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 29.09.2015 г. № _2__

О присуждении Алексееву Максиму Олеговичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методы нелинейного кодирования для повышения достоверности обработки информации» по специальности 05.13.01 – «Системный анализ, управление и обработка информации» принята к защите 23 июля 2015, протокол № 2 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 Алексеев Максим Олегович 1988 года рождения дипломный проект на тему «Пакетная передача с кодовым зашумлением» защитил в 2005 году в Санкт-Петербургском государственном университете аэрокосмического приборостроения, работает программистом в Институте высокопроизводительных компьютерных и сетевых технологий Федерального государственного автономного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» Министерства образования и науки Российской Федерации.

Диссертация выполнена на кафедре аэрокосмических компьютерных и программных систем Федерального государственного автономного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» Министерства образования и науки Российской Федерации.

Научный руководитель – доктор технических наук, профессор МИРОНЧИКОВ Евгений Тимофеевич, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», кафедра аэрокосмических компьютерных и программных систем, профессор.

Официальные оппоненты:

ЯКОВЛЕВ Виктор Алексеевич, доктор технических наук, профессор, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций имени профессора М. А. Бонч-Бруевича» (СПбГУТ), кафедра «Защищённые системы связи», профессор;

ТРИФОНОВ Пётр Владимирович, кандидат технических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого», кафедра «Распределённые вычисления и компьютерные сети», доцент

дали положительные отзывы на диссертацию.

Ведущая организация Санкт-Петербургский филиал "Научно-исследовательского и проектно-конструкторского института информатизации, автоматизации и связи на железнодорожном транспорте" (СПбФ ОАО «НИИАС»), г. Санкт-Петербург в своем положительном заключении, подписанном Кунгурцевым Вадимом Викторовичем, кандидатом технических наук, главным специалистом Службы разработки и внедрения навигационно-связных систем, Моисеевым Виктором Васильевичем, кандидатом технических наук, главным специалистом Службы разработки и проектирования систем диагностики и утверждённом Ададуровым А.С., кандидатом технических наук, директором СПбФ ОАО «НИИАС», указала, что в целом диссертационная работа М.О. Алексеева представляет собой завершенную научно-исследовательскую работу на актуальную тему повышения достоверности обработки информации в каналах со случайной структурой. Новые научные результаты, полученные диссертантом, имеют существенное значение для науки и для практики, поскольку решают задачу повышения достоверности обработки информации в каналах, которые могут быть описаны моделью канала с

алгебраическими манипуляциями. Вывод и рекомендации сопровождаются достаточными обоснованиями и доказательствами. Основные научные результаты достаточно полно опубликованы в работах соискателя. Автореферат диссертации отражает её основное содержание. Язык и стиль диссертации соответствует устоявшейся научно-технической терминологии и стилю изложения. Диссертация аккуратно оформлена. По каждой главе и работе в целом имеются содержательные выводы. Работа отвечает критериям, установленным п. 9 Положения о присуждении ученых степеней, утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 № 842, а её автор, Алексеев Максим Олегович, заслуживает присуждения ему учёной степени кандидата технических наук по специальности 05.13.01 «Системный анализ, управление и обработка информации (технические системы)».

Соискатель имеет 16 опубликованных работ, в том числе по теме диссертации 12 работ, опубликованных в рецензируемых научных изданиях 5 работ, из них опубликованных в изданиях, рекомендуемых ВАК РФ, - 5.

Основные научные результаты реализованы в 2 научно-исследовательских работах, осуществляемых ЗАО «Научные приборы» и Санкт-Петербургским государственным университетом аэрокосмического приборостроения, в 12 научных трудах общим объемом 123,85 с., из которых 3 статьи объемом 11,7 с., выполнены в соавторстве, а 9 статей объемом 112,15 с. – лично. Наиболее значительные работы по теме диссертации:

1. Громова, А. Н. Вариант алгоритма нахождения ошибок для БЧХ-кодов [Текст] / А.Н. Громова, **М.О. Алексеев** // Программные продукты и системы – Тверь: МНИИПУ. – 2010. – №2 (май). – С. 56-58.
2. **Алексеев, М.О.** Нижняя граница длины систематических равномерно надежных кодов [Текст] / М.О. Алексеев // Известия ВУЗов. Приборостроение. №8 (август), 2013. – С. 14-16.
3. **Алексеев, М.О.** Новая конструкция систематического надежного кода [Текст] / М.О. Алексеев // Известия ВУЗов. Приборостроение. – 2013. − №8 (август). − С. 24-27.

