Национальный исследовательский ядерный университет «МИФИ»

На правах рукописи

Белозубова Анна Игоревна

МЕТОД ПРОТИВОДЕЙСТВИЯ УТЕЧКЕ ИНФОРМАЦИИ ПО СКРЫТЫМ КАНАЛАМ ПО ВРЕМЕНИ В СЕТЯХ ПАКЕТНОЙ ПЕРЕДАЧИ ДАННЫХ

2.3.6 — методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Москва — 2025

Работа выполнена в Федеральном государственном автономном образовательном учреждении высшего профессионального образования «Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ).

Научный руководитель: **Епишкина Анна Васильевна**
Кандидат технических наук, доцент, Национальный исследовательский ядерный университет «МИФИ», заведующая кафедрой №42 «Криптология и кибербезопасность»

Официальные оппоненты: **Душкин Александр Викторович**
доктор технических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники», профессор кафедры информационной безопасности

Королёв Вадим Иванович
доктор технических наук, профессор, Федеральный исследовательский центр «Информатика и управление» Российской Академии Наук (ФИЦ ИУ РАН), профессор, ведущий научный сотрудник

Тулинова Анастасия Викторовна
кандидат технических наук, Федеральное государственное унитарное предприятие «Научно-исследовательский институт «Квант», научно-исследовательское отделение, главный специалист научно-технического отдела защиты информации в распределенных информационных системах

Защита состоится «7» апреля 2026 года в 15 час. 00 мин. на заседании диссертационного совета МИФИ.2.05 на базе «Национального исследовательского ядерного университета «МИФИ» по адресу: 115409, Москва, Каширское шоссе, д. 31, тел.: +7(499)324-87-66, +7(495)788-56-99.

С диссертационной работой можно ознакомиться в библиотеке «Национального исследовательского ядерного университета «МИФИ» и на сайте http://ods.mephi.ru.

Просим принять участие в работе совета или прислать отзыв в двух экземплярах, заверенный печатью организации.

Автореферат разослан _____2026

Ученый секретарь диссертационного совета Кессаринский Л.Н.

Общая характеристика работы

Актуальность работы. Информационные технологии широко применяются в процессах хранения, обработки и передачи информации в различных сферах деятельности человека и государства. Множество серверов, баз данных и оконечных устройств обработки информации, включая компоненты информационных систем, в которых хранится информация ограниченного доступа, связывает между собой сеть передачи данных. Это предъявляет требования к защите информации от угроз, осуществляемых с использованием возможностей сетей пакетной передачи данных. С учетом повсеместного распространения IP-сетей особо актуальной становится угроза негласного использования структурных особенностей протокола IP для скрытой передачи информации по каналам связи, выходящим за пределы защищаемого периметра.

В ГОСТ Р 53113.1 скрытым каналом называется коммуникационный канал, не предусмотренный разработчиком систем информационных технологий и автоматизированных систем, который может быть применен для нарушения политики безопасности. Существование скрытого канала в информационной системе несет угрозу нарушения конфиденциальности и целостности информационных ресурсов и программного обеспечения. В связи с этим, потенциальное наличие скрытого канала является серьезной проблемой информационной безопасности организации и требует принятия мер по предотвращению или ограничению его функционирования. Скрытые каналы опасны тем, что они не используют традиционные способы скрытой передачи информации и поэтому остаются «невидимыми» для распространенных средств защиты информации. Исследованием скрытых каналов занимается ряд отечественных и зарубежных ученых (Галатенко В.А., Грушо А.А., Тимонина Е.Е., Зандер С., Кабук С., Кеммерер Р.А., Кундюр Д., Лэмпсон Б.В. и другие). Проблема утечки информации, которой посвящена диссертационная работа, входит в Перечень приоритетных проблем научных исследований в области обеспечения информационной безопасности Российской Федерации.

Для любого сетевого оборудования и других вычислительных средств невозможно обеспечить полную уверенность в отсутствии недекларированных возможностей программно-аппаратного обеспечения и создание доверенной

