ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ САНКТ-ПЕТЕРБУРГСКОГО ИНСТИТУТА ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РОССИЙСКОЙ АКАДЕМИИ НАУК ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета 05.10.2017 г. № 1

О присуждении Биричевскому Алексею Романовичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 25 июля 2017 г., протокол № 1 диссертационным советом Д 002.199.01 на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержден приказом Рособрнадзора номер 2472-618 от 8 октября 2010 года.

Соискатель Биричевский Алексей Романович, 1987 года рождения, в 2010 г. с отличием окончил ГОУ ВПО «Сыктывкарский государственный университет» по специальности «Комплексная защита объектов информатизации» (диплом № ВСА 0509633), в 2015 г. окончил заочную аспирантуру в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН). Справка о сдаче кандидатских экзаменов № 14/204 выдана 29 декабря 2016 г. Федеральным государственным бюджетным учреждением науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН). В настоящее время Биричевский Алексей Романович работает ведущим инженером сектора телекоммуникации и связи отдела информатизации Отделения – Национального банка Северо-западного главного управления Центрального банка Российской Федерации.

Диссертация выполнена Федеральном государственном бюджетном учреждении

науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН).

Научный руководитель – доктор технических наук, профессор МОЛДОВЯН Николай Андреевич, основное место работы: Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), заведующий лабораторией криптологии.

Официальные оппоненты:

ЕМЕЛИН Вадим Иванович, доктор технических наук, старший научный сотрудник, главный научный сотрудник акционерного общества «Научно-исследовательский институт «Вектор» г. Санкт-Петербург;

ТАТАРНИКОВА Татьяна Михайловна, доктор технических наук, доцент, профессор кафедры безопасности информационных систем ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения» дали положительные отзывы на диссертацию.

Ведущая организация – Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна», г. Санкт-Петербург в своем положительном отзыве, подписанном Васильевой Елизаветой Константиновной, кандидатом технических наук, доцентом, заместителем заведующего кафедрой интеллектуальных систем и защиты информации, Вагнер Викторией Игоревной, кандидатом технических наук, доцентом кафедры интеллектуальных систем и защиты информации и утвержденном Макаровым Авиниром Геннадьевичем, доктором технических наук, профессором, проректором по научной работе ФГБОУ ВО «Санкт-Петербургский государственный университет промышленных технологий и дизайна», указала, что в целом диссертационная работа А.Р. Биричевского представляет собой завершенную научно-исследовательскую работу, выполненную на актуальную тему, отличается научной новизной и практической значимостью полученных результатов. Автором в диссертации сформулирована и решена важная научно-техническая задача расширения функциональности защищенных мобильных операционных систем.

Соискателем разработан метод аутентификации пользователей с использованием одноразовых паролей, генерируемых с помощью алгебраического алгоритма псевдовероятностного защитного преобразования, предложены метод противодействия активной отладке программного обеспечения с использованием псевдовероятностного защитного преобразования для введения ложных веток кода, метод хранения ключей шифрования, основанный на применении псевдовероятностного защитного преобразования для обеспечения возможности сокрытия наличия резервных серий ключей. Текст автореферата полностью соответствует содержанию диссертации. Диссертационное исследование «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем» является научно-квалификационной работой и соответствует критериям, изложенным в п. 9 “Положения о присуждении ученых степеней”, утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г., предъявляемых к кандидатским диссертациям, а его автор Биричевский Алексей Романович заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 17 опубликованных работ, в том числе по теме диссертации 12 работ, опубликованных в рецензируемых научных изданиях 3 работы, из них опубликованных в изданиях, рекомендуемых ВАК РФ – 3.

Основные научные результаты опубликованы в 12 научных трудах общим объемом 2,54 п.л., из которых 1,12 п.л. выполнены в соавторстве, а 1,42 п.л. – лично. Наиболее значимые работы по теме диссертации:

1. **Молдовян Н.А., Биричевский А.Р., Мондикова Я.А**. Отрицаемое шифрование на основе блочных шифров // Информационно управляющие системы. № 5. 2014. С. 80-86. *Личный вклад соискателя – 55%.*

2. **Биричевский А.Р., Молдовян Н.А., Березин А.Н., Рыжков А.В.,** Способ отрицаемого шифрования. // Вопросы защиты информации: Науч.-практ. журн. Москва:ФГУП "ВИМИ", 2013. Вып. 2 (101). С. 18-21. *Личный вклад соискателя – 35%.*

3. **Биричевский А.Р.** Универсальная мобильная операционная система с подсистемами аутентификации и защиты информации на основе

псевдовероятностного преобразования // Труды СПИИРАН. СПб.: Наука, 2016. №3. С.128-138.

4. **Биричевский А.Р.** Отрицаемое шифрование как механизм защиты приложений от отладки // Комплексная защита объектов информатизации и измерительные технологии: сб. науч. тр. Всероссийской науч.- практической конф. с международным участием. 16-18 июня 2014. -СПб.: Изд-во Политех. ун-та, 2014, С.8-12.

