ЗАКЛЮЧЕНИЕ ОБЪЕДИНЕННОГО ДИССЕРТАЦИОННОГО СОВЕТА Д 999.121.03, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ М. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» ФЕДЕРАЛЬНОГО АГЕНТСТВА СВЯЗИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО АВТОНОМНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ» МИНИСТЕРСТВА ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ «ВОЕНМЕХ» ИМ. Д.Ф. УСТИНОВА» МИНИСТЕРСТВА ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 20 декабря 2017 г. № 7

О присуждении Тихонову Сергею Владимировичу, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Исследование и разработка модификаций аппаратно-реализованных защитных блоковых преобразований, устойчивых к побочным атакам по цепям электропитания» по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность принята к защите 18 октября 2017 года, протокол № 6 объединенным диссертационным советом Д 999.121.03, созданном на базе федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» Федерального агентства связи, федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» Министерства образования и

науки Российской Федерации, федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» Министерства образования и науки Российской Федерации, 191186, Санкт-Петербург, наб. реки Мойки, д. 61, приказ № 44/нк от 30 января 2017 года.

Соискатель Тихонов Сергей Владимирович, 1989 года рождения, в 2013 году соискатель окончил федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича".

В 2017 году окончил освоение программы подготовки научно-педагогических кадров в аспирантуре федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича».

Диссертация выполнена на кафедре защищенных систем связи федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» Федерального агентства связи.

Научный руководитель – доктор технических наук, Коржик Валерий Иванович, федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», кафедра безопасности информационных систем, профессор кафедры.

Официальные оппоненты:

1. Молдовян Николай Андреевич, доктор технических наук, профессор, федеральное государственное бюджетное учреждение науки «Санкт-Петербургский институт информатики и автоматизации Российской академии

наук», научно-исследовательский отдел проблем информационной безопасности, заведующий лабораторией криптологии;

2. Левина Алла Борисовна, кандидат физико-математических наук, доцент, федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», кафедра проектирования и безопасности компьютерных систем, доцент кафедры

дали положительные отзывы на диссертацию.

Ведущая организация Закрытое акционерное общество «Институт телекоммуникаций», г. Санкт-Петербург, в своем положительном заключении, подписанном Овчинниковым Г.Р., канд. техн. наук, доц., заместителем начальника НИО-1, Аванесовым М.Ю., канд. техн. наук, научным секретарём, утверждённым Присяжнюком С.П., д-м техн. наук, проф., генеральным директором, указала, что в диссертации раскрываются новые аспекты реализации побочных атак по цепям электропитания и предлагается весьма эффективный метод защиты от них (подходящий для российских шифров типа ГОСТ), тема является чрезвычайно важной и актуальной. Результаты проведённого исследования являются востребованными научными и проектными организациями, занимающимися вопросами обеспечения информационной безопасности. Достоверность полученных результатов и научных положений диссертации определяется корректностью поставленной научной задачи, подробным анализом состояния исследований в этой теме, строгими аналитическими доказательствами, а также результатами проведённого компьютерного моделирования и экспериментов. Совокупность полученных основных научных результатов позволяет сделать вывод о достижении соискателем цели своего диссертационного исследования, а именно повышении безопасности информационно-коммуникационных технологий в части реализации защитных преобразований, выполняемых интегральными чипами. Диссертация выполнена на высоком научном уровне и содержит новые, достоверные и значимые результаты, которые несомненно имеют значение для современного