4. **Алексеев, М.О.** Об обнаружении алгебраических манипуляций с помощью операции умножения [Текст] / М.О. Алексеев // Информационно-управляющие системы. – 2014. – № 3 (июнь). – С. 103-108.
5. **Алексеев, М.О.** Защита от алгебраических манипуляций на основе операции скалярного умножения [Текст] / М.О. Алексеев // Проблемы информационной безопасности. Компьютерные системы. – 2014. – №2. – С. 47-53.
6. **Алексеев, М.О**. Пакетная передача с кодовым зашумлением. Теоретические основы и практическое применение [Текст] / М.О. Алексеев. – LAP LAMBERT Academic Publishing, 2012. – 57 с. – ISBN: 978-3-8484-1675-2.

На автореферат диссертации поступило 6 отзывов, все отзывы положительны:

1) Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. Отзыв составили профессор кафедры информационных систем, д.т.н., профессор Кудряшов Б.Д. и доцент кафедры информационных систем, к.т.н., доцент Бочарова И.Е. Замечания: с нашей точки зрения, недостатком автореферата является то, что для оценки новизны представленных результатов читатель должен хорошо ориентироваться в достаточно узкой и недавно появившейся области теории кодирования. Терминология и фундаментальные результаты теории кодов для обнаружения манипуляций были разработаны в середине 2000-х годов, в основном, М. Карповским. Из текста автореферата довольно трудно понять, какие утверждения являются новыми. Значительным усилением автореферата была бы, например, таблица с примерами сравнения характеристик новых и известных кодов. Надеемся, что такая таблица имеется в диссертации.

2) Петербургский государственный университет путей сообщения Императора Александра I. Отзыв составил заведующий кафедрой «Математика и моделирование», д.т.н., профессор Ходаковский В.А. Замечания: В качестве основной цели исследования автор выбрал разработку методов кодирования, повышающих достоверность обработки информации и обладающих меньшей вычислительной сложностью. Вместе с тем, в автореферате не приведены численные оценки

показателей степени повышения достоверности и снижения вычислительной сложности при применении разработанных методов по сравнению с известными. В автореферате автор приводит четыре положения, вынесенных на защиту, которые рассмотрены в 3, 4 главах работы. К сожалению, серьёзные результаты, изложенные во второй главе, не вошли в защищаемые результаты. Второй метод помехоустойчивого кодирования в положениях, вынесенных на защиту, назван как скалярное умножение компонентов информационного сообщения и значений случайной величины. Судя по формуле, приведенной на стр.18 автореферата, речь идет о скалярном умножении вектора на вектор, поскольку под случайной величиной автор понимает *r*-битное двоичное число.

3) Национальный минерально-сырьевой университет «Горный». Отзыв составил ассистент кафедры «Автоматизация технологических процессов и производств», к.т.н. Затуловский К.А. Замечания: в автореферате не обосновывается использование аддитивной модели ошибок. Применимость предлагаемых методов обеспечивается использованием корректной модели ошибок, при этом аддитивность реальных ошибок не является гарантированной. В автореферате не представлены примеры известных кодовых методов, обнаруживающих алгебраические манипуляции, перечисляются только математические объекты, на которых они основываются. По моему мнению, сравнение эффективности известных методов нелинейного кодирования и предлагаемых автором в автореферате представлено в недостаточной мере.

4) Институт математики им. С. Л. Соболева СО РАН. Отзыв составил ведущий научный сотрудник лаборатории совершенных комбинаторных структур, д.ф.-м.н. Соловьёва Ф.И. Замечания: в некоторых местах использована терминология, отличная от общепринятой в русскоязычной литературе. В частности, «надёжные» коды принято называть «массивными». Не представлен алгоритм обнаружения и исправления ошибок малой кратности для обобщённых систематических надежных кодов. Отсутствует наглядное сравнение предлагаемых кодов с аналогами, позволяющее сделать вывод об их эффективности. В тексте автореферата обнаружены некоторые несущественные опечатки.

