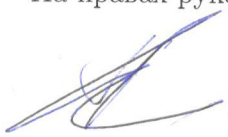
На правах рукописи



Трушина Оксана Вячеславовна

Разработка теоретико-информационных методов обеспечения анонимности в телекоммуникационных сетях

Специальность: 05.13.17 – Теоретические основы информатики

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва – 2017

Работа выполнена на кафедре радиотехники и систем управления Федерального государственного автономного образовательного учреждения высшего образования «Московский физико-технический институт (государственный университет)».

Научный руководитель: доктор технических наук, профессор
Габидулин Эрнст Мухамедович.

Официальные оппоненты: **Беззатеев Сергей Валентинович**,
доктор технических наук, доцент,
заведующий кафедрой технологий защиты информации Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (ГУАП),

Уривский Алексей Викторович,
кандидат физико-математических наук,
заместитель генерального директора ОАО «Информационные Технологии и Коммуникационные Системы».

Ведущая организация: Федеральное государственное бюджетное учреждение науки Институт вычислительных технологий Сибирского отделения Российской академии наук.

Защита состоится «_____»_____2017 г. в _____ часов

на заседании диссертационного совета Д 002.077.05 на базе ИППИ РАН по адресу Большой Каретный пер., д. 19, стр. 1, Москва, 127051.
С диссертацией можно ознакомиться в библиотеке ИППИ РАН и на сайте http://iitp.ru/.

Автореферат разослан «_____»_____2017 г.

Ученый секретарь
диссертационного совета
доктор физико-математических наук Цитович И.И.

Общая характеристика работы

Актуальность темы исследования. Современные системы связи предъявляют высокие требования к обеспечению защиты информации. Дисциплина «защита информации» решает множество вопросов, главным из которых является обеспечение секретности передаваемого сообщения. В конфиденциальности может нуждаться не только передаваемая информация, но также персональная информация отправителя и (или) получателя сообщения и информация о том, между кем происходит передача сообщений. Развитие информационных технологий привело к возникновению нового типа угроз, связанных с несанкционированным доступом к персональным данным. Например, злоумышленник может определить идентификаторы корреспондентов, желающих скрыть факт своего сотрудничества. В связи с этим обеспечение анонимности в сети представляет собой актуальное и быстро развивающееся направление защиты информации.

Проблему обеспечения анонимности можно разделить на две задачи. Первая задача состоит в том, чтобы секретным образом сформировать маршрут передачи сообщения. Маршрутная информация не должна быть известна злоумышленнику, иначе она даёт ему возможность вычислить идентификаторы корреспондентов. Вторая задача заключается в том, чтобы по установленному маршруту передавать сообщение так, чтобы его нельзя было прослеживать. Это достигается за счёт того, что сообщение, поступившее в некоторый промежуточный узел маршрута, изменяется таким образом, что сообщения на входе и выходе отличаются. Эту задачу называют задачей обеспечения несвязываемости сообщений. Начиная с первой работы[1], посвящённой анонимной передаче сообщений, задача обеспечения несвязываемости решается обычно с помощью шифрования. Шифрование осуществляет псевдослучайную перестановку, меняет вид сообщения, сохранив при этом информацию.

Современная криптография основана на предположении, что злоумышленник вычислительно ограничен. Для модели канала с подслушиванием возникло другое направление обеспечения секретности данных. Вместо вычислительных ограничений на злоумышленника накладываются физические ограничения. Предполагается, что злоумышленник не может перехватить сообщение целиком, а только его часть. Другое ограничение состоит в том, что канал, по которому злоумышленник получает сообщение, зашумлён больше, чем основной канал передачи. В этих условиях секретности можно достичь без криптографических примитивов, а путём использования теоретико-информационных средств, таких как коды.

Такое направление исследований называется теоретико-информационным. В настоящее время ведутся исследовательские работы по обеспечению секретности с использованием модели

[1] Chaum D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms // Communications of the ACM. 1981. V. 24 No. 2. P. 84–88.

канала с подслушиванием. Для беспроводных сетей задача обеспечения секретности часто ставится на физическом уровне, где методы на основе модели канала с подслушиванием являются основным средством. По сравнению с традиционной криптографией выделяют два важных преимущества теоретико-информационного направления: не существует строгих ограничений на вычислительные ресурсы злоумышленника и нет необходимости решать задачу распределения криптографических ключей, которая может быть довольно сложной и энергозатратной. Первое из этих преимуществ обеспечивает долгосрочную секретность. Второе преимущество существенно для систем связи с маломощными устройствами. Маломощными часто являются портативные устройства, такие как смартфоны.

Подход к обеспечению несвязываемости сообщений определяет в целом подход к обеспечению анонимности передачи данных. Так при теоретико-информационном подходе к несвязываемости можно говорить о теоретико-информационных методах анонимности.

Криптографический подход обеспечивает полный набор методов защиты информации, начиная с секретности сообщений и заканчивая несвязываемостью сообщений. Для того чтобы теоретико-информационный подход смог заменить традиционную криптографию, он также должен предлагать полный набор методов защиты информации. Методы обеспечения секретности на основе модели канала с подслушиванием представлены в литературе, но на данный момент нет методов обеспечения несвязываемости сообщений для такой модели.

В 2000 году был предложен новый способ передачи данных – сетевое кодирование. Этот способ передачи отличается от традиционной маршрутизации тем, что промежуточные узлы могут выполнять определённые алгебраические операции над поступившими пакетами, которые являются элементами конечного поля. Например составлять их линейные комбинации. Появление сетевого кодирования способствовало развитию исследований не только в области построения новых кодов, но также в области защиты информации, в частности, обеспечения анонимности. Стало понятно, что методы, успешно работающие в традиционных сетях передачи данных и в большинстве своём использующие классическую криптографию, не могут быть применимы к сетевому кодированию, так как не предусматривают выполнение операций с пакетами на внутренних узлах сети. Теоретико-информационные методы защиты информации, основанные на кодах, могут быть встроены в сетевое кодирование более простым способом по сравнению с криптографическими методами, адаптированными для использования в сетевом кодировании.

Таким образом, построение новых эффективных теоретико-информационных методов обеспечения анонимности в сети связи представляет собой актуальную научную задачу как для традиционной маршрутизации данных, так и для сетевого кодирования.

Целью диссертационной работы является построение теоретико-информационных методов несвязываемости на основе модели канала с подслушиванием и исследование их свойств.