замкнутой среды обмена информацией. Испытания в лабораторных условиях аппаратных комплексов, аудит открытого кода на предмет наличия скрытых возможностей в программном обеспечении представляют собой наукоемкие и длительные процедуры, даже после выполнения, которых невозможно гарантировать безопасность используемых технологий, а стандартные меры защиты информации, такие как шифрование или туннелирование трафика, не устраняют возможность передачи информации по некоторым видам скрытых каналов. Так, например, наличие функционала скрытой передачи информации в сетевом оборудовании компаний Huawei и Juniper, мобильных телефонах компании Apple, компьютерах с операционной системой Windows XP было обнаружено благодаря опубликованным Э. Сноуденом документам, в которых описывались программные и аппаратные закладки HEADWATER, HALLUXWATER, COTTONMOUTH, DROPOUTJEEP, SOMBERKNAVE и другие. Наличие подобных недекларированных возможностей не было обнаружено ранее, несмотря на то, что оборудование компаний широко распространено и исследовано. Опубликованная информация о кибератаках на коммерческие организации также подтверждает наличие существенных бизнес-рисков от утечек информации через скрытые каналы. Так, например, известно об использовании скрытых каналов в атаке на SolarWinds (SUNBURST), хакерской группировкой OilRig (APT34), в инструментах для шпионажа Pingback и Regin. Эти примеры подчеркивают необходимость исследования мер защиты от скрытых каналов в IP-сетях.

Требования и рекомендации по ограничению и подавлению скрытых каналов установлены в ГОСТ Р ИСО/МЭК 15408-2-2013, ГОСТ Р 53113.1-2008, ГОСТ Р ИСО/МЭК 27002-2012, Приказах ФСТЭК России №31, №239, №138, №131. Рекомендации по ограничению пропускной способности скрытых каналов приводят также зарубежные эксперты. Специалисты IBM Knowledge Center и авторы критериев определения безопасности компьютерных систем (Trusted Computer System Evaluation Criteria) отмечают, что скрытые каналы с пропускной способностью выше, чем 100 бит/с, недопустимы в информационной системе.

На практике используются три подхода к противодействию утечке информации по скрытым каналам: обнаружение, устранение скрытых каналов и ограничение их пропускной способности. Обнаружение скрытых каналов позволяет эффективно

использовать канал связи, но не гарантирует полную защиту от утечки информации. Это подтверждено исследованиями Грушо А.А., показавшего, что противник, знающий схему контроля в системе защиты, может создать необнаруживаемый контролирующим субъектом скрытый канал. Устранение скрытых каналов, заключающееся в фиксировании параметров IP-трафика или в построении инфраструктуры информационных систем и каналов связи, в которых на архитектурном уровне невозможно функционирование скрытых каналов, зачастую приводит к существенному снижению эффективности использования пропускной способности каналов связи, а также влечет за собой повышенную сложность эксплуатации такой инфраструктуры. Преимущество исследуемого в работе метода ограничения пропускной способности скрытых каналов заключается в контролируемом понижении пропускной способности коммуникационного канала при гарантированном активном противодействии утечке информации по скрытым каналам.

В работе исследуются скрытые каналы по времени, так как возможность их построения остается при использовании стандартных средств сетевой защиты, а полное подавление таких скрытых каналов может приводить к недопустимому понижению пропускной способности канала связи. Ограничение пропускной способности скрытых каналов реализуется двумя способами: частичной нормализацией параметров сетевого трафика и введением шума в скрытый канал. Для второго способа отсутствуют рекомендации по выбору значений параметров средств противодействия, реализующих данный подход, что послужило мотивацией для проведения настоящей работы. Одним из перспективных способов введения шума в скрытый канал является добавление случайных временных задержек перед отправкой IP-пакетов в коммуникационный канал, который исследуется в настоящей работе.

Целью диссертационной работы является предотвращение несанкционированной передачи информации ограниченного доступа по сетевым скрытым каналам по времени посредством введения дополнительных случайных задержек перед отправкой пакетов.

В диссертационной работе решается следующая научная задача: разработать методику ограничения пропускной способности сетевых скрытых каналов по времени, основанную на введении дополнительных случайных задержек перед отправкой

пакетов, позволяющую снижать пропускную способность скрытого канала до заданного значения.

В соответствии с поставленной целью в диссертационной работе решаются следующие задачи:

- выявление направлений исследования путём аналитического обзора способов построения сетевых скрытых каналов по времени и способов противодействия утечке информации по таким скрытым каналам;
- разработка способов оценки пропускной способности сетевых скрытых каналов по времени в условиях отсутствия противодействия и в условиях введения дополнительных случайных задержек перед отправкой пакетов с учетом характера распределения значений времени следования пакетов в сети;
- создание метода введения дополнительных случайных задержек перед отправкой пакетов для противодействия утечке информации по сетевым скрытым каналам по времени;
- разработка методики противодействия утечке информации по сетевым скрытым каналам по времени, основанным на изменении интенсивности передачи пакетов и длин межпакетных интервалов, путем ограничения их пропускной способности.

