ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.077.05 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ ИНСТИТУТА ПРОБЛЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ им. А. А. ХАРКЕВИЧА РОССИЙСКОЙ АКАДЕМИИ НАУК ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета

от «22» мая 2017 года, протокол № 30

О присуждении Трушиной Оксане Вячеславовне ученой степени кандидата физико-математических наук.

Диссертация «Разработка теоретико-информационных методов обеспечения анонимности в телекоммуникационных сетях» по специальности 05.13.17 – «Теоретические основы информатики» (физико-математические науки) принята к защите 15 марта 2017 года, протокол № 26, диссертационным советом Д 002.077.05 на базе федерального государственного бюджетного учреждения науки Института проблем передачи информации им. А. А. Харкевича Российской академии наук (127051, Москва, Б. Каретный пер., 19, строение 1, приказ о создании диссертационного совета от «10» июля 2015 года № 784/нк).

Соискатель Трушина Оксана Вячеславовна, гражданка Российской Федерации 1989 года рождения, в 2012 году окончила с отличием федеральное государственное автономное образовательное учреждение высшего профессионального образования «Московский физико-технический институт (государственный университет)», в 2016 году закончила аспирантуру федерального государственного автономного образовательного учреждения высшего образования «Московский физико-технический институт (государственный университет)».

Диссертация выполнена на кафедре радиотехники и систем управления Московского физико-технического института (государственного университета) Министерства образования и науки Российской Федерации.

Научный руководитель – заслуженный деятель науки, доктор технических наук, профессор Габидулин Эрнст Мухамедович, профессор кафедры радиотехники и систем управления федерального государственного автономного образовательного учреждения высшего образования «Московский физико-технический институт (государственный университет)».

Официальные оппоненты:

1. Беззатеев Сергей Валентинович, гражданин РФ, доктор технических наук, заведующий кафедрой технологий защиты информации федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения»;
2. Уривский Алексей Викторович, гражданин РФ, кандидат физико-математических наук, заместитель генерального директора ОАО «Информационные технологии и коммуникационные системы»;

дали ***положительные*** отзывы о диссертации.

Ведущая организация – Федеральное государственное бюджетное учреждение науки Институт вычислительных технологий Сибирского отделения Российской академии наук (ИВТ СО РАН), г. Новосибирск, в своем ***положительном*** заключении, подписанном доктором технических наук, профессором Рябко Борисом Яковлевичем, главным научным сотрудником лаборатории информационных систем и защиты информации и утвержденном кандидатом физико-математических наук Андреем Васильевичем Юрченко, временно исполняющим обязанности директора Федерального государственного бюджетного учреждения науки Институт вычислительных технологий Сибирского отделения Российской академии наук, указала, что диссертация Оксаны Вячеславовны Трушиной удовлетворяет всем требованиям ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук по специальности 05.13.17 – «Теоретические основы информатики» (отзыв заслушан и одобрен на заседании лаборатории

информационных систем и защиты информации « 4 » апреля 2017 года, протокол № 6).

Соискатель имеет 11 опубликованных работ, из них 10 по теме диссертации, в том числе 2 работы, опубликованные в рецензируемых научных изданиях, включенных в перечень изданий для опубликования основных научных результатов диссертаций. Соискателем опубликовано 7 работ в материалах всероссийских и международных конференций и симпозиумов. В работах, опубликованных в соавторстве, соавторам принадлежат постановки задач и частичный анализ литературы.

Наиболее значимые работы по теме диссертации:

1. Габидулин Э.М., Пилипчук Н.И., Трушина О.В. Защита информации в телекоммуникационных сетях // Труды МФТИ. 2013. Т. 5. N 3. С. 97-111.
2. Трушина О.В., Габидулин Э.М. Новый метод обеспечения анонимности и секретности в сетевом кодировании // Пробл. передачи информ. 2015. Т. 51. Вып. 1. С. 82-89. DOI: 10.1134/S0032946015010081.
3. Trushina O. On the Anonymity of Physical-Layer Network Coding Against Wiretapping // Proc. of XV International Symposium “Problems of Redundancy in Information and Control Systems”. Saint-Petersburg, Russia. September 26-29, 2016. P. 158-161. DOI: 10.1109/RED.2016.7779353.

На диссертацию и автореферат поступило 6 отзывов, включая отзывы официальных оппонентов и ведущей организации. Все отзывы положительные. В отзывах указывается, что материал диссертации представляет собой законченную научно-исследовательскую работу и соответствует специальности 05.13.17 – «Теоретические основы информатики». Диссертация удовлетворяет требованиям «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24.09.2013 № 842, предъявляемым к диссертациям на соискание ученой степени кандидата наук.

В отзыве ведущей организации сделаны следующие замечания.

В диссертационной работе нет данных о распределении исходного сообщения и о том, как оно влияет на стойкость методов.