Для достижения поставленной цели в работе рассмотрены следующие **задачи**.

1. Разработка и исследование метода обеспечения несвязываемости для цифрового когерентного и аналогового сетевого кодирования.

2. Разработка и исследование метода обеспечения несвязываемости для традиционной маршрутизации.

Методы исследования. В диссертационной работе используются методы теории информации, теории кодирования, теории вероятностей, теории конечных полей, преобразований Фурье.

Научная новизна результатов, полученных в диссертации, заключается в том, что предложен и реализован новый подход к обеспечению анонимности, а именно теоретико-информационный подход.

Теоретическая и практическая значимость. Исследовано применение модели канала с подслушиванием для обеспечения несвязываемости сообщений. Построенные на основе этой модели методы закрывают собой пробел в классе теоретико-информационных методов защиты информации, состоящий в отсутствии теоретико-информационных методов обеспечения анонимности. Показана возможность применения предложенных методов как в беспроводных, так и в проводных сетях.

Обоснованность и достоверность результатов обеспечена корректностью применения апробированного в научной практике исследовательского и 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, в том числе, рекомендованных ВАК РФ.

Положения, выносимые на защиту.

1. Построена теоретико-информационная модель анонимности, где анонимность определяется через несвязываемость. Предложено понятие совершенной несвязываемости. Построенная модель позволяет получать новые методы совершенной несвязываемости сообщений для разных видов сетей 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.

Апробация работы. Основные результаты работы докладывались и обсуждались на следующих конференциях: Seventh International Workshop on Optimal Codes and Related Topics (Albena, Bulgaria. September 6-13, 2013), 56-й научной конференции МФТИ (Долгопрудный, Россия. Ноябрь 25-30, 2013), XIV International Workshop on Algebraic and Combinatorial Coding Theory (Svetlogorsk, Russia. September 7-13, 2014), 57-й научной конференции МФТИ (Долгопрудный, Россия. Ноябрь 24-29, 2014), Международная конференция «Инжиниринг и Телекоммуникации» En&T (Долгопрудный, Россия. Ноябрь 15-19, 2015), XV International Workshop on Algebraic and Combinatorial Coding Theory (Albena, Bulgaria. June 18-24, 2016), International Symposium on Problems of Redundancy in Information and Control Systems (St. Petersburg, Russia. September 26-29, 2016).

Кроме того, основные результаты докладывались на семинарах кафедры радиотехники и систем управления МФТИ, на семинаре по теории кодирования ИППИ РАН, а также в форме стендового доклада в IEEE European School of Information Theory 2015.

Диссертационная работа является частью работ по гранту РФФИ, проекты № 12-07-00122-а и № 15-07-08480-а.

Публикации. По теме диссертации опубликовано 9 работ [1–9], из них 2 в научных журналах, 7 публикаций в трудах научных конференций.

Личный вклад в работах с соавторами. В совместных публикациях научному руководителю Э.М. Габидулину принадлежат постановки задач, а основные результаты и выкладки выполнены диссертантом. В работе [1] соавторам принадлежит аналитический обзор методов секретности, аналитический обзор методов анонимности выполнен диссертантом.

Объем и структура работы. Диссертация состоит из введения, 3 глав и заключения. Общий объем диссертации составляет 102 страницы, включая 19 рисунков, 1 таблицу и список литературы.

Содержание работы

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

Первая глава посвящена введению в анонимную передачу данных. В *разделе 1.1* даны основные определения.

Для того чтобы определить анонимность некоторого объекта, необходимо предположить наличие множества объектов со схожими характеристиками, которое называют множеством анонимности, а также необходимо определить модель злоумышленника.

Система терминов, описывающих анонимную передачу данных, начала формироваться в 2000 году А. Пфицманом[2].

Объект называется анонимным с точки зрения злоумышленника, если злоумышленник не может достоверно выделить его среди множества других схожих объектов[2].

Пусть до наблюдения за некоторыми объектами у злоумышленника есть предположение об их взаимодействии. Объекты называются несвязываемыми (unlinkable), если после наблюдения за ними предположение злоумышленника не становится более достоверным[2].

Удобно определять анонимность через несвязываемость. Так можно определить анонимность сеанса связи, которой посвящена диссертационная работа.

Сеанс связи, то есть процесс передачи сообщения, называется анонимным, если по отношению к этой паре отправитель–получатель каждое передаваемое сообщение является несвязываемым[2] .

Задачу анонимной передачи данных можно разделить на две задачи. Первая – задача секретной маршрутизации. Традиционно эта проблема решается следующим образом. Маршруты устанавливаются статически некоторым секретным способом. То есть таким, при котором маршрутная информация не передается явно по сети.

Но секретной маршрутизации недостаточно для анонимной передачи, так как данные, содержащиеся в сообщении, не меняются в течение всей передачи по маршруту, тогда на их основе можно прослеживать сообщение. Рассмотрим сеть, представленную на рисунке 1. Предположим, злоумышленник прослушал сообщение m некоторого отправителя, то есть прослушал соединение $s \to r_1$. Затем он прослушивает все выходные соединения узла r_1 и сравнивает данные пакетов, передающихся по этим соединениям, с данными пакета m, подслушанного на предыдущем шаге. Совпадение данных однозначно определяет соединение, по которому далее было отправлено сообщение m. Действуя по этой схеме, злоумышленник может проследить передачу сообщения вплоть до получателя, установив таким образом, кому именно передавал сообщение конкретный отправитель. Эта атака принадлежит широкому классу атак, носящему название анализ трафика (traffic analysis).

Вторая задача анонимной передачи состоит в противодействии этой атаке. Сообщение по уже установленному маршруту должно передаваться так, чтобы его нельзя было прослеживать на основе его содержимого. Решение состоит в обеспечении битовой несвязываемости (bitwise

[2]Pfitzmann A., Hansen M. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. 2010. // http://dud.inf.tudresden.de/literatur/Anon_terminology_v0.34.pdf.

