ЗАКЛЮЧЕНИЕ ОБЪЕДИНЕННОГО ДИССЕРТАЦИОННОГО СОВЕТА Д 999.121.03, СОЗДАННОГО 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 ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА ТЕХНИЧЕСКИХ НАУК

аттестационное дело № _____

решение диссертационного совета от 12 декабря 2018 г. № 9

О присуждении Таранову Сергею Владимировичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методы обеспечения целостности информации на основе вейвлетных преобразований для защиты средств хранения информации» по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность принята к защите 10 октября 2018 года, протокол № 6 объединенным диссертационным советом Д 999.121.03, созданным 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 Таранов Сергей Владимирович, 1991 года рождения, работает ассистентом кафедры проектирования и компьютерной безопасности в федеральном государственном автономном образовательном учреждении высшего образования "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики" Министерства науки и высшего образования Российской Федерации.

В 2014 году соискатель окончил федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики".

В 2018 году окончил освоение программы подготовки научно-педагогических кадров в аспирантуре федерального государственного автономного образовательного учреждения высшего образования "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики".

Диссертация выполнена в федеральном государственном автономном образовательном учреждении высшего образования "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики" Министерства науки и высшего образования Российской Федерации на кафедре проектирования и безопасности компьютерных систем.

Научный руководитель – кандидат физико-математических наук, доцент, Левина Алла Борисовна, основное место работы: федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики", кафедра проектирования и безопасности компьютерных систем, доцент.

Официальные оппоненты: 1. Молдовян Александр Андреевич, доктор технических наук, профессор, основное место работы: федеральное государственное бюджетное учреждение науки "Санкт-Петербургский институт информатики и автоматизации Российской академии наук", лаборатория безопасности информационных систем, главный научный сотрудник; заместитель генерального директора по информационной безопасности; 2. Макаров Антон

Александрович, доктор физико-математических наук, основное место работы: федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет», кафедра параллельных алгоритмов, доцент, дали положительные отзывы на диссертацию.

Ведущая организация Общество с ограниченной ответственностью "Удостоверяющий центр ГАЗИНФОРМСЕРВИС", Санкт-Петербург, в своем положительном заключении, подписанном Кирюшкиным Сергеем Анатолиевичем, канд. техн. наук, советником генерального директора, Станкевич Татьяной Леонидовной, канд. техн. наук, ведущим специалистом, утвержденном Кустовым Владимиром Николаевичем, д-ром техн. наук, проф., генеральным директором, указала, что диссертационная работа Таранова С.В. является законченной научно-квалификационной работой, посвященной вопросам обеспечения целостности информациии в средствах хранения данных при наличии алгебраических манипуляций. В работе предлагаются новые методы обеспечения целостности, построенные на основе линейных и нелинейных вейвлетных кодов, которые позволяют обеспечить защиту от атак на основе алгебраических манипуляций, в том числе при неравномерном распределении входных кодовых слов. В диссертации Таранова С.В. предложен ряд рекомендаций по использованию разработанных методов обеспечения целостности, которые включают использование их для обеспечения целостности кэш памяти микропроцессоров, оперативной памяти, NAND флеш памяти в SSD-дисках. Достоверносць полученных результатов и научных положений диссертационной работы определяется корректностью поставленной научной задачи, математическими обоснованиями, а также результатами компьютерного моделирования. Диссертация соответствует п. 9 "Положения о присуждения ученых степеней", а ее автор заслуживает присуждения ему 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 17. Из них опубликовано в рецензируемых научных изданиях – 3. Диссертация не содержит недостоверных сведений об опубликованных соискателем работах. Помимо 3-х работ в рецензируемых научных изданиях, соискатель ученой степени имеет 9 публикаций в изданиях, входящих в международную систему цитирования Scopus, 5 – в сборниках научных трудов и

материалов конференций. Общий объём авторского вклада в работы составляет 3,0 п.л. из общего количества 5,0 п.л.

Наиболее значительные научные работы по теме диссертации:

1. Таранов, С.В. Построение линейных и надежных кодов на основе коэффициентов масштабирующих функций вейвлетных преобразований / А.Б. Левина, С.В. Таранов // Сибирский журнал индустриальной математики. — 2015. — Т. 18, № 63. — С. 49–56.

2. Taranov, S.V. Investigation of influence of encoding function complexity on distribution of error masking probability / A.B. Levina, S.V. Taranov // Научно-технический вестник информационных технологий, механики и оптики. — 2016. — Т. 16, № 2 (102). — С. 331–337.

3. Taranov, S.V. Algorithms of constructing linear and robust codes based on wavelet decomposition and its application / A.B. Levina, S.V. Taranov // Lecture Notes in Computer Science. — 2015. — Vol. 9084. — pp. 247–258.

4. Taranov, S.V. New Construction of Algebraic Manipulation Detection Codes Based on Wavelet Transform / A.B. Levina, S.V. Taranov // Proceedings of the 18th Conference of Open Innovations Association FRUCT. — 2016. — pp. 187–192.