При анализе сложности разработанных методов не приведено сравнение со сложностью решения этой задачи обеспечения анонимности с помощью криптографических методов.

По тексту диссертации имеются небольшие замечания по стилю изложения материала – встречаются канцеляризмы.

Вышеперечисленные замечания не оказывают влияния на общую положительную оценку работы.

В отзыве официального оппонента доктора технических наук, доцента Сергея Валентиновича Беззатеева отмечены следующие недостатки.

Безусловно было бы интересно и полезно, с точки зрения полноты представленной работы, рассмотреть возможности использования других классов кодов (не ранговой метрики) и провести их сравнение.

В работе имеются некоторые неточности и различие в обозначениях, что несколько затрудняет ее прочтение. На странице 13 и далее можно отметить не совсем удачное использование термина «онион» при общепризнанном в настоящее время термине «луковичный». К тому же автор местами использует именно этот термин. На странице 37 ранг матрицы B с элементами из F_q^m над полем F_q, обозначается r(B; q), а на странице 44 и далее используется обозначение Rk(B). Первоначально в разделе 2.2.2 речь идет о пакетах длины m, что логично объясняется степенью расширения поля. На этой же странице в последнем абзаце раздела 2.2.2 для длины пакета предложено обозначение N. На странице 56 вместо (n; k) кода Рида-Соломона должен быть (n, μ) код. Крайне неудачное расположение рисунка 3.7 и поясняющего его текста. Текст к рисунку расположен через две страницы от рисунка, что крайне затрудняет чтение представленного материала.

В отзыве официального оппонента кандидата физико-математических наук Алексея Викторовича Уривского указаны следующие недостатки.

Разработанные методы обеспечения несвязываемости носят теоретико-информационный характер, но в модели канала с подслушиванием. Это означает, что возможности злоумышленника все же ограничены, но не вычислительно, а коммуникационно. А именно тем, что злоумышленнику доступна лишь доля передаваемых сообщений или его канал подслушивания зашумлен сильнее канала

передачи сообщений. Представляется уместным, чтобы упоминание о таких ограничениях присутствовало более четко во вводной части работы.

Приводимый обзор известных методов обеспечения анонимности носит научно-популярный характер, и использует меняющуюся терминологию и обозначения, что не позволяет напрямую сравнивать рассматриваемые методы.

По тексту диссертации периодически меняется способ обозначения узлов – разнообразные прописные и строчные латинские буквы, – что затрудняет восприятие материала.

Утверждение в разделе 2.2 о том, что передача данных во всех сетях осуществляется посредством маршрутизации нельзя признать верным, в частности широковещательные сети могут ее не использовать.

В разделах про анализ предлагаемых методов обеспечения несвязываемости в качестве меры эффективности, кроме оценок сложности реализации, было бы уместным явно показать, какие вносятся накладные расходы (избыточность).

Отмечено несколько опечаток и пунктуационных ошибок: стр. 16, 31, 56.

Приведенные недостатки не снижают научной ценности полученных в диссертационной работе результатов.

В отзыве на автореферат Владимира Михайловича Фомичева, доктора физико-математических наук, профессора, научного консультанта Службы сертификации Общества с ограниченной ответственностью «Код Безопасности», в качестве замечаний отмечено небольшое количество погрешностей стилистического характера.

Указано, что это замечание не снижает положительного впечатления от работы.

В отзыве на автореферат Сергея Семеновича Анисова, кандидата физико-математических наук, аналитика Общества с ограниченной ответственностью «АйПиВеб», в качестве замечаний отмечено следующее. Приведенное описание стойкости методов слишком краткое и не позволяет понять, в чем состоит влияющие на стойкость особенности методов. Кроме того, использование термина «алгебраическая решетка» в рассматриваемом контексте некорректно, надо использовать «целочисленная решетка».

В отзыве отмечено, что, несмотря на замечания, диссертационная работа является законченной научно-исследовательской работой, результаты которой можно квалифицировать как решение новой научной задачи.

В отзыве на автореферат Владимира Викторовича Витязева, доктора технических наук, профессора, заведующего кафедрой телекоммуникаций и основ радиотехники Рязанского государственного радиотехнического университета и Евгения Александровича Лихобабина, кандидата технических наук, старшего научного сотрудника кафедры телекоммуникаций и основ радиотехники Рязанского государственного радиотехнического университета сделаны следующие замечания.

Довольно краткое описание принципа сетевого кодирования не дает возможности понять почему разработанный в диссертации метод применим к нему лучше, чем криптографические методы. В диссертации утверждается, что секретность передаваемых сообщений является необходимым условием для обеспечения несвязываемости. Криптографический подход обеспечивает семантическую секретность, в то время как для предлагаемого теоретико-информационного подхода семантическая секретность рассмотрена только для гауссовского канала и не рассмотрена для других каналов, что приводит к неясности возможна ли семантическая секретность для этих каналов.