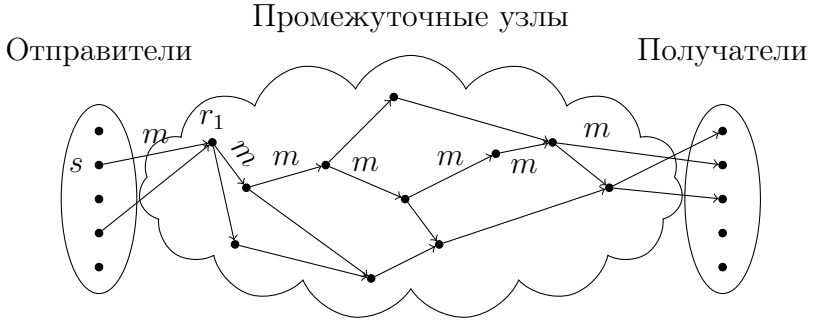


Рис. 1. Схема сети передачи данных

unlinkability). Битовая несвязываемость сообщений гарантирует, что они выглядят по-разному, то есть нельзя найти закономерностей в битовых последовательностях этих сообщений.

Раздел 1.2 посвящен описанию моделей злоумышленника. Злоумышленник может быть пассивным или активным в зависимости от того, просто ли он прослушивает передаваемые по сети сообщения или может вставлять в процесс передачи свои собственные сообщения. Далее злоумышленники делятся на глобальных, которые имеют доступ ко всем соединениям сети, и локальных, которые имеют доступ только к подмножеству соединений. Также злоумышленник может быть адаптивным или статическим в зависимости от того способен ли он во время проведения атаки менять стратегию на основе получаемых им данных. Наконец, выделяют внешнего и внутреннего злоумышленников. Внутренний злоумышленник участвует в передаче сообщений в роли легального узла, в то время как внешний злоумышленник, напротив, никак не участвует в передаче сообщений, а имеет доступ только к соединениям сети.

Разделы 1.3 и 1.4 посвящены сравнительному анализу существующих методов анонимности для традиционной маршрутизации и сетевого кодирования соответственно. Анализ демонстрирует, что основной метод обеспечения несвязываемости сообщений принадлежит к криптографическому подходу и реализован посредством шифрования.

Раздел 1.5 посвящен сравнительному анализу численных характеристик анонимности, которые раскрывают понятие «достоверности», используемое в определениях анонимности.

В *разделе 1.6* вводится понятие совершенной несвязываемости сообщений.

Обозначим через f некоторый алгоритм, который преобразовывает сообщение M, являющееся случайной величиной, в сообщение $X \in \mathbb{X}$ для его последующей передачи, $f : \mathbb{M} \to \mathbb{X}$. В общем случае функция f не является детерминированной. Пусть X^{in} является входным сообщением некоторого промежуточного узла. Пусть выходное сообщение этого промежуточного узла, соответствующее сообщению X^{in}, описывается случайной величиной X^{out}. Определим *совершенную несвязываемость* сообщений.

Определение 1. *Сообщения X^{in} и X^{out} называются совершенно несвязываемыми, если выполняется $I(X^{in}; X^{out}|M) = 0$.*

Совершенная несвязываемость гарантирует, что наблюдая сообщения, принадлежащие одному сеансу связи, в разных точках маршрута, нельзя установить, что эти сообщения действительно принадлежат одному сеансу связи.

Пусть подслушав сообщение X^{in}, злоумышленник получил W^{in}, то есть $W^{in} = g(X^{in})$, $g : \mathbb{X} \to \mathbb{W}$, а подслушав X^{out}, он получил W^{out}. Тогда

Определение 2. *Сообщения X^{in} и X^{out} называются совершенно несвязываемыми с точки зрения злоумышленника, если $I(W^{in}; W^{out}|M) = 0$.*

Использование условной взаимной информации подчеркивает, что информация, полученная злоумышленником, то есть сообщения W^{in}, W^{out} относятся к одному и тому же сеансу связи. В общем случае информационное сообщение M может быть как известно злоумышленнику, так и неизвестно. Для методов, предлагаемых в диссертационной работе, показана необходимость того, чтобы сообщение M не было известно злоумышленнику.

В *разделе 1.6* сделаны выводы к главе.

Вторая глава посвящена изложению теоретико-информационных методов обеспечения несвязываемости сообщений для цифрового когерентного сетевого кодирования и традиционной маршрутизации.

В *разделе 2.1* введены основные понятия из алгебры и теории кодирования.

В *разделе 2.2* изложен принцип сетевого кодирования. Сетевое кодирование обобщает идею маршрутизации, позволяя промежуточным узлам выполнять любое преобразование над поступившими пакетами. Наиболее изучено линейное сетевое кодирование, идея которого состоит в том, что промежуточные узлы передают дальше линейные комбинации принятых пакетов. Если векторы коэффициентов, с помощью которых формируются линейные комбинации и которые носят названия кодирующих векторов, задаются централизованно до начала передачи, то сетевое кодирование называется когерентным. Линейная зависимость между пакетами, поступающими в узел и отправляемыми им, может использоваться злоумышленником для компрометации корреспондентов посредством прослеживания сообщения, как это было рассмотрено ранее на примере, изображенном на рисунке 1.

В *подразделе 2.2.1* приведены необходимые для дальнейшего понимания сведения из теории ранговых кодов. В *подразделе 2.2.2* даны теоретические обоснования линейного сетевого кодирования.

Предлагаемый во второй главе метод обеспечения несвязываемости основан на использовании кодирования смежными классами, предложенного для канала с подслушиванием типа II, которому посвящен *раздел 2.3*. Этот канал был предложен Л. Озаровым и А. Вайнером[3]. Они

[3]Ozarow L.H., Wyner A.D. Wire-Tap Channel II // Advances in Cryptology Lecture Notes in Computer Science. 1985. Vol. 209. P. 33-50.

рассматривали секретную передачу сообщения по каналу с отводом. Канал с отводом можно представить как два дискретных канала без памяти: основной и отводный. Основной – это канал между источником и получателем, передача по которому происходит без ошибок, а отводный – канал между источником и злоумышленником, который является каналом со стираниями. Предположим, источник хочет передать по каналу сообщение S, состоящее из k символов. Злоумышленник способен прослушивать любое подмножество J передаваемых символов мощности не более чем заданная $|J| = \mu$. Пусть W – вектор длины n, который определяет информацию, поступающую к злоумышленнику. Тогда μ элементов этого вектора известны, а в остальных символах W произошли стирания. Совершенная секретность, условие которой задается в виде $I(S;W) = 0$, может быть достигнута таким образом, что отправителю и получателю сообщения не нужно обладать каким-либо общим секретом. Это реализуется с помощью группового кода. Множество $\{0,1\}^n$ разбивается на 2^k подмножеств $\{A_m\}_{m=1}^{2^k}$ одинаковой мощности $|A_m| = 2^{n-k}$. Пусть $\mathbf{H}$ – проверочная матрица размера $k \times n$ и ранга k. Разбиение $\{A_m\}$ определяет код, заданный $\mathbf{H}$, и его смежные классы. Чтобы закодировать сообщение $S \in \{0,1\}^k$, кодер произвольным образом выбирает X как один из 2^{n-k} элементов смежного класса, определяемого синдромом S. Если код с проверочной матрицей $\mathbf{H}$ есть код с максимальным расстоянием (МДР), тогда можно передать k символов секретно при $\mu \leq n - k$.

