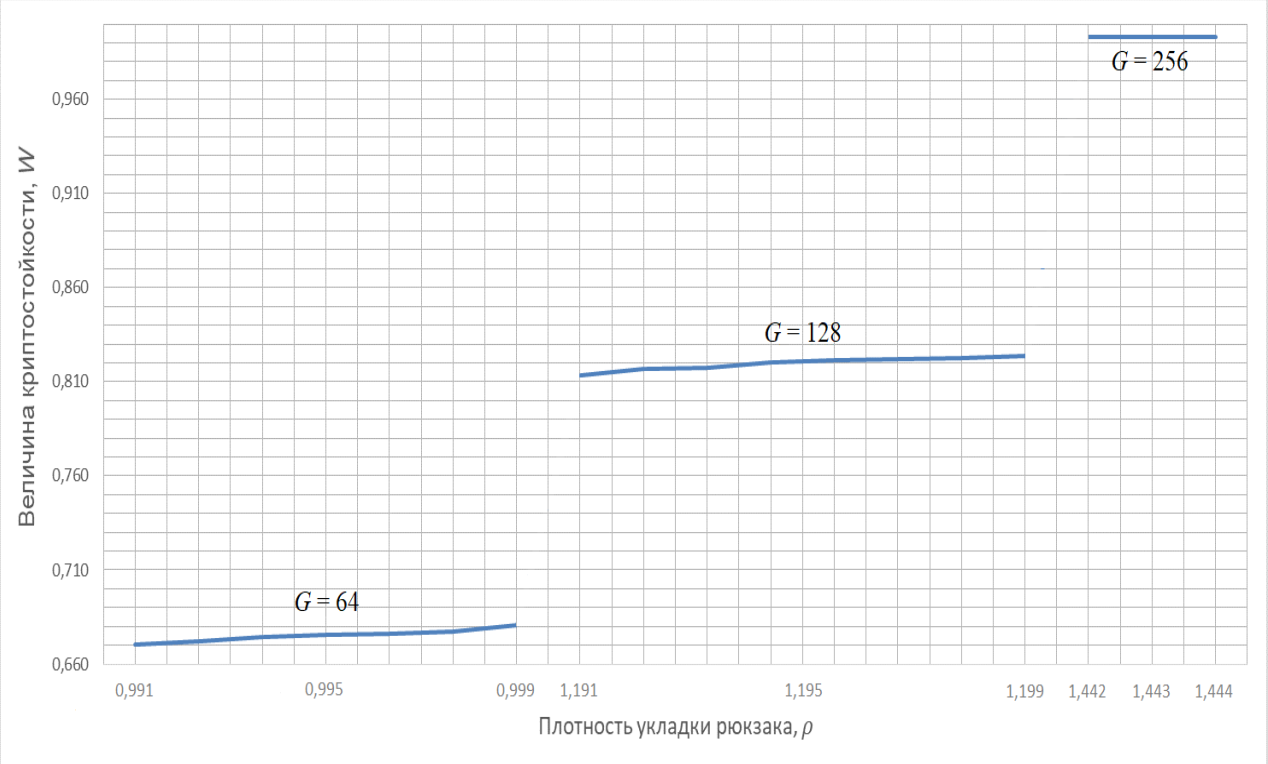

Рисунок 3 – Зависимость криптостойкости от плотности укладки рюкзака

Результаты *NIST*-тестов (таблица 1) подтвердили тот факт, что последовательность, являющая результатом работы шифра, похожа на случайную, что в свою очередь говорит о высоком уровне криптостойкости предложенной системы.