развития информационно-коммуникационных технологий и обеспечения их информационной безопасности, а также могут быть непосредственно использованы для защиты аппаратных реализаций блоковых защитных преобразований, и прежде всего российских шифров ГОСТ. Личный вклад автора в получении результатов не вызывает сомнений. Все положения, выносимые на защиту, прошли апробацию на научных семинарах и конференциях. Они опубликованы в достаточной степени в рецензируемых изданиях, рекомендованных ВАК и непосредственно относящихся к тематике диссертации. Представленная диссертация является законченной научно-квалификационной работой, в которой содержится решение научной задачи по разработке метода, позволяющего обеспечить защиту аппаратных реализаций защитных блоковых преобразований от побочных атак по цепям электропитания, имеющей значение для развития отрасли информационной безопасности и защиты информации. Диссертация соответствует п. 9 «Положения о порядке присуждения ученых степеней», а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 13 опубликованных работ, в том числе по теме диссертации 13 работ, опубликованных в рецензируемых научных изданиях 6. Диссертация не содержит недостоверных сведений об опубликованных соискателем ученой степени работах. Помимо 6 работ в рецензируемых научных изданиях, соискатель имеет 6 – в сборниках научных статей, трудов, тезисов докладов и материалах конференций; 1 – отчет по НИР. Из них 7 работ опубликовано соискателем без соавторства. Общий объем авторского вклада в работы составляет 10,86 печ.л. из общего количества 26,14 печ.л.

Наиболее значительные научные работы по теме диссертации:

1. Тихонов, С.В. О возможности взлома аппаратной реализации шифра ГОСТ / В.И. Коржик, С.В. Тихонов // Проблемы информационной безопасности. Компьютерные системы. – 2012. – № 3. – С. 53-62 (из перечня ВАК).

2. Тихонов, С.В. Экспериментальное исследование утечек информации, обрабатываемой интегральными чипами, по цепи электропитания / С.В. Тихонов // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 1. – С. 82-93 (из перечня ВАК).

3. Тихонов, С.В. Экспериментальное исследование возможности взлома по цепям электропитания аппаратно реализованных блоковых шифров / С.В. Тихонов // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 2. – С. 106-117 (из перечня ВАК).

4. Тихонов, С.В. Универсальный метод защиты блочных шифров от побочных атак по цепям питания / С.В. Тихонов // Проблемы информационной безопасности. Компьютерные системы. – 2017. – № 3. – С. 70-81 (из перечня ВАК).

5. Тихонов, С.В. Метод защиты аппаратной реализации шифра ГОСТ от атаки измерения потребляемой мощности в цепи питания / С.В. Тихонов, В.И. Коржик //Проблемы информационной безопасности. Компьютерные системы. – 2013. – № 3. – С. 62-72 (из перечня ВАК).

6. Тихонов, С.В. Исследование основных направлений создания средств и систем защиты электронных документов нового поколения / Отчет о НИР: АО "Научные приборы"; рук.: Позднышев М.М.; исполн.: Бородинов А.Г., Тихонов С.В. [и др.]. – СПб., 2014. – 323 с. – Библиогр.: с. 249–280. – Инв. № 231-АО от 16.11.2015 г.

На диссертацию и автореферат поступили отзывы:
ведущей организации ЗАО «Институт телекоммуникаций»; официального оппонента Молдовяна Н.А.; официального оппонента Левиной А.Б.; Макарова С.Б., д-а техн. наук, проф., директора института физики, нанотехнологий и телекоммуникаций Санкт-Петербургского государственного политехнического университета; Воробьёва Е.Г., канд. техн. наук, доц., заведующего кафедрой «Информационная безопасность» Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина); Мазепы В.А., канд. техн. наук, доцента кафедры боевого применения

средств связи, военного института ДПО ВУНЦ ВМФ «Военно-морская академия»; Авсентьтева О.С., д-ра техн. наук, проф., профессора кафедры информационной безопасности Воронежского института МВД России; Хисамова Ф.Г., д-ра техн. наук, проф., проректора по научной работе НЧОУ ВО «Кубанский институт информзащиты»; Хохлова Н.С., д-ра техн. наук, проф., профессора кафедры, Глушакова А.Н., канд. техн. наук, доц., доцента кафедры инфокоммуникационных систем и технологий Воронежского института МВД России; Борисенко Н.П., канд. техн. наук, доц., сотрудника Академии Федеральной службы охраны Российской Федерации; Зимы В., канд. техн. наук, доц., профессора кафедры систем сбора и обработки информации Военно-космической академии имени А.Ф. Можайского. Все отзывы положительны, но имеют критические замечания:

1) Недостаточно полно раскрыты преимущества предложенного метода защиты (например, в плане скорости выполнения и требующихся дополнительных ресурсов чипа) по сравнению с известными аналогами; не была в полной мере обоснована оптимальность (например, с точки зрения защищённости, скорости выполнения, универсальности) предложенной структуры узлов предобработки и постобработки, составляющих разработанный метод защиты; необходимо было более детально (как аналитически, так и экспериментально) проработать вопрос защищённости предложенного метода защиты.