5. **Биричевский А.Р.** Способ применения отрицаемого шифрования для хранения ключей // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2015 г.: Материалы конференции / СПОИСУ. – СПб. 2015. С. 98-99.

Оригинальность содержания диссертации составляет не менее 91% от общего объёма текста; цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем учёной степени в соавторстве без ссылок на соавторов не выявлено. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют.

На автореферат диссертации поступило 7 отзывов, все отзывы положительны:

1) Федеральное государственное бюджетное образовательное учреждение высшего образования «Омский государственный университет им. Ф.М. Достоевского». Отзыв составил проректор по научной работе, д.т.н., профессор Белим С.В. Замечания: в автореферате не достаточно полно описан разработанный метод аутентификации пользователей системы, обеспечивающий защиту от принуждающей атаки. В частности не описан процесс генерации файла шифртекстов.

2) Федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный университет». Отзыв составил заведующий кафедрой радиофизики и электроники, д.ф.-м.н., профессор Бычков И.В. Замечания: в автореферате достаточно сложное описание алгоритма аутентификации пользователей на одноразовых паролях с защитой от принуждающей атаки. В данной части автореферата стоило предусмотреть блок-схему.

3) Федеральное государственное бюджетное образовательное учреждение высшего образования «Сыктывкарский государственный университет имени Питирима Сорокина». Отзыв составил доцент кафедры информационной безопасности института точных наук и информационных технологий, к.ф.-м.н., доцент Гольчевский Ю.В. Замечания: в автореферате не достаточно полно описан алгоритма аутентификации пользователей. Из автореферата сложно понять каким образом был сгенерирован файл хранилища шифротекстов.

4) Публичное акционерное общество «Ростелеком». Отзыв составил ведущий специалист отдела информационной безопасности, к.т.н., Глабай С.Н. Замечания: в предложенном алгоритме псевдовероятностного защитного преобразования предлагается применять устаревший стандарт шифрования ГОСТ 28147-89.

5) Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого». Отзыв составил Профессор кафедры «Информационная безопасность компьютерных систем», д.т.н., заслуженный деятель наук РФ, профессор Зегжда П.Д. Замечания: при вычислении временных паролей (стр.7) проводится применение операции XOR для парольной фразы и вектора инициализации, хотя они имеют различную длину; при описании модели разработанной защищенной операционной системы для мобильных устройств рассмотрены методы защиты от статического и активного анализа, но не указано, как защитить данные аутентификации на стороне клиента; в работе присутствуют ссылки на использование алгоритма ГОСТ 28147-89, хотя в настоящее время используется более современный вариант (ГОСТ Р 34.12-2015); отмечается некоторая небрежность оформления, а именно, отдельные параметры формул не раскрываются, и их смысл можно извлечь только из контекста.

6) Федеральное государственное бюджетное образовательное учреждение высшего образования "Государственный университет морского и речного флота имени адмирала С.О. Макарова". Отзыв составил заведующий кафедрой «Комплексное обеспечение информационной безопасности», д.т.н., доцент Соколов С.С. Замечания: не приводятся численные значения производительности разработанных алгоритмов псевдовероятностного защитного преобразования; в работе рассматривается

применение стандарта ГОСТ 28147-89, хотя принят новый стандарт блочного шифрования ГОСТ Р 34.12-2015.

7) Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина). Отзыв составил заведующий кафедрой «Информационная безопасность», к.т.н., доцент Воробьев Е.Г. Замечания не отмечались.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., старший научный сотрудник Емелин В. И. является известным ученым в области информационной безопасности и защиты информации; д.т.н., доцент, Татарникова Т. М. – известный специалист в области информационной безопасности информационных систем; ведущая организация, федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна», является известным в России образовательным учреждением, осуществляет подготовку кадров высшей квалификации по многим направлениям, в том числе по специальности «Информационная безопасность».

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработаны методы и алгоритмы псевдовероятностного защитного преобразования и методы реализации защитных функции ОС на основе последнего.

предложены:

метод аутентификации пользователей с использованием одноразовых паролей, генерируемых с помощью алгебраического алгоритма псевдовероятностного защитного преобразования, который обеспечивает защиту от принуждающих атак;

метод псевдовероятностного защитного преобразования информации и алгоритм на его основе, обеспечивающий защиту информации от несанкционированного доступа в случае атак с принуждением;

метод защиты программного обеспечения от дизассемблирования, основанный на введении ложных веток кода с помощью псевдовероятностного защитного преобразования кода;

метод противодействия активной отладке программного обеспечения, основанный на введении ложных веток кода с использованием псевдовероятностного защитного преобразования;

метод хранения ключей шифрования, основанный на применении псевдовероятностного защитного преобразования и обеспечивающий возможность сокрытия наличия резервных серий ключей;

доказана перспективность использования псевдовероятностного защитного преобразования информации для встраивания новых защитных функций в операционные системы, расширяющих функциональность защищенных операционных систем в плане обеспечения защиты информации от несанкционированного доступа в случае атак с принуждением.