Таблица 1 – Результаты *NIST* – тестирования

Название теста	Полученное значение r / требуемое			Значение ω (результат теста)
	Текст №1	Текст №2	Текст №3	
Частотный побитовый тест	0,48 / 0,01	0,49 /0,01	0,49 / 0,01	1 (пройден)
Частотный блочный тест	0,13 / 0,01	0,17 / 0,01	0,15 / 0,01	1 (пройден)
Тест на последовательность одинаковых битов	0,67 / 0,01	0,64 / 0,01	0,61 / 0,01	1 (пройден)
Тест на самую длинную последовательность единиц в блоке	0,70 / 0,01	0,73 / 0,01	0,76 / 0,01	1 (пройден)
Тест рангов бинарных матриц	0,24 / 0,01	0,25 / 0,01	0,27 / 0,01	1 (пройден)
Спектральный тест	0,21 / 0,01	0,19 / 0,01	0,22 / 0,01	1 (пройден)
Тест на совпадение неперекрывающихся шаблонов	0,05 / 0,01	0,05 / 0,01	0,06 / 0,01	1 (пройден)
Тест на совпадение перекрывающихся шаблонов	0,09 / 0,01	0,07 / 0,01	0,09 / 0,01	1 (пройден)
Универсальный статистический тест Маурера	0,15 / 0,01	0,16 / 0,01	0,13 / 0,01	1 (пройден)
Тест на линейную сложность	0,37 / 0,01	0,34 / 0,01	0,36 / 0,01	1 (пройден)
Тест на периодичность	0,25 / 0,01	0,21 / 0,01	0,23 / 0,01	1 (пройден)
Тест приблизительной энтропии	0,49 / 0,01	0,46 / 0,01	0,50 / 0,01	1 (пройден)
Тест кумулятивных сумм	0,21 / 0,01	0,21 / 0,01	0,23 / 0,01	1 (пройден)
Тест на произвольные отклонения	0,09 / 0,01	0,07 / 0,01	0,11 / 0,01	1 (пройден)
Другой тест на произвольные отклонения	0,04 / 0,01	0,04 / 0,01	0,05 / 0,01	1 (пройден)

Исследование производительности позволяет сделать следующие выводы: спроектированная криптосистема работает в среднем на 7-9% быстрее, чем функция *DH_AES* в стандартном шифронаборе *TLS* и на 25-28% быстрее, чем рюкзачная криптосистема, в основе которой лежит супервозрастающий базис независимо от типа и объема исходных данных (рисунки 4-5).

Полученные характеристики позволяют делать выводы о возможности применения разработанного семейства алгоритмов в композициях с другими стандартами, такими как *AES*, *DES* и *GOST1989*, для создания дополненного шифронабора в протоколе *TLS*.

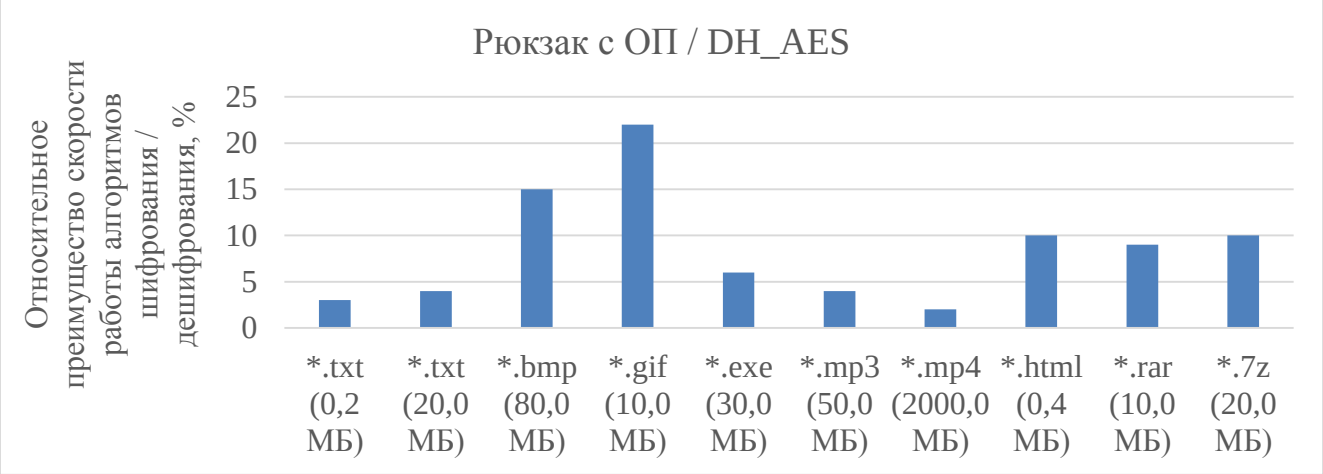

Рисунок 4 – Относительное преимущество скорости работы алгоритмов шифрования / дешифрования рюкзака с ОП к *DH_AES*