Пусть n символов сообщения X передаются по сети, работающей по принципу сетевого кодирования. Д. Силва и Ф. Кшишанг[4] доказали, что если $\mathbf{H}$ – проверочная матрица кода с максимальным ранговым расстоянием (МРР кода), то сообщение может быть передано совершенно секретно при любом сетевом коде, то есть при любом наборе кодирующих векторов.

В *разделе 2.4* представлен метод обеспечения несвязываемости в случае пассивного злоумышленника.

Подраздел 2.4.1 содержит описание модели сети. Сеть представляется направленным мультиграфом $G(V,E)$, вершины V которого есть узлы сети, а ребра E – соединения единичной пропускной способности. Это значит, что в единицу времени по каждому соединению передается один пакет данных. Сообщения передаются по принципу когерентного сетевого кодирования без ошибок.

В *подразделе 2.4.2* обсуждается модель злоумышленника. Рассматривается два вида злоумышленника. Первый – внешний адаптивный пассивный локальный. Этот злоумышленник может прослушивать не более, чем μ входных соединений некоторого узла и не более, чем μ выходных соединений. Второй вид злоумышленника – внешний адаптивный пассивный глобальный. Он может прослушивать все соединения сети.

Д. Силва и Ф. Кшишанг[4] предложили конкретную схему кодирования смежными классами

[4]Silva D., Kschischang R. Univelsal Secure Network Coding via Rank-Metric Codes // IEEE Trans. Inf. Theory. 2011. Vol. 57. No. 2. P. 1124-1135.

для сетевого кодирования. Эта схема используется в настоящей работе для кодирования источника и рассматривается в *подразделе 2.4.3*. Обозначим через C $(n, n-k)$ MPP код над полем $\mathbb{F}_{q^m}$ с порождающей матрицей $\mathbf{G} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ и проверочной матрицей $\mathbf{H} \in \mathbb{F}_{q^m}^{k\times n}$. Предположим, источник хочет секретно передать информационное сообщение $\mathcal{S} \in \mathbb{F}_{q^m}^{k}$. Вектор $\mathcal{X}$ можно представить в виде

$$\mathcal{X} = \mathbf{P}^\top \mathcal{S} + \mathbf{G}^\top \mathcal{V}, \tag{1}$$

где $\mathbf{P} \in \mathbb{F}_{q^m}^{k\times n}$ – произвольная матрица такая, что $\mathbf{H}\mathbf{P}^\top = \mathbf{I}_k$, а $\mathcal{V} \in \mathbb{F}_{q^m}^{(n-k)}$ – случайный независимый от $\mathcal{S}$ вектор с равномерным распределением. Вектор $\mathcal{X}$ принадлежит смежному классу, который задается синдромом $\mathcal{S}$, и имеет равномерное распределение в этом смежном классе. Этот метод кодирования обеспечивает совершенно секретную передачу сообщения $\mathcal{S}$, если злоумышленник прослушивает не более, чем $\mu \leq n-k$ элементов вектора $\mathcal{X}$.

В *подразделе 2.4.4* излагается метод обеспечения несвязываемости. Его суть заключается в следующей известной лемме[5]. Пусть X и Y – независимые случайные величины, заданные на конечном поле. Если X имеет равномерное распределение, то $Z = X + Y$ также имеет равномерное распределение и не зависит от Y.

Для обеспечения несвязываемости эта лемма применяется следующим образом. Пусть промежуточный узел принял сообщение $\mathcal{X}^{in}$. Рассмотрим вектор

$$\mathcal{X}^{out} = \mathcal{X}^{in} + \mathbf{G}^\top \mathcal{V}' = \mathbf{P}^\top \mathcal{S} + \mathbf{G}^\top (\mathcal{V} + \mathcal{V}'), \tag{2}$$

где $\mathcal{V}'$ равномерно распределен на $\mathbb{F}_{q^m}^{n-k}$ и не зависит от $\mathcal{X}^{in}$. Вектор $\mathcal{X}^{out}$ принадлежит смежному классу, задаваемому $\mathcal{S}$, то есть тому же смежному классу, что и $\mathcal{X}^{in}$. Следовательно, $\mathcal{X}^{out}$ передает ту же информацию что и $\mathcal{X}^{in}$. Так как вектор $\mathcal{V}'$ имеет равномерное распределение, а векторы $\mathcal{X}^{in}$ и $\mathcal{X}^{out}$ принадлежат смежному классу, который есть конечное множество, то справедлива

Теорема 1. *При заданном $\mathcal{S}$ вектор $\mathcal{X}^{out}$ равномерно распределен и не зависит от $\mathcal{X}^{in}$.*

По теореме 1 выполняется

$$I(\mathcal{X}^{out}; \mathcal{X}^{in} | \mathcal{S}) = 0.$$

Локальный злоумышленник, прослушав μ входных соединений узла, получает $\mathcal{W}^{in} = \mathbf{B}^{in}\mathcal{X}^{in}$, где строки матрицы $\mathbf{B}^{in} \in \mathbb{F}_q^{\mu\times n}$ суть кодирующие векторы прослушанных соединений. Прослушав μ выходных соединений, злоумышленник получает $\mathcal{W}^{out} = \mathbf{B}^{out}\mathcal{X}^{out}$.