5. Taranov, S.V. Creation of codes based on wavelet transformation and its application in ADV612 chips / A.B. Levina, S.V. Taranov // International Journal of Wavelets, Multiresolution and Information Processing. — 2017. — Vol. 15, no. 2. — p. 1750014.

На диссертацию и автореферат поступили отзывы: официального оппонента Молдовяна А.А.; официального оппонента Макарова А.А.; ведущей организации ООО "Удостоверяющий центр ГАЗИНФОРМСЕРВИС"; Овсянникова Е.П., канд. тех. наук, доц., доцента кафедры аэрокосмических компьютерных и программных систем (кафедра 14) Санкт-Петербургского государственного университета аэрокосмического приборостроения; Катаржнова А.Д., канд. техн. наук, с.н.с., специалиста по противодействию техническим разведкам ЗАО "Эврика"; Стенюкова Н.С., канд. техн. наук, в.н.с. НИО "Вектор-Н1" АО НИИ "Вектор"; Ежова С.Н., канд. тех. наук, доц., заместителя декана по научной работе Санкт-Петербургского государственного электротехнического университета "ЛЭТИ" им. В.И. Ульянова (Ленина); Кустова Д.В., руководителя сектора разработки телевизионного оборудования АО "Диаконт"; Коробейникова А.Г., д-ра техн. наук, проф., заместителя директора по науке Института земного магнетизма,

ионосферы и распространения радиоволн им. Н.В. Пушкова Российской академии наук; Петрова Ю.В., канд. техн. наук, доц., доцента кафедры "Радиоэлектронные системы" Балтийского государственного технического университета "ВОЕНМЕХ" им. Д.Ф. Устинова; Бызова А.Н., канд. техн. наук, начальника лаборатории АО "Заслон". Все отзывы положительные, но имеются следующие критические замечания:

1) Неполное сравнение разработанных методов обеспечения целостности с аналогами. В частности, в диссертации производится оценка вероятности необнаруживаемой ошибки, но не показаны вероятности битовой и блоковой ошибки (BER и FER). Нет экспериментальных сравнений с отечественными методами обнаружения ошибок, способными работать при неравномерном распределении входных кодовых слов, например, с универсальным методом кодирования, предложенным Л.М. Финком и В.И. Коржиком. Не представлено сравнение со сверхточными помехоустойчивыми кодами Фарамаза Фекри.

2) Некорректное описание некоторых положений теории вейвлетных разложений в конечных пространствах. Например, имеют место неверные формулировки в определении ортогонального кратномасштабного анализа. Отсутствует подробное описание алгоритма построения дуального и комплементарного фильтров для некоторого заданного вейвлет-фильтра.

3) В диссертации присутствует частичное или неполное описание некоторых экспериментов, например, в п.п. 2.5. и 2.6 опускается описание алгоритмов, с помощью которых задавалось неравномерное распределение входных значений; в автореферате не показаны определения следующих понятий: "алгебраические манипуляции", "надежные коды", "совершенно нелинейные" и "почти совершенно нелинейные функции"; нет четкого описания преимуществ использования вейвлет разложений для разработанных методов обеспечения целостности.

4) Не показаны преимущества и недостатки при использовании стохастических функций кодирования. Нет сравнений с недерминированными вариантами функций кодирования, например, с функциями Майорана-Мак Фарланда.

Выбор официальных оппонентов и ведущей организации обосновывается их широкой известностью своими достижениями в темах, связанных с проблематикой, представленной к защите диссертации, наличием значительного количества публикаций по тематике диссертации и способностью определить научную и практическую ценность работы.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований: разработаны метод обеспечения целостности информации на основе вейвлетных разложений и преобразования Грея; метод обеспечения целостности информации на основе нелинейных вейвлетных кодов, совершенно нелинейных и почти совершенно нелинейных функций; практические рекомендации по использованию разработанных методов обеспечения целостности; предложены метод обеспечения целостности для системы сжатия и обработки видео ADV612; метод одновременного обнаружения ошибок для быстродействующей памяти (например, кэш памяти процессора, NAND флеш памяти SSD дисков); доказана уязвимость линейных помехоустойчивых кодов к алгебраическим манипуляциям; перспективность использования вейвлетных разложений для построения кодовых методов с целью защиты от атак на основе алгебраических манипуляций.