Теоретическая значимость исследования обоснована тем, что:

доказаны сформулированные в работе теоретические утверждения с использованием формальных математических доказательств.

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов)

использованы аппарат и методы алгебры, теории вероятности, дискретной математики, теории чисел, теории информационной безопасности;

изложено описание новых методов псевдовероятностного защитного преобразования и их применения в подсистеме обеспечения информационной безопасности мобильных операционных систем;

раскрыты проблема расширения функциональности средств защиты информации, обеспечения переносимости программных средств защиты информации на различные типы мобильных устройств (на различные типы технических платформ) и встраивания механизмов защиты от атак с принуждением;

изучены особенности реализации существующих защищенных мобильных операционных систем на примере операционных систем для смарт-карт;

проведена модернизация существующих методов встраивания защитных функции в подсистему безопасности мобильных операционных систем.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены (указать степень внедрения) следующие результаты диссертационной работы:

– способы практического применения производительных алгоритмов псевдовероятностного защитного преобразования в операционных системах;

– методы аутентификации пользователей с использованием алгоритмов псевдовероятностного защитного преобразования для защиты от принуждающей атаки;

внедрены в учебный процесс на кафедре «Информационная безопасность» Сыктывкарского государственного университета имени Питирима Сорокина при подготовке студентов по специальности «090900 – Информационная безопасность» на дисциплинах «Информационная безопасность автоматизированных систем», «Программно-аппаратная защита информация»;

– методы защиты программного обеспечения от дизассемблирования, основанные на введении ложных веток кода с помощью псевдовероятностного защитного преобразования кода;

– метод хранения ключей шифрования, основанный на применении псевдовероятностного защитного преобразования для обеспечения возможности сокрытия наличия резервных серий ключей;

используются в работе специалистами ООО «Крейф»; ООО «Крейф» занимается разработкой перспективных средств криптографической защиты информации;

определены возможности и перспективы практического использования полученных результатов диссертации при разработке эффективных защищенных мобильных операционных систем;

создана алгоритмическая основа расширения защитных функций операционных систем и модель защищенной мобильной операционной системы, обладающей повышенным уровнем безопасности;

представлены предложения и направления для дальнейших научных исследований, в основу которых могут быть положены разработанные методы построения и применения псевдовероятносного защитного преобразования.

Оценка достоверности результатов исследования выявила:

достоверность полученных результатов подтверждена проведением всестороннего анализа работ по исследуемой проблеме, корректным применением научно-методического аппарата в виде использованных методов и теорий, апробацией основных результатов диссертации в печатных трудах и докладах на международных и всероссийских конференциях;

теория построена на известных методах защитных преобразований информации, основанных вычислительно сложных задачах, согласуется с опубликованными частными результатами других исследователей;

идея базируется на анализе работ отечественных и зарубежных исследователей в области защитных преобразований информации;

использованы вычислительные эксперименты для проверки теоретических данных по разработке алгоритмов псевдовероятностного защитного преобразования;

установлено качественное и количественное соответствие результатов вычислительных экспериментов с теоретически рассчитанными значениями.

Личный вклад соискателя состоит в:

– анализе функциональных возможностей и особенностей реализации существующих мобильных операционных систем и на его основе разработать модель угроз информационной безопасности объекта исследования, архитектуру и программный код универсальной защищенной операционной системы для мобильных систем;

– разработке методов аутентификации пользователей, стойких к принуждающим атакам;

– разработке методов защитного преобразования передаваемой по открытым каналам информации, стойких к атакам с принуждением пользователя раскрыть ключ защитного преобразования;

– разработке методов защиты программного обеспечения от дизассемблирования;

– разработка метода защиты хранимой информации, стойкого к атакам с принуждением пользователя раскрыть ключ защитного преобразования;

– подготовке экспериментальных стендов для проведения испытаний разработанных методов;

– подготовке основных публикаций по выполненной работе.

Диссертационный совет считает, что Биричевский А.Р. в своей диссертационной работе решил задачу встраивания механизмов защиты информации на различные типы мобильных устройств за счет разработки методов и алгоритмов псевдовероятностного защитного преобразования, имеющую важное социально-экономическое и хозяйственное значение.

На заседании 05.10.2017 г. диссертационный совет принял решение присудить Биричевскому А.Р. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 20 человек, из них 6 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 20, против нет, недействительных бюллетеней нет.

Зам. председателя диссертационного совета
доктор технических наук,
профессор Ронжин Андрей Леонидович

Ученый секретарь диссертационного совета
кандидат технических наук Зайцева Александра Алексеевна
05.10.2017 г.