Теорема 2. *Пусть $\mathcal{W}^{in} = \mathbf{B}^{in}\mathcal{X}^{in}$, $\mathcal{W}^{out} = \mathbf{B}^{out}\mathcal{X}^{out}$, векторы $\mathcal{X}^{in}$ и $\mathcal{X}^{out}$ равномерно распределены и независимы при заданном $\mathcal{S} \in \mathbb{F}_{q^m}^{k}$, $\mathbf{B}^{in}, \mathbf{B}^{out} \in \mathbb{F}_q^{\mu\times n}$, $\mathrm{Rk}\mathbf{B}^{in} = \mathrm{Rk}\mathbf{B}^{out} = \mu$, $\mu \leq n-k$. Тогда векторы $\mathcal{W}^{in}$ и $\mathcal{W}^{out}$ независимы при заданном $\mathcal{S}$.*

[5]Rizzi A. Statistical methods for Cryptography, Data Analysis and Classification // Proc. of the 6th Conference of the Classification and Data Analysis Group of the Societa Italiana di Statistica. 2010. P. 13-21.

По теореме 2 выполняется

$$I(\mathcal{W}^{out}; \mathcal{W}^{in} | \mathcal{S}) = 0,$$

следовательно, с точки зрения злоумышленника сообщения также будут совершенно несвязываемыми.

Раздел 2.5 посвящен методу несвязываемости сообщений в случае активного злоумышленника, который может не только прослушивать пакеты, но и вставлять ограниченное число своих пакетов. Действия активного злоумышленника в сети, где данные передаются без ошибок, можно рассматривать как действия пассивного злоумышленника в сети с ошибками. В этом случае меняется способ кодирования источника.

В *подразделе 2.5.1* описывается способ кодирования источника для передачи с ошибками, также предложенный Д. Силвой и Ф. Кшишангом. Смежные классы кода покрывают все пространство, на котором задан код. Для обеспечения возможности исправления ошибок смежными классами кода нужно покрывать не все пространство, а подпространство. Другими словами, нужно использовать два вложенных кода, один из которых покрывается смежными классами другого.

В *пункте 2.5.2* разработан метод обеспечения несвязываемости сообщений, который аналогичен методу, представленному в подразделе 2.4.4, а именно, он состоит в суммировании принятого вектора со случайным кодовым вектором кода C_2. Показано, что возникающие аддитивные ошибки, которые суть вредоносные пакеты злоумышленника, не нарушают несвязываемости, что обеспечивается теоремами 1 и 2. Кратко это можно объяснить следующим образом. Сумма нескольких величин, заданных над конечным полем, одна из которых имеет равномерное распределение, также имеет равномерное распределение и не зависит от остальных слагаемых. Следовательно, выходное сообщение не зависит от входного даже при наличии вставленных ошибочных пакетов.

В *разделе 2.6* представлен теоретико-информационный метод обеспечения несвязываемости для традиционной маршрутизации, который основан на той же идее использования кодирования смежными классами.

В *подразделе 2.6.1* рассмотрена модель сети, в *подразделе 2.6.2* – модель злоумышленника, который является пассивным локальным внешним адаптивным. Локальность злоумышленника заключается в том, что он может прослушивать не более, чем μ входных пакетов входящего сообщения и не более μ пакетов выходящего сообщения.

В стандартах 100 гигабитного Ethernet для исправления ошибок используется код Рида-Соломона. Структура порождающей матрицы кода Рида-Соломона позволяет использовать метод кодирования источника, рассмотренный в подразделе 2.5.1, что показано в *подразделе 2.6.3*.

Метод обеспечения несвязываемости идейно аналогичен представленному в подразделе 2.5.2 методу, что показано в *подразделе 2.6.4*.

Анализ предложенных методов обеспечения несвязываемости представлен в *разделе 2.7. Подраздел 2.7.1* посвящен анализу стойкости методов. Показано, что секретность является необходимым условием для обеспечения совершенной несвязываемости. Приведена атака, демонстрирующая, что совершенная несвязываемость невозможна в случае глобального злоумышленника. В *подразделе 2.7.2* приводится анализ сложности методов. Сложность метода обеспечения несвязываемости для сетевого кодирования составляет $O(nm^2)$ операций в $\mathbb{F}_q$, где n – длина кодового слова, а m – степень расширения поля, а сложность метода для традиционной маршрутизации оценивается сложностью кодирования кода Рида-Соломона.

В *разделе 2.8* сформулированы выводы ко второй главе.

В **третье главе** представлен теоретико-информационный метод обеспечения несвязываемости сообщений для аналогового сетевого кодирования. Предлагаемый метод основан на кодировании смежными классами для алгебраических решёток.

В *разделе 3.1* изложен принцип аналогового сетевого кодирования. Под аналоговым понимается сетевое кодирование, которое используется на физическом уровне, то есть применяется непосредственно к передаваемым сигналам. Аналоговое сетевое кодирование было разработано для беспроводных сетей. Принцип аналогового сетевого кодирования основан на использовании широковещательной природы беспроводных сетей: сигналы, отправленные некоторыми источниками, получают все узлы, находящиеся в зоне действия источников, следовательно, если сигналы отправляются одновременно, то узлы получают их сумму. Беспроводной канал моделируют гауссовским каналом, для которого успешно применяются коды на алгебраических решётках.

В *подразделе 3.2.1* изложены основные результаты теории решеток в евклидовом пространстве[6]. Пусть $g_1, g_2, \dots g_n \in \mathbb{R}^n$ – линейно независимые векторы и $\mathbf{G} = (g_1\ g_2 \dots g_n)$. Решётка Λ – это множество вида

$$\Lambda = \{\lambda = \mathbf{G}z : z \in \mathbb{Z}^n\},$$

матрица $\mathbf{G}$ называется порождающей матрицей решётки. Минимальное множество $\mathcal{P}_0$, удовлетворяющее условию

$$\dot{\bigcup_{x \in \mathcal{P}_0}} \Lambda_x = \mathbb{R}^n, \text{ где } \Lambda_x = \Lambda + x = \{\lambda + x : \lambda \in \Lambda\},$$

называется фундаментальной областью решётки, а Λ_x – смежный класс решетки. Можно определить операцию квантования вектора x как $\lambda = Q_{\mathcal{P}_0}(x)$, а

$$x_e = x \mathrm{mod}_{\mathcal{P}_0} \Lambda = x - Q_{\mathcal{P}_0}(x) \tag{3}$$

называется ошибкой квантования. Можно определить квантайзер Вороного

$$Q_\Lambda(x) = \arg\min_{\lambda \in \Lambda} \|x - \lambda\|, \tag{4}$$

[6]Zamir R. Lattice Coding for Signals and Networks. Cambridge University Press, 2014.