В отзыве отмечено, что несмотря на недостатки, полученные результаты дают основание для положительной оценки диссертации. Диссертация О. В. Трушиной является законченной научно-исследовательской работой, представляющей научный интерес.

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью в исследуемой области, что подтверждается научными публикациями и патентами. Доктор технических наук, доцент Сергей Валентинович Беззатеев является авторитетным специалистом в области кодирования и защиты информации, автором патента и множества научных работ в высокорейтинговых журналах. Кандидат физико-математических наук Алексей Викторович Уривский является признанным специалистом в вопросах защиты информации, имеет множество патентов, участвует в разработке национальных стандартов защиты информации. Ведущая организация Институт

вычислительных технологий Сибирского отделения Российской академии наук выполняет теоретические и прикладные исследования в области передачи и защиты информации, результаты которых публикуются в рецензируемых научных изданиях.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- задача обеспечения анонимности сформулирована в терминах задачи обеспечения несвязываемости и впервые поставлена в теоретико-информационном смысле;
- развита концепция количественной меры несвязываемости пары сообщений через взаимную информацию между ними;
- введено новое понятие теории анонимной передачи данных - понятие совершенной несвязываемости;
- разработана теоретико-информационная модель обеспечения несвязываемости сообщений, позволяющая получать методы обеспечения несвязываемости для различных видов передачи данных в модели канала с подслушивающим злоумышленником;
- разработаны методы обеспечения несвязываемости, реализующие предложенный подход для цифрового когерентного сетевого кодирования, традиционной маршрутизации и аналогового сетевого кодирования. Эти методы можно использовать в сетевом кодировании без усложнения процесса передачи в отличие от существующих ранее криптографических методов, которые для использования в сетевом кодировании, требуют введения дополнительных операций.

Теоретическая значимость исследований обоснована тем, что:

- предложен теоретико-информационный подход к задаче обеспечения информационной безопасности и анонимности, который, в частности, представляет большой интерес в виду отсутствия предположений о вычислительных возможностях злоумышленника или о возможности перехода к альтернативной вычислительной парадигме, например построения квантового компьютера;

- изучена возможность применения методов кодирования для решения задачи обеспечения несвязываемости.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что разработанная теоретико-информационная модель обеспечения несвязываемости сообщений позволяет получать методы, применимые как в проводных, так и в беспроводных сетях передачи данных.

Оценка достоверности результатов исследования выявила, что корректно использован апробированный в научной практике исследовательский и аналитический аппарат, математические доказательства и рассуждения являются строгими и корректными, результаты исследований обсуждались на международных и всероссийских научных конференциях и опубликованы в рецензируемых научных изданиях.

Личный вклад соискателя состоит в непосредственном получении результатов, в изложении их с полными доказательствами в тексте диссертационной работы, а также в подготовке публикаций по выполненной работе.

Представленная Оксаной Вячеславовной Трушиной диссертация отвечает паспорту специальности 05.13.17 – «Теоретические основы информатики» в части пункта 1 «Исследование, в том числе с помощью средств вычислительной техники, информационных процессов, информационных потребностей коллективных и индивидуальных пользователей» и пункта 11 «Разработка методов обеспечения высоконадежной обработки информации и обеспечения помехоустойчивости информационных коммуникаций для целей передачи, хранения и защиты информации; разработка основ теории надежности и безопасности использования информационных технологий».

Диссертационный совет пришел к выводу о том, что диссертация представляет собой завершенную научно-квалификационную работу, в которой решена актуальная задача разработки и исследования теоретико-информационных методов обеспечения несвязываемости передаваемых сообщений, имеющая значение для изучения теоретических основ обеспечения анонимности и разработки методов защиты информационных коммуникаций.

По актуальности, новизне, теоретической значимости диссертация соответствует требованиям, установленным «Положением о порядке присуждения ученых степеней», утвержденным постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842, предъявляемым к диссертациям на соискание ученой степени кандидата наук.

На заседании 22 мая 2017 года диссертационный совет принял решение присудить Трушиной Оксане Вячеславовне ученую степень кандидата физико-математических наук по специальности 05.13.17 – «Теоретические основы информатики».

При проведении тайного голосования диссертационный совет в количестве 26 человек, из них 4 доктора наук по специальности и отрасли наук рассматриваемой диссертации, участвовавших в заседании, из 35 человек, входящих в состав совета, проголосовали: за присуждение учёной степени – 25, против присуждения учёной степени – 0, недействительных бюллетеней – 1.

Председатель
диссертационного совета Д 002.077.05 Кулешов А.П.

Ученый секретарь
диссертационного совета Д 002.077.05 Цитович И.И.

22 мая 2016 г.