Научная новизна диссертационной работы заключается в следующем:

1. Впервые предложены способы оценки пропускной способности скрытых каналов, основанных на изменении интенсивности передачи пакетов и длин межпакетных интервалов, в условиях отсутствия противодействия и в условиях введения задержек перед отправкой пакетов с учётом временных характеристик следования трафика в коммуникационном канале, позволяющие определить необходимость введения противодействия.

2. Предложен метод противодействия утечке информации по рассматриваемым сетевым скрытым каналам по времени, заключающийся во введении задержек перед отправкой пакетов, значения которых различным образом распределены на некотором интервале. Предложенный метод противодействия позволяет, в отличие от существующих, снижать пропускную способность скрытого канала до заданного значения с сохранением приемлемой пропускной способности коммуникационного канала.

3. Разработана методика противодействия утечке информации по рассматриваемым сетевым скрытым каналам по времени, отличающаяся от известных тем, что она применима в случае, когда политикой информационной безопасности допускается наличие в информационной системе скрытого канала и устанавливается допустимое значение его пропускной способности.

Теоретическую значимость представляют:

- способ оценки максимальной пропускной способности скрытых каналов, основанных на изменении интенсивности передачи пакетов и длин межпакетных интервалов, в условиях отсутствия противодействия;
- способ оценки максимальной пропускной способности рассматриваемых сетевых скрытых каналов в условиях введения противодействия;
- методика противодействия утечке информации по рассматриваемым сетевым скрытым каналам по времени путем введения дополнительных случайных задержек перед отправкой пакетов.

Практическая ценность и внедрение результатов исследования. Разработанная методика противодействия утечке информации по сетевым скрытым каналам по времени используется при построении систем защиты информации на предприятиях группы компаний ПАО «ГМК «Норильский никель». В ООО «Триметр» внедрение методики противодействия утечке информации, основанной на управляемом введении случайных задержек в сетевой трафик, позволило снизить нагрузку на коммуникационный канал на 38%. Разработанные программные средства внедрены в автоматизированный программный комплекс компании ООО «ИБС Платформикс», позволяющий контролировать и анализировать параметры удаленного подключения сотрудников к автоматизированным рабочим местам, располагающимся внутри защищенной инфраструктуры. Разработанная методика противодействия утечке информации по сетевым скрытым каналам по времени и разработанные программные средства для ее реализации используются в компании АО «АМТ-Груп» при проектировании и внедрении средств защиты информации. Полученные результаты исследования применяются в рамках проведения лабораторных работ при реализации образовательного курса «Защита информации от утечки по скрытым каналам» кафедры №42 «Криптология и кибербезопасность» Национального исследовательского ядерного университета «МИФИ».

Имеются четыре свидетельства о государственной регистрации программ для ЭВМ.

Основными методами исследования, используемыми в работе, являются методы теории информации, теории вероятности, дифференциального и интегрального исчисления.

Достоверность и обоснованность положений и выводов диссертационной работы обеспечивается корректным использованием математического аппарата, а также апробацией предложенной методики противодействия утечке информации по сетевым скрытым каналам по времени и полученными в её результате значениями параметров противодействия.

Основные положения, выносимые на защиту:

1. Способ оценки пропускной способности скрытых каналов, основанных на изменении интенсивности передачи пакетов и длин межпакетных интервалов, в условиях отсутствия противодействия и в условиях введения противодействия.

2. Метод введения дополнительных случайных задержек перед отправкой пакетов для понижения пропускной способности сетевых скрытых каналов по времени.

3. Алгоритм выбора значения параметра метода противодействия утечке информации по скрытым каналам, основанным на изменении интенсивности передачи пакетов и длин межпакетных интервалов.

4. Методика противодействия утечке информации по сетевым скрытым каналам по времени, основанным на изменении интенсивности передачи пакетов и длин межпакетных интервалов, путем введения дополнительных случайных задержек перед отправкой пакетов.

Публикации и апробация работы. Результаты диссертационной работы изложены в 14 опубликованных работах, в том числе в четырех научных статьях в изданиях, включенных в Перечень ВАК, семи научных статьях в журналах, индексируемых международной системой научного цитирования Scopus. Имеются четыре свидетельства о государственной регистрации программ для ЭВМ. Результаты работы докладывались на конференциях и семинарах различного уровня, в том числе на:

- конференции российских молодых исследователей в области электротехники и электроники 2021 (2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering);

- конференции российских молодых исследователей в области электротехники и электроники 2018 (2018 IEEE Russia Young Researchers in Electrical and Electronic Engineering Conference);

- 24-й и 28-й научно-технических конференциях «Методы и технические средства обеспечения безопасности информации»;

- 18-й Средиземноморской электротехнической конференции MELECON (18th Mediterranean Electrotechnical Conference MELECON);

- европейской конференции по информационной безопасности (European Intelligence and Security Informatics Conference);

- XXII всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы».