где $\|\cdot\|$ – евклидова норма. Множество

$$\mathcal{V}_\lambda(\Lambda) = \{x : Q_\Lambda(x) = \lambda \in \Lambda\}$$

называется ячейкой Вороного точки λ. Ячейка Вороного нулевой точки решётки $\mathcal{V}_0(\Lambda)$ является фундаментальной областью. Две решётки Λ_1 и Λ_2 называются вложенными $\Lambda_2 \subset \Lambda_1$, если базисные векторы решётки Λ_2 представляют собой целочисленные линейные комбинации базисных векторов решётки Λ_1. Пусть $\mathcal{P}_0(\Lambda_2)$ является некоторой фундаментальной областью решётки Λ_2. Множество $\Lambda_1 \cap \mathcal{P}_0(\Lambda_2)$ является фундаментальной областью решётки Λ_2 относительно решётки Λ_1. Тогда

$$\Lambda_1 = \dot{\bigcup_{\lambda \in \Lambda_1 \cap \mathcal{P}_0(\Lambda_2)}} (\lambda + \Lambda_2).$$

В *разделе 3.2.2* описана конкретная схема передачи для аналогового сетевого кодирования, предложенная Б. Нейзером и М. Гастпаром[7]. Эта схема использует коды на решётках.

Предлагаемый в этой главе метод несвязываемости основан на кодировании смежными классами для гауссовского канала с подслушиванием. Гауссовский канал с подслушиванием принадлежит к классу каналов с подслушиванием типа I, который рассматривается в *разделе 3.2*. Канал с подслушиванием типа I был предложен А. Вайнером[8]. Он рассматривал два дискретных канала: основной и отводный. Основной – это канал между источником и получателем с входным алфавитом $\mathbb{X}$, выходным алфавитом $\mathbb{Y}$ и матрицей переходных вероятностей $P_{Y|X}(y|x)$, а отводный – канал между источником и злоумышленником с входным алфавитом $\mathbb{X}$, выходным алфавитом $\mathbb{W}$ и матрицей переходных вероятностей $P_{W|X}(w|x)$. Секретность при передаче по такому каналу достигается за счет физических ограничений, накладываемых на злоумышленника.

Было показано, что секретность, условие которой задается в виде $\lim\limits_{n\to\infty} I(S;W) = 0$, достигается в том случае, если канал злоумышленника зашумлен больше, чем основной канал, то есть $I(U;Y) \geq I(U;W)$ для всех цепей Маркова $U \to X \to (Y,W)$.

Для достижения секретности А. Вайнер предложил идею, суть которой состоит в том, чтобы не использовать всю пропускную способность основного канала для передачи информации, а резервировать часть пропускной способности для передачи случайных символов, которые призваны запутать злоумышленника. Эта идея предъявляет требование к конструкции кода. Код C должен состоять из множества подкодов $\{C_1, C_2, \ldots C_{|\mathbb{M}|}\}$. Источник каждому сообщению M ставит в соответствие $C_M,\ M = 1, 2 \ldots, |\mathbb{M}|$ и передает случайно выбранное из C_M кодовое слово $X \in \mathbb{X}$. Информативной частью сообщения X является индекс подкода, которому оно принадлежит. Идея А. Вайнера реализуется, если мощность подкодов не менее $2^{nI(X;W)}$. Это приводит

[7]Nazer B., Gastpar M. Compute-and-forward: Harnessing interference through structured codes // IEEE Trans. Inf. Theory. 2011. Vol. 57. No. 10. P. 6463-6486.

[8]Wyner A.D. The wire-tap channel // The Bell System Technical Journal. 1975. Vol. 54. No 8. P. 1355-1387.

к тому, что вся пропускная способность канала злоумышленника расходуется на случайные символы.

В криптографии широко используется понятие семантической секретности. Для канала с подслушиванием семантическую секретность определяют следующим образом[9]. Сообщение M семантически секретно, если

$$\lim_{n\to\infty} \sup_{f,M}(2^{-H_\infty(f(M)|W)} - 2^{-H_\infty(f(M))}) = 0,$$

где $H_\infty(M) = -\log_2(\max\limits_m P(M = m))$ и супремум берется по всем случайным величинам M, заданным на $\mathbb{M}$ и всем функциям f на множестве $\mathbb{M}$. Семантическая секретность достигается, если[9]

$$\exists\gamma > 0, n_0 : \ \forall n > n_0 \ \max_{P(M)} I(M;W) \leq e^{-n\gamma}, \tag{5}$$

где максимум берется по всем распределениям исходного сообщения M.

Если основной и отводный канал представляют собой гауссовские каналы, то говорят о гауссовском канале с подслушиванием.

Критерий криптостойкости используемого кода для гауссовского канала с подслушиванием задается уровнем плато решётки. Для заданной решётки Λ можно определить Λ-периодическое гауссовское распределение как

$$f_{\sigma,\Lambda}(x) = \sum_{\lambda\in\Lambda} f_{\sigma,\lambda}(x) = \frac{1}{(\sqrt{2\pi}\sigma)^n} \sum_{\lambda\in\Lambda} e^{-\frac{\|x-\lambda\|^2}{2\sigma^2}}. \tag{6}$$

Уровень плато для решётки Λ и параметра σ определяется как[10]

$$\epsilon_\Lambda(\sigma) = \max_{x\in\mathcal{P}_0(\Lambda)} \left| \frac{f_{\sigma,\Lambda}(x)}{\frac{1}{V(\Lambda)}} - 1 \right|.$$

По гауссовскому каналу с подслушиванием можно передавать сообщения семантически секретно (5), если уровень плато решётки экспоненциально убывает. Если для последовательности решеток Λ_n выполняется $\epsilon_{\Lambda_n} = e^{-\Omega(n)}$, то такая последовательность называется криптостойкой[10].

Прежде чем решать задачу для общего случая гауссовского канала, часто сначала рассматривают упрощенную версию, а именно modΛ гауссовский канал. Этот канал характеризуется тем, что на выходе канала выполняется операция взятия по модулю решётки (3). В *разделе 3.3* представлен теоретико-информационный метод обеспечения несвязываемости сообщений для этого случая.

---

[9] Bellare M., Tessaro S., Vardy A. A Cryptographic Treatment of the Wiretap Channel // https://arxiv.org/abs/1201.2205.

