ОТЗЫВ
официального оппонента на диссертационную работу
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»

Актуальность темы диссертационной работы

Объем и ценность информации, передаваемой по телекоммуникационным сетям, постоянно возрастают. Это приводит к необходимости решения новых задач защиты информации, одной из которых является обеспечение анонимности корреспондентов. Несмотря на то, что имеется множество работ, посвященных методам анонимности, это направление защиты информации остается новым и недостаточно изученным.

Постоянный рост вычислительных мощностей, которыми могут обладать не только легальные пользователи сети, но и злоумышленник, сохраняет интерес исследователей к теоретико-информационному подходу к защите информации, так как он позволяет строить методы защиты, стойкость которых не зависит от вычислительной трудоемкости каких-либо задач.

В этой связи решаемая в диссертационной работе задача разработки и исследования теоретико-информационных методов обеспечения анонимности является актуальной.

Содержание работы

Работа состоит из введения, трех глав, заключения и списка литературы.

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 на примере описывается задача анонимной передачи, которая разделяется на составляющие: задачу секретной маршрутизации и задачу обеспечения несвязываемости передаваемых по маршруту сообщений. Показано, что секретной

маршрутизации недостаточно для обеспечения анонимности передачи, и несвязываемость необходима. Диссертационная работа посвящена обеспечению несвязываемости сообщений. Приведенный обзор существующих работ, посвященных анонимной передаче, демонстрирует отсутствие теоретико-информационных методов обеспечения несвязываемости, что показывает актуальность и значимость поставленных в диссертационной работе задач. Также в первой главе введено новое понятие совершенной несвязываемости. Необходимость введения этого понятия обоснована обзором существующих численных характеристик анонимности, которые не подходят для описания несвязываемости сообщений.

Во второй и третьей главах предложены оригинальные методы обеспечения несвязываемости сообщений для различных типов передачи данных. Все предложенные методы объединены общей идеей – они основаны на кодировании смежными классами, но отличаются деталями реализаций, так как для разных типов передачи данных рассматриваются операции над разными множествами. Во второй главе рассматриваются традиционная маршрутизация и цифровое когерентное сетевое кодирование. Для этих типов передачи данных используются конечные поля. В третьей главе рассматривается аналоговое сетевое кодирование, которое использует операции над целочисленными решетками. Все предложенные методы теоретически обоснованы. Приведенный анализ стойкости методов формулирует условия, при которых методы обеспечивают совершенную несвязываемость.

В заключении резюмируются основные результаты диссертационной работы.

Новизна исследований и полученных результатов

В качестве новых научных результатов, полученных в диссертации, следует отметить следующие положения.

1. Анонимность определена через несвязываемость и построена теоретико-информационная модель несвязываемости. Введено понятие совершенной несвязываемости. Построенная модель позволяет получать новые методы

совершенной несвязываемости сообщений для разных видов передачи данных.

2. Предложен и теоретически обоснован метод обеспечения совершенной несвязываемости сообщений для цифрового когерентного сетевого кодирования, основанный на применении модели канала с подслушиванием.
3. Предложен и теоретически обоснован метод обеспечения совершенной несвязываемости сообщений для традиционной маршрутизации, основанный на применении модели канала с подслушиванием.
4. Предложен и теоретически обоснован метод обеспечения совершенной несвязываемости сообщений для аналогового сетевого кодирования, основанный на применении модели гауссовского канала с подслушиванием.

Теоретическая и практическая значимость

Проведенные в диссертации исследования в определенной степени заполняют пробелы, оставленные в предыдущих теоретических работах, относящихся к исследованию обеспечения анонимности. Результаты, полученные в диссертации, имеют несомненную теоретическую и практическую важность. Это следует из самой постановки задачи и доведения полученных результатов до конкретных методов обеспечения несвязываемости сообщений для проводных и беспроводных сетей.

Степень обоснованности и достоверности научных положений и выводов, сформулированных в диссертации, и их достоверность

Все выводы, сделанные в диссертации, обоснованы, а теоретические результаты доказаны. Их достоверность подтверждена корректностью применения аналитического аппарата, строгостью и корректностью математических доказательств и рассуждений, а также обсуждением результатов исследования на международных и всероссийских научных конференциях, публикациями результатов исследования в рецензируемых научных изданиях.

Недостатки работы

1. 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.
2. В работе имеются некоторые неточности и различие в обозначениях, что несколько затрудняет ее прочтение:
   - Стр.13 и далее: не совсем удачное использование термина «онион» при общепризнанном в настоящее время термине «луковичный». К тому же автор местами использует именно этот термин.
   - Стр. 37: рангом матрицы B с элементами из F_q^m над полем F_q, обозначается r(B; q), а на стр. 44 и далее используется обозначение Rk(B).
   - Стр. 41 : 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.
   - Стр . 56 : последние μ строк формируют порождающую матрицу (n, k) кода Рида-Соломона. Должно быть (n, μ) кода.
   - Стр. 81-83: крайне неудачное расположение рисунка и поясняющего его текста. Текст к рисунку расположен через две страницы от рисунка, что крайне затрудняет чтение представленного материала.

Заключение

Диссертация О. В. Трушиной является законченной научно-квалификационной работой, содержащей решение актуальной задачи разработки и исследования теоретико-информационных методов обеспечения анонимности. Полученные автором результаты достоверны, выводы и заключения обоснованы. Основные научные результаты диссертации достаточно полно отражены в 9 публикациях соискателя, в том числе в 2 из перечня изданий, рекомендованных ВАК. Содержание и название работы полностью

соответствуют друг другу. Автореферат дает ясное представление о содержании и основных результатах автора.

Таким образом, диссертация О. В. Трушиной удовлетворяет требованиям Положения ВАК о порядке присуждения ученых степеней, а ее автор Оксана Вячеславовна Трушина заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.17 – «Теоретические основы информатики».

Заведующий кафедрой технологий защиты информации Санкт-Петербургского государственного университета аэрокосмического приборостроения,
доктор технических наук, доцент 2 мая 2017 г.

С. В. Беззатеев

Подпись работника ГУАП Беззатеева С.В.
Заверяю
Начальник Управления персонала
01 05 2017 г.

Отзыв подготовил:
Сергей Валентинович Беззатеев, гражданин Российской Федерации, доктор технических наук по специальности 05.13.01 – «Системный анализ, управление и обработка информации».
Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (ГУАП), кафедра технологий защиты информации.
Адрес: Россия, 190000, Санкт-Петербург, ул. Б. Морская, д. 67
Тел.: (812) 494-70-77, Email: bsv@aanet.ru