Личный вклад автора. Все основные результаты работы получены автором самостоятельно и единолично. В публикациях в соавторстве автору принадлежат: анализ и классификация сетевых скрытых каналов [15], систематизация возможностей нарушителя [16], формулы для расчета остаточной пропускной способности скрытого канала [1-6, 13, 17], рекомендации по выбору значений параметра метода противодействия утечке информации по скрытому каналу [13, 14, 17], формулы для расчета остаточной пропускной способности скрытых каналов при генерации фиктивного трафика и рекомендации по выбору значений параметра метода противодействия утечке информации [12], доработанный метод противодействия утечке информации, основанный на введении дополнительных случайных задержек перед отправкой пакетов [11].

Структура и объем работы. Диссертация состоит из введения, четырех разделов, заключения, списка литературы, включающего 204 наименования, и одиннадцати приложений. Диссертация изложена на 125 страницах, не включая приложения, с 48 рисунками и 14 таблицами.

Содержание диссертации соответствует пунктам: Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет (п.5), Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия

нарушениям и компьютерным атакам в компьютерных сетях (п.6), Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования (п.7), Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения (п.8), Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности (п.15), Методы, модели и средства разработки безопасного программного обеспечения, выявления в нем дефектов безопасности, противодействия скрытым каналам передачи данных и выявления уязвимостей в компьютерных системах и сетях (п.17) паспорта специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность.

Основное содержание работы

Во введении обосновывается актуальность темы диссертации, проводится обзор предметной области, определяется цель, формулируются задачи исследования, описываются структура и логика диссертационной работы.

В первом разделе проводится аналитический обзор результатов в области построения сетевых скрытых каналов (ССК) и противодействия утечке информации с их использованием. Выявлено, что особое внимание следует уделять защите от сетевых скрытых каналов по времени (ССКВ), так как возможность их построения остается и при использовании стандартных средств сетевой защиты. В результате проведенного исследования способов ограничения пропускной способности ССК выявлено, что актуальной задачей является разработка метода введения дополнительных случайных задержек перед отправкой пакетов для ограничения пропускной способности ССКВ до заданного значения

Под скрытым каналом в ГОСТ Р 53113.1 понимается не предусмотренный разработчиком систем информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности. Различные рекомендации и требования по контролю скрытых каналов в автоматизированных системах приведены в ГОСТ Р 53113.2, ГОСТ Р ИСО/МЭК

15408, Приказах №76, №31, №239, №138 ФСТЭК России. Зарубежные специалисты IBM, NIST, авторы TCSEC рекомендуют ограничивать пропускную способность скрытых каналов. Ограничение пропускной способности сетевых скрытых каналов реализуется путем нормализации параметров передаваемых пакетов и путем введения шума в скрытый канал. При этом способ введения шума в скрытый канал исследован недостаточно, отсутствуют рекомендации по выбору параметров средств противодействия, реализующих данный подход. Принципиально важно исследование методов ограничения пропускной способности скрытых каналов до заданного уровня допустимой пропускной способности и получение рекомендаций по выбору параметров таких способов противодействия.

Второй раздел посвящен разработке способа оценки пропускной способности скрытых каналов, основанных на изменении интенсивности передачи пакетов (ССК-1) и длин межпакетных интервалов (ССК-2), с учетом времени следования пакетов в сети в условиях отсутствия противодействия утечке информации. Пропускная способность ССК-1 и ССК-2 с учетом наиболее распространенных условий в сети пакетной передачи данных (СППД) определяется по формуле

$$C = \max_{X}\left(\frac{I(X,Y)}{t}\right), \qquad (1)$$

где I — взаимная информация случайных величин X, Y, описывающих входные и выходные характеристики скрытого канала, t — среднее время передачи пакетов. Взаимная информация вычисляется по формуле:

$$I(X,Y) = H(Y) - H(Y \mid X), \qquad (2)$$

где $H(Y) = -\sum_{y\in\{0,1\}} p_{\text{вых}}(y)\log_2 p_{\text{вых}}(y)$ — энтропия случайной величины Y, $H(Y \mid X) = -\sum_{x\in\{0,1\}} p_{\text{вх}}(x)\sum_{y\in\{0,1\}} p(y \mid x)\log_2 p(y \mid x)$ — условная энтропия случайной величины Y относительно случайной величины X. Считаем, что символы, передаваемые по скрытому каналу, подаются на вход с вероятностями $p_{\text{вх}}(0) = q,\ p_{\text{вх}}(1) = p = 1 - q.$

Пусть в ССК-1 информация передается через значения интенсивности передачи пакетов: ноль и значение, отличное от нуля. Таким образом, пакет отправляется в интервале t, если необходимо послать значение «1», и не отправляется — если значение «0». Получатель отмеряет интервалы длиной t. Каждый интервал времени t, в течение

которого был получен пакет, соответствует «1», в ином случае — «0». Ниже на рисунке 1 показана передача сообщения «01101» по ССК-1.