Теоретическая значимость исследования обоснована тем, что: доказаны теоремы, показывающие преимущества вейвлетных нелинейных кодов на основе PN (совершенно нелинейных) и APN (почти совершенно нелинейных) функций над аналогами при оценке вероятности маскировки ошибки и множества необнаруживаемых ошибок; эффективность использования вейвлетных разложений и дополнительных преобразований входных значений для повышения устойчивости функций кодирования к изменениям в законе распределения входных кодовых слов; применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) использованы методы оценки вероятности маскировки ошибки и множества необнаруживаемых ошибок; методы измерения показателей нелинейности функций кодирования на основе производной по направлению; методы линейной алгебры, методы математического и компьютерного моделирования; изложены элементы теории вейвлетных разложений в конечных пространствах; положения ортогонального кратномасштабного анализа в конечных полях; элементы теории совершенно нелинейных и почти совершенно нелинейных функций; раскрыты новые свойства существующих угроз обеспечения целостности для средств хранения информации; уязвимости стандартных помехоустойчивых методов кодирования к атакам на основе алгебраических манипуляций; изучены влияние неравномерного закона распределения входных значений на обнаруживающие характеристики кодовых

конструкций; связи между преобразованием входных значений, распределением входных значений и изменениями в вероятности маскировки ошибки; проведена модернизация алгоритмов оценки вероятности маскировки ошибки при неравномерном распределении входных значений; существующих схем одновременного обнаружения ошибок с помощью нелинейных и линейных вейвлетных кодов; алгоритмов обеспечения целостности информации в системе сжатия и обработки видео ADV612.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что: разработаны и внедрены методы обеспечения целостности информации на основе вейвлетных разложений; методы обнаружения ошибок, использующие вейвлетные коды 1) в научно-исследовательских работах ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», 2) в производственную деятельность ООО "ВЕСТ-ТЕР" и ООО "Технологии безопасности"; определены пределы и перспективы практического использования вейвлетных кодовых конструкций с дополнительными преобразованиями на практике; границы вероятности маскировки ошибки для тестируемых кодовых конструкций; создана практические рекомендации по использованию разработанных методов обеспечения целостности на основе вейвлетных разложений, включающие рекомендации по выбору определенных функций кодирования, преобразований входных значений; алгоритмы модификации существующих систем обнаружения ошибок; представлены предложения по дальнейшему усовершенствованию разработанных методов обеспечения целостности на основе вейвлет-преобразований, в частности, использование стохастических функций кодирования, засекречивание вейвлетной части кодового слова, разработка преобразований входных значений для вейвлетных кодов со стохастической функцией кодирования.

Оценка достоверности результатов исследования выявила: для экспериментальных работ результаты получены на общедоступном или лицензированном программном обеспечении (системы компьютерной алгебры Matlab, Sage); исходные коды, входные данные и настраиваемые параметры для всех экпериментов отражены в тексте и приложениях диссертации, что позволяет при необходимости воспроизвести результаты диссертационного исследования; теория построена на известных подходах к созданию каскадных кодовых

конструкций с помощью PN и APN функций, а также на проверенной теории вейвлетных разложений в конечных пространствах. Полученные результаты не противоречат и согласуются с опубликованными экспериментальными данными по теме диссертации; идея базируется на объединении теории вейвлетных разложений в конечных пространствах с теорией кодов, обнаруживающих алгебраические манипуляции; на анализе вероятности маскировки ошибок при неравномерном распределении входных кодовых слов; на обобщении передового опыта в области защиты от алгебраических манипуляций; использованы вейвлетные кодовые конструкции как маскирующий и защитный механизм, позволяющий снизить максимум вероятности маскировки ошибки при неравномерном распределении входных кодовых слов; установлено количественное совпадение авторских результатов с результатами, представленными в независимых источниках по данной тематике, а именно, в случаях использования кодов на основе PN и APN функций при равномерном распределении входных кодовых слов; использованы методы оценки вероятности маскировки ошибки при неравномерном распределении входных кодовых слов; модели атак на основе алгебраических манипуляций, использующие кусочные функции в качестве закона распределения для входных кодовых слов.

Личный вклад соискателя состоит в обобщении и систематизации существующих методов обеспечения целостности информации, применяемых в средствах хранения информации в случае алгебраических манипуляций; анализе существующих угроз нарушения целостности, описываемых с помощью модели алгебраических манипуляций; разработке метода обеспечения целостности на основе линейных вейвлетных кодов с дополнительным преобразованием Грея входных значений; разработке каскадного кода на основе вейвлетного линейного кода, PN и APN функций; разработке практических рекомендаций по использованию методов обеспечения целостности, полученных в диссертации; анализе и обработке экспериментальных данных по оценке вероятности маскировки ошибки при неравномерном распределении входных кодовых слов; разработке схем одновременного обнаружения ошибок для защиты быстродействующей памяти.

Диссертация «Методы обеспечения целостности информации на основе вейвлетных преобразований для защиты средств хранения информации» соответствует требованиям, установленным п. 9 «Положения о присуждении

ученых степеней» и пунктам 6 и 13 паспорта научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

На заседании 12 декабря 2018 года диссертационный совет принял решение присудить Таранову С.В. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 18 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 25 человек, входящих в состав совета, проголосовали: за – 18, против – 0, недействительных бюллетеней – 0.

Председатель диссертационного совета,
доктор технических наук, профессор

Бачевский Сергей Викторович

Ученый секретарь диссертационного совета,
кандидат технических наук

Владыко Андрей Геннадьевич

14 декабря 2018 года