2) Изложение ряда аспектов диссертационного исследования в автореферате является недостаточным, например, было необходимо привести более полное описание и обоснование разработанной архитектуры измерительной установки, предназначенной для снятия данных об энергопотреблении чипа (включая описание назначения её компонентов, требований к полосе пропускания и чувствительности); требовалось детальнее описать условия проведения натурного эксперимента; подробнее пояснить причины по которым модель расстояния Хэмминга будет не эффективной при анализе утечки от некоторых операций, и причины большей эффективности использования в атаке подхода с расчетом корреляционных векторов по сравнению с ковариационными; детальнее пояснить

условия получения результатов приведённых в 1-3 таблицах, а также представить более полный их анализ.

3) В работе встречаются орфографические, грамматические, оформительские, стилистические ошибки, опечатки, а также ряд неточностей, например: некорректно сформулирован второй пункт научной новизны – вместо «учтены новые особенности энергопотребления интегральных чипов», необходимо было бы написать, что «учтены новые особенности зависимостей энергопотребления интегральных чипов от обрабатываемых данных»; недостаточно полно раскрыто понятие «рациональности» разрабатываемой конструкции аппаратно-программного комплекса, предназначенного для анализа «утечек» информации по цепям электропитания, а также понятие «утечки»; на 18-й странице говорится, что перебор 248 вариантов ключа оказывается вычислительно нереализуемой задачей, а 245 реализуемой с использованием мощных вычислительных ресурсов, – разница в 8 раз не представляется чрезвычайно большой, поэтому правильно было бы сказать, что перебор 248 вариантов ключа является чрезвычайно трудно реализуемой задачей с точки зрения вычислений (а не невозможной); при обосновании актуальности темы, следовало конкретизировать, что для создания полной копии невскрываемого чипа, помимо взлома, выполняющегося на нём защитного преобразования, атакующему необходимо детальное знание выполняемой чипом программы; при описании научной новизны и практической значимости указано, что для снятия данных об энергопотреблении чипа, вместо осциллографа, предлагается использовать АЦП – учитывая тот факт, что АЦП входит в состав любого осциллографа, возникает некоторая путаница; в работе следовало привести описание и результаты натурного эксперимента по взлому шифра «Кузнечик».

Выбор официальных оппонентов и ведущей организации обосновывается тем, что в круг научных интересов вышеуказанных ученых и ведущей организации входят темы, связанные с проблематикой представленной к защите диссертации, а также наличием значительного количества публикаций по

тематике диссертации, что гарантирует их способность определить научную и практическую значимость работы.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований разработаны: архитектура средства моделирования побочных атак по цепям электропитания; модель «утечки» информации, обрабатываемой интегральным чипом, по цепи электропитания, основанная на результатах проведённого комплекса измерений; модель побочных атак по цепям электропитания на аппаратные реализации шифров ГОСТ; метод защиты преобразований на интегральных чипах от побочных атак по цепям электропитания; предложены конструкция аппаратно-программного комплекса, предназначенного для анализа «утечек» информации по цепям электропитания; идея метода защиты от атак по цепям электропитания аппаратно реализованных защитных блоковых преобразований; доказана уязвимость блочных шифров описанных стандартом ГОСТ Р 34.12-2015 к побочным атакам по цепям электропитания; преимущество использования, при практической реализации атаки DPA, подхода с расчётом корреляционных векторов, по сравнению с ковариационными.