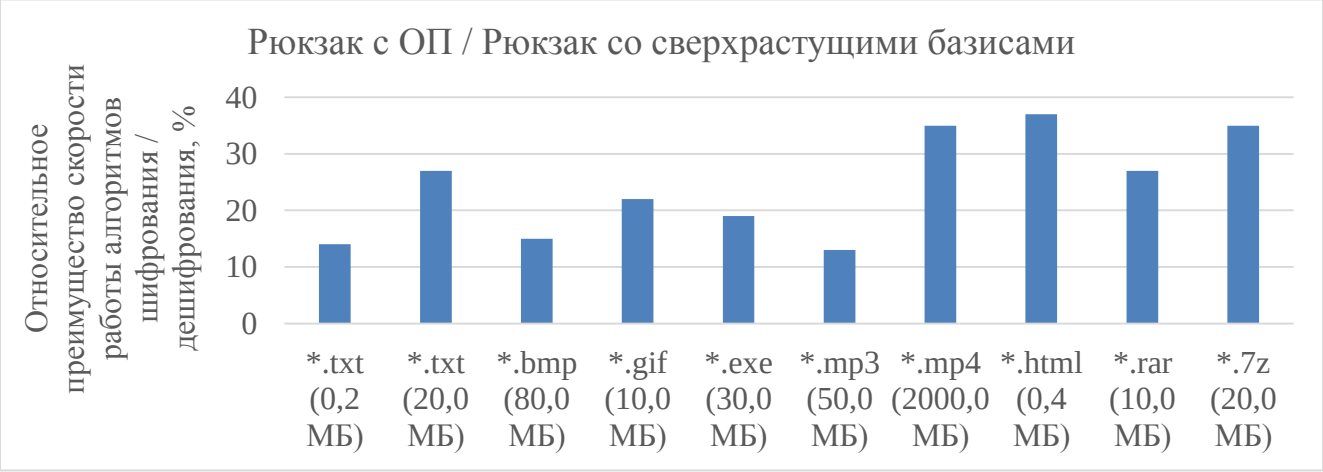

Рисунок 5 – Относительное преимущество скорости работы алгоритмов шифрования / дешифрования рюкзака с ОП к сверхрастущему рюкзаку

В **главе 4** «*Практическая разработка и внедрение средств организации защищенного канала связи*» 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.

В состав реализованного ПО входит: приложение для генерации из выбранного массива документов общей памяти (*SM_generator*); основное приложение для шифрования и дешифрования сообщений с помощью разработанного семейства алгоритмов *CBC*-блочной симметричной рюкзачной криптосистемы с общей памятью и передачи выходных данных получателю (*Knapsack cryptosystem*).

В качестве одного из вариантов внедрения разработанных средств организации защищённого КС разработано клиент-серверное приложение для защиты авторского медиаконтента на основе семейства *CBC*-блочных алгоритмов симметричной рюкзачной криптосистемы с общей памятью (*media_knapsack_system*) в рамках работы по гранту УМНИК-2015.

Применение результатов в ООО «Русский мастер» (Владимирская область, поселок Льнозавод) позволило безопасно хранить данные предприятия, составляющие коммерческую тайну, а также безопасно их передавать между подразделениями; снизить материальные затраты на активные средства по защите. Внедрение в ООО «ДИВАНиЯ» (Владимирская область, поселок Льнозавод) позволило организовать безопасный удаленный доступ к конфиденциальным данным; снизить до минимума материальные затраты на активные средства по их защите, ускорить работу с этими данными в 3 раза; уменьшить количество инцидентов по взлому серверов на 95%, ускорить работу удаленных пользователей с серверами в 2 раза, время на аутентификацию каждого пользователя сокращено с минуты до десяти секунд. Использование в ИП Щерба А.Ю (г. Владимир) позволило безопасно хранить данные индивидуального предпринимателя, составляющие коммерческую тайну и максимально снизить материальные затраты на активные средства по их защите.

Основные результаты диссертационного исследования:

1. КС сетей *TCP/IP* не имеет встроенных средств защиты, механизмы обеспечения ИБ реализованы на сеансовом уровне *OSI* и имеют множество уязвимостей. Перспективным подходом является использование криптостойкого шифрования *TCP/IP*-потока с использованием протокола *TLS*, который обеспечивает криптозащиту, но имеет недостаточное быстродействие и относительно низкую криптостойкость. Для повышения быстродействия и криптостойкости КС перспективным является использование средств симметричной рюкзачной криптографии.

2. 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.

3. Предложена модификация симметричной рюкзачной криптосистемы с общей памятью семейством *CBC*-блочных алгоритмов шифрования и дешифрования информации, что еще в большей мере повышает криптостойкость: при минимальном размере рюкзачного базиса в 64 бита плотность укладки рюкзака лежит в пределах $0.9907 \leq \rho \leq 0.9989$, что в соответствии с

рекомендациями Костера – Одлыжко значительно затрудняет реализацию L^3-атаки (ее вероятность не более 1 - 2 %).

