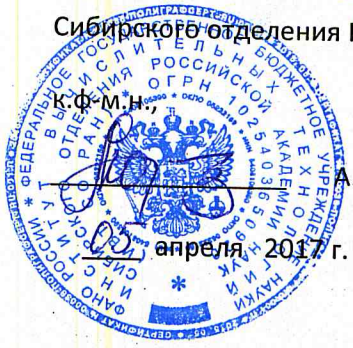
«УТВЕРЖДАЮ»
Врио директора Федерального
государственного бюджетного учреждения
науки Института вычислительных технологий
Сибирского отделения РАН (ИВТ СО РАН)
к.ф-м.н.,



_____ А.В.Юрченко
«__» апреля 2017 г.

ОТЗЫВ

ведущей организации на диссертацию Трушиной Оксаны Вячеславовны

«Разработка теоретико-информационных методов обеспечения анонимности в телекоммуникационных сетях», представленную на соискание ученой степени кандидата физико-математических наук

по специальности 05.13.17 – «Теоретические основы информатики»

Диссертационная работа Трушиной О.В. посвящена обеспечению анонимности легальных пользователей в системах передачи информации. В настоящее время большинство исследований при решении подобных задач применяют криптографические методы, использующие шифрование. Криптостойкость таких систем зависит от производительности современной вычислительной техники. С повышением этого уровня с течением времени, например, когда реализуются квантовые компьютеры, криптостойкость будет существенно снижена. Уход от таких серьёзных проблем предложен в данной работе, в которой успешно применён теоретико-информационный подход.

Структура и содержание

Работа структурирована обычным образом: введение, три содержательные главы, заключение и список цитируемой литературы, в который также внесены работы автора диссертации.

Во введении обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана значимость полученных результатов, представлены выносимые на защиту научные положения.

В первой главе приведены основные определения, сформулирована задача обеспечения анонимности на основе теоретико-информационного подхода. Показано, что необходимым условием обеспечения анонимности в системе со многими пользователями является создание информационного разрыва между сообщениями, входящими в узел сети связи и выходящими из него. Это событие здесь определено как обеспечение несвязываемости сообщений. Введено новое понятие - несвязываемость. И далее в остальной части диссертационной работы показано, как именно надо создавать несвязываемость в различных условиях.

Кроме того, в первой главе приведён обзор и анализ существующих методов обеспечения анонимности: основные характеристики, модели злоумышленников и, что важно, введены новые понятия совершенной несвязываемости по аналогии с шенноновской совершенной секретностью.

Во второй главе представлены разработанные методы обеспечения совершенной несвязываемости применительно к когерентному сетевому кодированию и к традиционному способу передачи данных.

В третьей главе описаны методы обеспечения совершенной несвязываемости для аналогового сетевого кодирования.

В заключении приведены основные результаты диссертационной работы.

Научная новизна

В отличие от известного, криптографического подхода, разработан новый, теоретико-информационный подход для решения задачи обеспечения анонимности в сетях со многими пользователями. В рамках этого подхода автор диссертации, Трушина О.В. ввела новое понятие несвязываемости и на его основе разработала три метода решения этой задачи для трёх различных видов информационных сетей.

Теоретическая и практическая ценность

В теоретическом плане проведённое исследование содержит решение важной задачи обеспечения анонимности легальных пользователей в сетях со многими пользователями, где имеются нелегальные пользователи, прослушивающие передаваемые сообщения в определённом объёме. Решение этой задачи закрыло собой пробел в области теоретико-информационных методов обеспечения анонимности.

В работе показана возможность применения разработанных методов на практике, как в беспроводных, так и в проводных сетях связи.

Полнота опубликованных научных результатов

Результаты диссертационной работы опубликованы в 9 научных статьях, из них 2 статьи в рецензируемых изданиях, входящих в перечень ВАК, и 7 статей в сборниках трудов конференций, включая международные и традиционные конференции МФТИ.

Замечания к диссертационной работе

Отмечены следующие недостатки.

1. В диссертационной работе нет данных о распределении исходного сообщения и о том, как оно влияет на стойкость методов.
2. При анализе сложности разработанных методов не приведено сравнение со сложностью решения этой задачи обеспечения анонимности с помощью криптографических методов.
3. По тексту диссертации имеются небольшие замечания по стилю изложения материала – встречаются канцеляризмы.

Автореферат полностью и точно отражает содержание диссертации.

Заключение

Вышеперечисленные недостатки не оказывают влияния на общую положительную оценку работы. Диссертация написана четким, ясным языком и правильно структурирована. Основные результаты работы своевременно опубликованы. В научно-квалификационной работе решена актуальная научная задача по разработке и исследованию теоретико-информационных методов обеспечения анонимности, имеющая теоретический и практический интерес.

Диссертационная работа Оксаны Вячеславовны Трушиной «Разработка теоретико-информационных методов обеспечения анонимности в телекоммуникационных сетях» соответствует требованиям пункта 9 Положения о порядке присуждения ученых степеней, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук по специальности 05.13.17 – «Теоретические основы информатики», а ее автор Трушина Оксана Вячеславовна заслуживает присуждения ученой степени кандидата физико-математических наук по этой специальности.

Отзыв на диссертацию обсужден и одобрен на заседании лаборатории информационных систем и защиты информации, протокол № 6 от 04.04.2017 года.

Рябко Борис Яковлевич д.т.н., профессор, г.н.с.

05.04. 2017 г. тел. +7383 334-91-24 доб. 11-89

Федеральное государственное бюджетное учреждение науки
Институт вычислительных технологий Сибирского отделения Российской академии наук (ИВТ СО РАН)

Адрес: 630090 Новосибирск, пр. Академика Лаврентьева, 6

Тел.: (383) 330-61-50

Факс: (383) 330-63-42

Адрес электронной почты: ict@ict.nsc.ru

Адрес официального сайта: http://www.ict.nsc.ru/