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

Цифровизация информационного взаимодействия проникла во все сферы нашей жизни. Естественным образом это ведет к усилению требований по защите информации. С усложнением структуры и объема информационного взаимодействия, кроме традиционных услуг информационной безопасности, таких как обеспечение доступности, целостности и конфиденциальности информации, возникают запросы к предоставлению и других услуг. В частности весьма востребованным является сокрытие структуры информационного взаимодействия, то есть защиты информации о том, между какими абонентами происходит информационный обмен. В этом смысле можно говорить об обеспечении анонимности передаваемой информации.

Для ряда информационных систем регуляторами в области информации безопасности в России предъявляются требования сокрытия структуры сети взаимодействующих абонентов, что по сути и есть задача обеспечения анонимности взаимодействия. Наиболее простые методы решения такой задачи состоят в инкапсуляции трафика и его последующего шифрования или использовании трансляции сетевых адресов. Практическая реализация таких мер защиты относительно проста, но их надежность или применимость весьма ограничены.

Вопросы обеспечения анонимности в контексте аутентификации и

цифровой подписи отражены в международных стандартах ISO/IEC 20008, 20009 и 29191. Причем надо заметить, что в этих стандартах понимание свойств анонимности и несвязываемости носит качественный характер и, хуже того, несогласованный между разными стандартами.

В целом теоретические основы решения задачи обеспечения анонимности на сегодняшний день сформулированы не до конца и изучены лишь фрагментарно. Большой интерес представляет теоретико-информационный подход к задаче обеспечения информационной безопасности, и анонимности в частности, в виду отсутствия предположений о вычислительных возможностях злоумышленника или о возможности перехода к альтернативной вычислительной парадигме, например построения квантового компьютера. В этой связи решаемая в диссертационной работе задача разработки и исследования теоретико-информационных методов обеспечения анонимности является, безусловно, актуальной.

Содержание работы

Диссертационная работа состоит из введения, трех глав, в которых изложены основные результаты работы, 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.

Первая глава посвящена анализу существующих методов обеспечения анонимности и их количественным характеристикам анонимности. В задаче обеспечения анонимности выделяется две части. Первая представляет собой задачу маршрутизации, а вторая – задачу обеспечения несвязываемости передаваемых сообщений. Задача обеспечения несвязываемости состоит в том, чтобы передавать сообщения через промежуточный узел таким образом, чтобы у злоумышленника не было возможности соотнести сообщения, поступающие в

узел, с сообщениями, выходящими из него. Именно на задаче обеспечения несвязываемости и сосредоточено диссертационное исследование, так как она является необходимым условием анонимности. Для оценки несвязываемости сообщений в теоретико-информационном смысле в первой главе введено новое понятие совершенной несвязываемости, по аналогии с понятием совершенной секретности.

Во второй главе предложены методы обеспечения несвязываемости для цифрового сетевого кодирования и традиционной маршрутизации. Эти методы используют кодирование смежными классами для дискретного канала с подслушиванием. Теоретически доказана корректность предложенных методов. Даны оценки сложности методов и сформулированы условия достижения совершенной несвязываемости.

В третьей главе рассматривается обеспечение несвязываемости для аналогового сетевого кодирования. Предложенный метод использует кодирование смежными классами для гауссовского канала с подслушиванием. Метод теоретически обоснован, проведен анализ его стойкости и сложности.

В заключении резюмируются основные результаты диссертационной работы.

Новизна исследований и полученных результатов

К новым результатам следует отнести следующие положения, полученные в диссертационной работе.

1. Развита концепция количественной меры несвязываемости пары сообщений через взаимную информацию между ними и определена совершенная несвязываемость.
2. Разработаны и оценены методы обеспечения несвязываемости сообщений для различных способов передачи данных в модели канала с подслушивающим злоумышленником.

Теоретическая и практическая значимость

Исследовано применение теоретико-информационных методов для обеспечения несвязываемости сообщений. Предложенная в диссертационной работе идея позволяет строить методы обеспечения несвязываемости для различных способов передачи данных.

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

Полученные теоретические результаты математически строго обоснованы. Соискатель владеет методами теории информации, теории кодирования и алгебры. Достоверность положений и выводов диссертации также подтверждается апробацией работы, основные результаты которой докладывались на российских и международных конференциях и семинарах.

Недостатки работы

По содержанию работы имеются следующие замечания

1. 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.
2. Приводимый обзор известных методов обеспечения анонимности носит научно-популярный характер, и использует меняющуюся терминологию и обозначения, что не позволяет напрямую сравнивать рассматриваемые методы.
3. По тексту диссертации периодически меняется способ обозначения узлов

– разнообразные прописные и строчные латинские буквы, – что затрудняет восприятие материала.

4. 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.
5. 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).
6. Отмечено несколько опечаток и пунктуационных ошибок: стр. 16, 31, 56.

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

Выводы по диссертации

Диссертационная работа Трушиной О.В. содержит совокупность новых научных результатов, выдвинутых на защиту, и свидетельствует о способности автора к самостоятельной исследовательской работе. Предложенные в работе методы аргументированы и критически оценены в сравнении с другими известными решениями, выводы обоснованы. Заимствованные результаты и утверждения имеют соответствующие ссылки. Основные научные результаты своевременно и полно опубликованы, в том числе в изданиях, рекомендованных ВАК. Автореферат правильно отражает содержание работы.

На основе вышеизложенного можно заключить, что диссертация Трушиной О. В. «Разработка теоретико-информационных методов обеспечения анонимности в телекоммуникационных сетях» является законченной научно-квалификационной работой и удовлетворяет критериям «Положения о порядке присуждения ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24.09.2013 г. № 842, предъявляемым к диссертациям на соискание ученой

степени кандидата наук, а ее автор, Трушина Оксана Вячеславовна, заслуживает присуждения ей ученой степени кандидата физико-математических наук по специальности 05.13.17 – «Теоретические основы информатики».

02 мая 2017 г.

Официальный оппонент,
зам. генерального директора по науке и инновациям
ОАО «Информационные технологии и коммуникационные системы»,
кандидат физико-математических наук А. В. Уривский

Подпись Уривского А.В. заверяю:

Заместитель генерального директора ОАО «ИнфоТеКС» Д.М. Гусев

Сведения об оппоненте:
Алексей Викторович Уривский, гражданин Российской Федерации, кандидат физико-математических наук по специальности 05.13.17 – «Теоретические основы информатики», зам. генерального директора по науке и инновациям Открытого акционерного общества «Информационные технологии и коммуникационные системы».
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, дом 1/23, стр. 1.
Тел.: +7 (495) 737-61-92, Email: alexey.urivskiy@mail.ru, urivskiy@infotecs.ru