4. Экспериментально выявлено, что между вероятностью успешной реализации L^3-атаки и плотностью укладки рюкзака при различных объемах исходного текста есть сильная статистическая зависимость (значение $|R| \sim 0.90$). Зашифрованные по предложенным алгоритмам тексты успешно прошли статистические *NIST* – тесты, что говорит о стойкости криптосистемы к частотному анализу и типовым атакам.

5. 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*, канал работает в среднем на 7-9% быстрее, чем использующий *DH_AES* в стандартном *TLS* и на 25-28% быстрее, чем рюкзачная криптосистема, в основе которой лежит супервозрастающий базис независимо от типа и объема исходных данных.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в изданиях рекомендованных ВАК РФ

1. Метлинов А.Д. Симметричная рюкзачная криптосистема с общей памятью и плотностью укладки больше единицы / Александров А.В., Метлинов А.Д. // «Проблемы ИБ. Компьютерные системы». – 2014. - №4. - С. 58-65;

2. Метлинов А.Д. Симметричная рюкзачная криптосистема с общей памятью и высокой плотностью укладки / Александров А.В., Метлинов А.Д. // Изв. вузов. Приборостроение. – 2015. - №5(Т.58). - С. 344-350;

3. Александров А.В., Метлинов А.Д. «Алгоритмические и статистические свойства разреженной рюкзачной криптосистемы с общей памятью» // Изв. вузов. Приборостроение. 2017. Т. 60, № 1.

4. Метлинов А. Д. Модификация протокола *TLS* на основе разреженной криптосистемы с общей памятью // Изв. вузов. Приборостроение, 2018, Т. 61, № 1, С. 61—65.

Публикации в других научных изданиях

5. Александров А.В, Метлинов А.Д. «О симметричной рюкзачной криптографической системе, устойчивой к L^3-атакам», Сборник трудов IX Международной научной конференции «Перспективные технологии в средствах передачи информации», г. Суздаль, том 1, с. 167-170, 2013;

6. Александров А.В, Метлинов А.Д. «Симметричная рюкзачная криптографическая система, устойчивая к L^3-атакам», I Международной научно-

практической конференции «Информационная безопасность в свете Стратегии Казахстан - 2050», г. Астана, сборник научных трудов, с. 425-430, 2013;

7. Александров А.В., Метлинов А.Д. «К вопросу об особенностях реализации симметричной рюкзачной криптосистемы с общей памятью и плотностью укладки больше единицы» // XXXIII Всероссийская НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем», г. Серпухов, сборник научных трудов, часть 4, с. 161-167, 2014;

8. Александров А.В., Метлинов А.Д., Зимников А.С. «О семействе рюкзачных блочных шифров с общей памятью и плотностью укладки больше единицы и хеш-функций на их основе» // Сборник научных трудов II Международной научно-практической конференции «Информационная безопасность в свете Стратегии Казахстан - 2050», г. Астана, с. 31-35, 2014;

9. Александров А.В., Метлинов А.Д. «О реализации и свойствах хеш-функций, основанных на *XOR*-свертке блоков симметричной рюкзачной криптосистемы с общей памятью» // V Всероссийская научно-техническая конференция ИКВО НИУ ИТМО «Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур», г. Санкт-Петербург, с. 13-16, 2014;

10. Метлинов А.Д. «Передача сообщений на основе схемы *SMT LSS*» // Инновации в науке, Аэтерна, г. Уфа, сборник научных трудов, том 1, с. 3-6, 2014;

11. Александров А.В., Метлинов А.Д. «О симметричных рюкзачных криптографических системах с разреженной плотностью укладки» // Пятая международная научная конференция «Современные методы и проблемы теории операторов и гармонического анализа и их приложения V» в г. Ростов-на-Дону, издательский центр ДГТУ, с. 150-151, 2015;

12. Метлинов А.Д. «Скоростные характеристики симметричной рюкзачной криптосистемы с общей памятью и плотностью укладки больше единицы. *NIST* - тестирование» // Сборник научных трудов III Международной научно-практической конференции «Информационная безопасность в свете Стратегии Казахстан - 2050», г. Астана, с. 247-252, 2015;

13. Метлинов А.Д. «О скоростных особенностях и *NIST*-тестировании симметричной рюкзачной криптографической системы с общей памятью» // Сборник трудов XI Международной научной конференции «Перспективные технологии в средствах передачи информации», г. Суздаль, 2015.

Подписано в печать 19.03.18.
Формат 60×84/16. Усл. печ. л. 1,0. Тираж 100 экз.
Издательство Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
600000, Владимир, ул. Горького, 87.