5) Санкт-Петербургский филиал ОАО «РТИ». Отзыв составил директор Санкт-Петербургского филиала ОАО «РТИ», к.т.н. Миллер В.Е. Замечания: отсутствие

анализа предложенного автором метода декодирования обобщённых надёжных кодов. В автореферате отсутствуют оценки энергопотребления разработанных автором методов обнаружения ошибок в каналах со сложной структурой помех.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., профессор Яковлев В.А. является известным ученым в области теории связи, защиты информации и автоматизации; к.т.н., доцент Трифонов П.В. – крупный специалист в области теории передачи информации, помехоустойчивого кодирования и компьютерной алгебры; ведущая организация, "Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте" (ОАО «НИИАС»), является головным институтом отрасли железнодорожного транспорта в создании комплексов и систем обеспечения безопасности движения, в том числе систем автоматизации, управления и связи. ОАО «НИИАС» имеет большой научный задел в области повышения надёжности и качества функционирования автоматизированных информационных систем.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработаны конструктивные методы повышения помехоустойчивости и надёжности технических систем на основе нелинейных кодов, позволяющие увеличить вероятность обнаружения искажения информации, обрабатываемой, хранимой или передаваемой автоматизированными системами обработки информации и управления, снизить сложность реализации процедур кодирования и декодирования за счёт использования вычислительно более простых кодирующих нелинейных функций;

предложен оригинальный подход к усовершенствованию существующих методов нелинейного кодирования, заключающийся в обобщении известных методов построения кодов на случай более общей модели ошибок за счёт привнесения случайности в кодируемое сообщение, отличительной особенностью которого является расширение функциональности известных кодов простыми методами;

предложены две модификации существующих методов кодирования, позволяющие варьировать параметры кодов, которые могут быть применены к широкому классу кодов с целью упрощения их реализации;

доказана эффективность использования предлагаемых методов повышения помехоустойчивости в условиях рассматриваемой модели канала, достигаемая за счёт обеспечения заданной вероятности обнаружения ошибок вне зависимости от их величины, что обеспечивает повышение качества функционирования технических систем в условиях каналов с непредсказуемым потоком ошибок;

введены новые понятия, термины и определения, позволяющие структурировать имеющиеся знания о нелинейных методах кодирования, раскрыть суть нового метода построения кодов, обнаруживающих алгебраические манипуляции, и проводить исследования нелинейных кодов более полно и с единых позиций.

Теоретическая значимость исследования обоснована тем, что:

выведены теоретические границы параметров нелинейных кодов, позволяющие судить о неоптимальности некоторых существующих конструктивных методов построения нелинейных кодов и задающие направления для дальнейших исследований;

доказаны возможность построения кодов, обнаруживающих алгебраические манипуляции, из надёжных кодов за счёт привнесения случайности в кодируемое сообщение; возможность увеличения минимального кодового расстояния обобщённых систематических надёжных кодов с последующим исправлением ошибок малой кратности с помощью предлагаемого в диссертационной работе алгоритма декодирования; возможность использования операции скалярного умножения в конечном поле в качестве кодирующей функции для кодов, обнаруживающих алгебраические манипуляции, в узком смысле;

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

использованы методологический аппарат теории информации, методы теории помехоустойчивого алгебраического кодирования, теории вероятностей и элементы теории нелинейных функций над конечными полями;

проведена модификация существующих методов построения нелинейных кодов, позволяющая уменьшить вычислительную сложность их реализации и варьировать параметры получаемых кодов;

раскрыты расхождения между вероятностью обнаружения ошибок, достигаемой с помощью существующих методов построения кодов, обнаруживающих алгебраические манипуляции, на основе обобщённых кодов Рида-Маллера, и теоретической нижней границей обнаруживающей способности для кодов данной конструкции; расхождения между длиной систематических равномерно надёжных кодов, получаемых с помощью конструктивных методов их построения, и теоретической нижней границей их длины;

изучены принципы проектирования помехозащищённых технических систем с использованием техники параллельного обнаружения ошибок, позволяющей оперативно обнаруживать произошедшие искажения обрабатываемой информации;

изложены теоретические основы и практические приложения рассматриваемой модели дискретного канала с алгебраическими манипуляциями.