Теоретическая значимость исследования обоснована тем, что доказана возможность реализации побочных атак по цепям электропитания применительно к российским шифрам ГОСТ 34.12-2015; большая эффективность, при реализации атаки DPA, использования подхода с расчётом корреляционных векторов, по сравнению с ковариационными; применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) использованы сбор, систематизация и анализ научно-технической информации; системный, причинно-следственный и сравнительный анализ; методология программирования, компьютерное моделирование и натурный эксперимент; изложены элементы теории побочных атак по цепям электропитания: физические основы таких атак, их математические модели и аспекты практической реализации, характеристика основных методов защиты от подобных атак; раскрыты особенности зависимостей энергопотребления чипов от

выполняемых операций и обрабатываемых данных; изучены влияние утечек информации по цепям электропитания, вызванных выполнением различных операций на эффективность реализации атаки DPA; проведена модернизация теоретической модели побочных атак по цепям электропитания и методов защиты от них.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что разработаны и внедрены (указать степень внедрения): рациональная конструкция измерительной установки, предназначенной для сбора данных об энергопотреблении микрочипов; алгоритм предварительной обработки данных об энергопотреблении микрочипов с возможностью автоматизации его выполнения; результаты исследования величины утечек информации по цепи питания микроконтроллеров фирмы Atmel для уточнения требований к разрабатываемым электронным идентификационным документам и повышения надёжности функционирования оборудования со встроенными блоками электронной идентификации на предприятии АО "Научные приборы"; определены перспективы использования модели «утечки» информации по цепи электропитания для оценки эффективности реализации побочных атак по цепям электропитания и методов защиты от них; создана модель побочной атаки по цепям электропитания на аппаратные реализации российских шифров ГОСТ, позволяющая осуществить их взлом за обозримое время; метод защиты аппаратных реализаций защитных блоковых преобразований от атаки DPA, обладающий относительно низкими требованиями к дополнительным аппаратным ресурсам чипа, простотой реализации и невысокой стоимостью, а также широкой универсальностью относительно защищаемых алгоритмов; представлена архитектура измерительной установки, позволяющей существенно снизить требуемые вложения в оборудование, необходимое для реализации побочных атак по цепям электропитания.

Оценка достоверности результатов исследования выявила для экспериментальных работ результаты получены при помощи детально описанной методики, на измерительной системе, компоненты которой доступны в открытой

продаже, могут быть многократно воспроизведены и проверены; теория основана на развитии известных подходов; строгих, проверяемых, доказательствах, подтверждаемых компьютерным моделированием и натурным экспериментом; идея базируется на систематизации, обобщении и анализе известных подходов к реализации атак DPA и методов защиты от них, учёте полученных автором новых теоретических выводов, результатах моделирования и натурного эксперимента; использованы современные средства и методики сбора (измерений) и обработки данных об энергопотреблении анализируемых чипов.

Личный вклад соискателя состоит в обобщении и систематизации имеющихся знаний теоретических и практических аспектов реализации атак по цепям электропитания, а также методов защиты от них; доработке теоретической модели атак по цепям электропитания (при этом как фундаментальных частей так и прикладных, касающихся, например, реализации атаки DPA в отношении российских шифров ГОСТ); разработке экспериментального стенда, предназначенного для снятия данных об энергопотреблении чипов; анализе и обработке экспериментальных данных, уточнении на их основе модели атак по цепям электропитания; реализации натурного эксперимента взлома российского шифра; разработке метода защиты от побочных атак по цепям электропитания; публикации основных и частных научных результатов (лично и в соавторстве); апробации полученных результатов на конференциях; внедрении и реализации основных научных результатов.

Диссертация «Исследование и разработка модификаций аппаратно-реализованных защитных блоковых преобразований, устойчивых к побочным атакам по цепям электропитания» соответствует требованиям, установленным п. 14 «Положения о присуждении ученых степеней» и научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность, отрасль науки – техническая науки. Диссертация соответствует пунктам 3, 7, 13 паспорта специальности 05.13.19.

На заседании 20 декабря 2017 года диссертационный принял решение присудить Тихонову С.В. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 17 человек, из них 5 докторов наук (отдельно по каждой специальности рассматриваемой диссертации), участвовавших в заседании, из 25 человек, входящих в состав совета, проголосовали: за 16, против нет, недействительных бюллетеней 1.

Председатель диссертационного совета,
доктор технических наук, профессор

Бачевский Сергей Викторович

Ученый секретарь диссертационного совета,
кандидат технических наук

Владыко Андрей Геннадьевич

22 декабря 2017 года