[10] Ling C., Luzzi L., Belfiore J.-C., Stehlé D. Semantically secure lattice codes for the gaussian wiretap channel // IEEE Trans. Inf. Theory. 2014. Vol. 60. P. 6399-6416.

В *подразделе 3.3.1* представлена модель беспроводной сети, особенностью которой является то, что соединения сети представляют собой $\mathrm{mod}\Lambda$ гауссовские каналы.

К. Линг с соавторами предложил метод кодирования смежными классами для $\mathrm{mod}\Lambda$ гауссовского канала с подслушиванием, где отводный канал зашумлен более, чем основной[10]. В настоящей работе этот метод используется для кодирования источника. Ему посвящен *подраздел 3.3.2*. В $\mathbb{R}^n$ заданы n-мерные решётки $\Lambda_s \subset \Lambda_a \subset \Lambda_r$. Решётка Λ_r используется для передачи информации. Решётка Λ_a задает случайные символы, которые призваны запутать злоумышленника. Эта решётка должна быть криптостойкой. Решётка Λ_s используется в качестве «огибающей» – именно по модулю этой решётки берется выход канала. Каждому сообщению источника $m \in \mathbb{M}$ ставится в соответствие $\lambda_m \in \Lambda_r \cap \mathcal{P}_0(\Lambda_a)$. Источник равномерно выбирает точку $\lambda \in \Lambda_a \cap \mathcal{V}_0(\Lambda_s)$ и отправляет $\mathcal{X} = \lambda_m + \lambda$. Точка $\mathcal{X}$ принадлежит смежному классу $\Lambda_a + \lambda_m$ и равномерно распределена в этом смежном классе. Авторы метода показали, что сообщение m передается семантически секретно.

Семантическая секретность метода кодирования источника гарантирует, что вероятность ошибки декодирования злоумышленником точек решётки Λ_r может быть сколь угодно близкой к единице. При этом злоумышленник способен декодировать точки решётки Λ_a, что показано в *подразделе 3.3.3*, где рассматривается модель злоумышленника. Это означает, что получив $\mathcal{W}$, злоумышленник может восстановить точку $\lambda \in \Lambda_a \cap \mathcal{V}_0(\Lambda_s)$, которая составляет случайную часть сообщения $\mathcal{X}$. В этом же подразделе показано как злоумышленник может использовать эту возможность для компрометации анонимности. В том, что злоумышленник может восстановить только случайную часть сообщения и заключается локальность рассматриваемого злоумышленника, который также является внешним и пассивным.

Метод обеспечения несвязываемости представлен в *подразделе 3.3.4*. Пусть

$$\mathcal{X}^{in} = \lambda_m + \lambda_1,\ \lambda_m \in \Lambda_r \cap \mathcal{P}_0(\Lambda_a),\ \lambda_1 \in \Lambda_a \cap \mathcal{V}_0(\Lambda_s).$$

Рассмотрим

$$\mathcal{X}^{out} = (\mathcal{X}^{in} + \lambda_2)\mathrm{mod}\Lambda_s,$$

где λ_2 выбирается равномерно на $\Lambda_a \cap \mathcal{V}_0(\Lambda_s)$ и независимо от $\mathcal{X}^{in}$. Выражение для $\mathcal{X}^{out}$ можно преобразовать к виду

$$\mathcal{X}^{out} = \lambda_m + (\lambda_1 + \lambda_2)\mathrm{mod}\Lambda_s.$$

Лемма 1. *Пусть точка λ_2 равномерно распределена на $\Lambda_a \cap \mathcal{V}_0(\Lambda_s)$. Тогда точка $\hat{\lambda} = (\lambda_1 + \lambda_2)\mathrm{mod}\Lambda_s$ равномерна на $\Lambda_a \cap \mathcal{V}_0(\Lambda_s)$ и не зависит от λ_1.*

Следовательно, случайные части сообщений $\mathcal{X}^{in}$ и $\mathcal{X}^{out}$ независимы. Лемма 1 приводит к следующему результату.

Теорема 3. *При заданной точке λ_m точка $\mathcal{X}^{out}$ имеет равномерное распределение и не зависит от $\mathcal{X}^{in}$.*

Из теоремы 3 следует, что

$$I(\mathcal{X}^{out}; \mathcal{X}^{in} | \lambda_m) = 0.$$

Методу несвязываемости для канала общего вида посвящен *раздел 3.4*. Кодирование источника для гауссовского канала с подслушиванием общего вида, предложенный также К. Лингом и его соавторами, представлен в *подразделе 3.4.1*.

Рассматриваются две заданные на $\mathbb{R}^n$ вложенные решётки $\Lambda_a \subset \Lambda_r$. Источник устанавливает взаимно однозначное соответствие между множеством сообщений $\mathbb{M} = \{1, \ldots, 2^{nR}\}$ и множеством смежных классов, то есть каждому $m \in \mathbb{M}$ ставится в соответствие $\lambda_m \in \Lambda_r \cap \mathcal{P}_0(\Lambda_a)$. В отсутствии внешней решётки Λ_s решётка Λ_a представляет собой счетное множество, на котором нельзя задать равномерное распределение. Авторы предлагают выбирать случайную часть сообщения согласно дискретному гауссовскому распределению, заданному на решётке Λ_a.

Дискретное гауссовское распределение на решётке Λ с центром в $\mu \in \mathbb{R}^n$ задается функцией распределения[10]

$$D_{\Lambda,\sigma,\mu}(\lambda) = \frac{f_{\sigma,\mu}(\lambda)}{f_{\sigma,\Lambda}(\mu)}, \ \forall \lambda \in \Lambda,$$

где $f_{\sigma,\Lambda}(\mu)$ – периодическое распределение (6). Случайная часть сообщения λ выбирается согласно распределению $D_{\Lambda_a,\sigma_s,-\lambda_m}$. Тогда итоговое сообщение $\mathcal{X} = \lambda_m + \lambda$ распределено на смежном классе $\Lambda_a + \lambda_m$ по закону $D_{\Lambda_a+\lambda_m,\sigma_s,0}$. Авторы метода показали, что сообщение m передается семантически секретно, если решётка Λ_a криптостойкая.

Другими авторами было предложено использовать этот метод кодирования для сети, где сообщения передаются по принципу аналогового сетевого кодирования, но не было дано строгих обоснований этого[11]. Для обоснования того, что метод можно с канала распространить на сеть, обеспечивая при этом тот же уровень секретности и надежности передачи, необходимо показать, что сумма точек решётки, имеющих дискретное гауссовское распределение, также имеет дискретное гауссовское распределение. Это сделано в *подразделе 3.4.2*, посвященном модели сети.