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

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

1) метод нелинейного кодирования на основе класса обобщённых систематических надёжных кодов, алгоритм обнаружения и исправления ошибок малой кратности для обобщённых систематических надёжных кодов, нижние границы параметров нелинейных кодов, а также обзор атак по сторонним каналам в учебных курсах «Кодирование и декодирование сообщений» и «Методы и средства защиты компьютерной информации», читаемых студентам специальности 230102 – «Автоматизированные системы обработки информации и управления» Санкт-Петербургского государственного университета аэрокосмического приборостроения и в дисциплине «Защита информации», читаемой магистрам направления 09.04.01 – «Информатика и вычислительная техника» Санкт-Петербургского государственного университета аэрокосмического приборостроения;

2) метод нелинейного кодирования на основе класса обобщённых систематических надёжных кодов, алгоритм обнаружения и исправления ошибок малой кратности для обобщённых систематических надёжных кодов, метод нелинейного кодирования на основе операции скалярного умножения компонентов

информационного сообщения и значения случайной величины, а также его модификации в Санкт-Петербургском государственном университете аэрокосмического приборостроения в рамках НИР по теме «Разработка и исследование надёжных методов хранения информации в аэрокосмических системах и комплексах»;

3) метод нелинейного кодирования, основанный на операции скалярного умножения компонентов информационного сообщения и значения случайной величины, модификация кодового метода на основе расширения случайной величины с целью уменьшения информационной избыточности коды в рамках выполнения НИР по разработке методов проектирования электронных идентификационных документов;

определены возможности и перспективы практического использования полученных результатов диссертации при проектировании помехозащищённых автоматизированных систем обработки информации, управления и связи;

представлены предложения и направления научных исследований для дальнейшего совершенствования методов нелинейного помехоустойчивого кодирования, предназначенных для повышения достоверности обработки информации и повышения надёжности технических систем.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ воспроизводимость результатов многократных экспериментов, выполненных на сертифицированном современном оборудовании; соответствие аналитически вычисленной обнаруживающей способности нелинейных кодов результатам компьютерного моделирования их использования в исследуемом канале; достоверность полученных решений задачи повышения надёжности технических систем и достоверности обработки информации подтверждена корректным использованием математических методов; количественным и качественным согласованием с результатами, полученными на основе известных методов решения;

элементы теории построены на известных принципах, проверенных данных и фактах с использованием современных известных и апробированных методов исследования, согласуется с опубликованными экспериментальными данными по теме диссертации;

идея базируется на анализе работ отечественных и зарубежных исследователей в области разработки и исследования методов нелинейного кодирования; на обобщении передового опыта в этой области;

использованы полученные экспериментальные результаты для сравнения с данными, приведенными в современной научной литературе по повышению помехоустойчивости с помощью нелинейных кодовых методов;

установлено качественное и количественное соответствие результатов решения задач повышения достоверности обработки информации с помощью предлагаемых в диссертационной работе методов нелинейного кодирования с использованием стандартных методов линейного кодирования и методов нелинейного кодирования, разработанных другими авторами; при определённых параметрах технических систем подтверждено преимущество решения поставленной задачи с помощью предлагаемых методов;

использованы сертифицированные оборудование и программные средства.

Личный вклад соискателя состоит в: разработке новых методов повышения помехоустойчивости на основе нелинейных кодов, обладающих меньшей вероятностью нарушения целостности данных и меньшей вычислительной сложностью, чем существующие методы, выводе теоретических границ параметров нелинейных кодов, позволяющих судить об их оптимальности, анализе современного состояния объекта и предмета исследования, а также в непосредственном участии в проведении компьютерного моделирования с целью подтверждения заявленной эффективности предлагаемых методов. Автору принадлежит решающая роль в апробации результатов исследования, разработке новых методов построения нелинейных кодов и исследовании параметров получаемых кодов, разработке алгоритмического обеспечения процедур кодирования и декодирования нелинейных кодов, подготовке основных публикаций по выполненной работе.

Диссертационный совет считает, что Алексеев М.О. в своей диссертационной работе решил научную задачу разработки методов нелинейного кодирования в каналах с алгебраическими манипуляциями для повышения достоверности обработки информации, имеющую важное социально-экономическое и хозяйственное значение.

На заседании 29.09.2015 г. диссертационный совет принял решение присудить Алексееву М.О. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 23 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 23, против нет, недействительных бюллетеней нет.

Председатель диссертационного совета Юсупов Рафаэль Мидхатович

Ученый секретарь диссертационного совета Фаткиева Роза Равильевна

29.09.2015 г.