Теорема 4. *Пусть $\mathcal{X}_1$ имеет распределение $D_{\Lambda,\sigma_1,\mu_1}$, а $\mathcal{X}_2$ распределение $D_{\Lambda,\sigma_2,\mu_2}$, и пусть уровень плато решётки Λ с параметром $\frac{\sigma_1\sigma_2}{\sqrt{\sigma_1^2+\sigma_2^2}}$ удовлетворяет условию $\epsilon_\Lambda(\frac{\sigma_1\sigma_2}{\sqrt{\sigma_1^2+\sigma_2^2}}) = \epsilon < \frac{1}{6}$. Рассмотрим $\mathcal{Y} = \mathcal{X}_1 + \mathcal{X}_2$. Статистическое расстояние между распределением величины $\mathcal{Y}$ и распределением $D_{\Lambda,\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}$ не превосходит 12ϵ, то есть $\sum\limits_{y\in\Lambda} |P_{\mathcal{Y}}(y) - D_{\Lambda,\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)| \leq 12\epsilon$.*

[11]Forutan V., Fischer R.F.H. On the Security of Lattice-based Physical-layer Network Coding Against Wiretap Attacks // Proc. of 10th ITG International Conference on Systems, Communications and Coding. Hamburg, Germany. February 2-5, 2015 P. 1-5.

Получив сообщение, промежуточные узлы восстанавливают целочисленную линейную комбинацию точек решётки. В *подразделе 3.4.3*, посвященному несвязываемости сообщений, показано, что после декодирования у промежуточных узлов останется линейная комбинация только информационных частей сообщений, то есть $\sum\limits_j a_j\lambda_{m_j},\ a_j \in \mathbb{Z}$. Передавать далее сообщение в этом виде нельзя, так как это нарушает секретность и не дает возможности обеспечить несвязываемость. Предлагается действовать следующим образом. Получившееся после декодирования сообщение промежуточные узлы снова кодируют по методу, который используют источники и который рассмотрен в подразделе 3.3.4. Другими словами, промежуточные узлы выбирают новую случайную часть сообщения $\tilde{\lambda}$ с распределением $D_{\Lambda_a,\sigma_s,-\sum\limits_j a_j\lambda_{m_j}}$. Дальше передается точка

$$\mathcal{X}^{out} = \sum_j a_j\lambda_{m_j} + \tilde{\lambda}.$$

Точка $\mathcal{X}^{out}$ принадлежит тому же смежному классу, что и принятая промежуточным узлом точка

$$\mathcal{X}^{in} = \sum_j a_j\mathcal{X}_j^{in} = \sum_j a_j\lambda_{m_j} + \sum_j a_j\lambda_j,$$

так как определяет смежный класс информационная часть сообщения $\sum\limits_j a_j\lambda_{m_j}$, которая одинакова у $\mathcal{X}^{out}$ и $\mathcal{X}^{in}$. Так как точка $\tilde{\lambda}$ выбирается независимо от принятой точки, то точки $\mathcal{X}^{in}$ и $\mathcal{X}^{out}$ несвязываемы.

Анализ предложенного метода обеспечения несвязываемости представлен в *разделе 3.5. Подраздел 3.5.1* посвящен анализу стойкости метода. Показано, что секретность является необходимым условием для обеспечения несвязываемости. В *подразделе 3.5.2* приводится анализ сложности метода. Сложность метода в случае modΛ канала определяется вычислением квантайзера Вороного (4), что является ключевой операцией кодирования и декодирования решётчатых кодов и в общем случае имеет экспоненциальную сложность. Поясняется в каком случае эта операция упрощается. Для канала общего вида основные вычислительные затраты приходятся на то, чтобы выбрать точку $\tilde{\lambda}$ согласно дискретному гауссовскому распределению. Наиболее известный алгоритм, решающий эту задачу, имеет сложность $O(n^4 \log_2^2 b)$, где b – максимальная норма базисных векторов решётки[12].

Выводы к главе сформулированы в *разделе 3.6*.

В **заключении** сформулированы основные результаты диссертационной работы.

Для цифрового когерентного сетевого кодирования, традиционной маршрутизации и аналогового сетевого кодирования разработаны и теоретически обоснованы методы обеспечения совершенной несвязываемости сообщений, проведён анализ стойкости и сложности предложенных методов.

[12]Klein P. N. Finding the closest lattice vector when it's unusually close // Proc. of the 11th Annual ACM-SIAM Symposium on Discrete Algorithms. San Francisco, California, USA. January 9-11, 2000. P. 937-941 .

Список публикаций

[1] Габидулин Э.М., Пилипчук Н.И., Трушина О.В. Защита информации в телекоммуникационных сетях // Труды МФТИ. 2013. Т. 5. №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] Gabidulin E., Trushina O. Anonymous and Secure Network Coding // Proc. of 7th International Workshop on Optimal Codes and Related Topics. Albena, Bulgaria. September 6-13, 2013. P. 85-90.

[4] Trushina O. Anonymous Coherent Network Coding Against Active Adversary // Proc. of XV Wnternational Workshop on Algebraic and Combinatorial Coding Theory. Albena, Bulgaria. June 18-24, 2016. P. 278-283.

[5] Габидулин Э.М., Трушина О.В. Метод анонимной и секретной передачи данных в сетях с сетевым кодированием // Труды 56-й научной конференции МФТИ. Долгопрудный, Россия. Ноябрь 25-30, 2013. С. 34-35.

[6] Trushina O. Towards to Anonymity in Physical-Layer Network Coding // Proc. of XIV International Workshop on Algebraic and Combinatorial Coding Theory. Svetlogorsk, Russia. September 7-13, 2014. P. 319-323.

[7] Трушина О.В. Обеспечение независимости передаваемых сообщений в гауссовском канале с подслушиванием // Труды 57-й научной конференции МФТИ. Долгопрудный, Россия. Ноябрь 24-29, 2014. С. 196-197.

[8] Трушина О.В. Об анонимности в беспроводной сети // Труды конференции Инжиниринг & Телекоммуникации - En&T. Долгопрудный, Россия. Ноябрь 18-19, 2015. С. 48-50.

[9] 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