В ССК-2 пакеты отправляются с интервалом t_0, если необходимо послать значение «0», и с интервалом t_1 — если значение «1». Тогда длина межпакетного интервала на стороне получателя, лежащая в пределах (0; $t_{гр}$), соответствует «0», а превышающая $t_{гр}$ — «1», где $t_{гр}$ — граничное значение длины межпакетного интервала, определяемое как $t_{гр}=(t_0+t_1)/2$. На рисунке 2 схематично изображена передача сообщения «00110» с использованием ССК-2. Длина межпакетного интервала в ССК-2 определяется моментами прибытия на сторону получателя двух подряд пришедших пакетов.

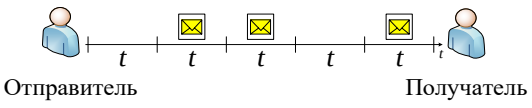

Рисунок 1 — Передача сообщения «01101» в ССК-1

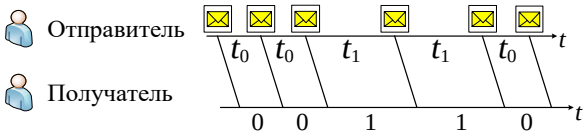

Рисунок 2 — Передача сообщения «00110» в ССК-2

При этом на функционирование ССКВ могут влиять задержки в сети, приводящие к возникновению шума в скрытом канале, поэтому далее в работе учитывается характер распределения случайной величины, определяющей время следования пакетов в сети от отправителя к получателю (ВСП). Под временем следования пакетов в сети (ВСП) в работе считается временная задержка от момента отправки пакета узлом-отправителем до момента его приёма получателем или на точке наблюдения. Проведенный анализ существующих работ показал, что чаще всего ВСП подчиняется нормальному и экспоненциальному законам распределения. При этом нормальное распределение ВСП описывает трафик, в котором задержки формируются в результате действия множества факторов, что характерно для сети Интернет. Экспоненциальное распределение ВСП описывает простые пакетные очереди при малом объеме трафика, в ограниченном временном интервале, при малом количестве узлов обработки пакетов на маршруте его следования, что может быть использовано как базовая модель при оценке пропускной способности ССКВ для дальнейшего развития модели и сравнения с другими законами распределения ВСП.

Во втором разделе предложен способ оценки пропускной способности ССК-1 и ССК-2, основанный на применении методов теории информации. Выражения для

расчета условных вероятностей получения символов в скрытом канале используются для определения пропускной способности ССК-1 и ССК-2 в условиях различных распределений ВСП. Оценена пропускная способность ССК-1 и ССК-2 в условиях, когда ВСП определяется нормальным и экспоненциальным законами распределения, а вероятность появления символов в скрытом канале не фиксирована. Определены предельные значения пропускной способности ССК-1 и ССК-2 посредством оптимизации параметров скрытых каналов.

В третьем разделе предложен метод противодействия утечке информации по сетевым скрытым каналам по времени, основанный на введении дополнительных случайных задержек перед отправкой пакетов. Данный метод позволяет понизить пропускную способность скрытого канала до заданного допустимого значения.

Метод противодействия заключается в добавлении дополнительных случайных временных задержек перед перемещением IP-пакетов в канал связи для передачи получателю. Таким образом реализуется введение шума в скрытый канал, что приводит к возникновению ошибок в скрытом канале и, как следствие, снижению его пропускной способности. Для ССК-1 введение задержек может приводить к тому, что отправленный в определенном интервале времени t пакет придет на стороне получателя в следующем интервале t. Введение задержек перед отправкой пакетов в ССК-2 изменяет длину межпакетных интервалов и приводит к тому, что межпакетные интервалы длиной t_0 могут превращаться в интервалы длиной t_1 на стороне получателя и наоборот.

На рисунках 3 и 4 показана отправка сообщения «01011» в ССК-1 и «0101» в ССК-2 соответственно и введение задержки τ перед отправкой пакетов, которое приводит к возникновению ошибок в скрытых каналах.

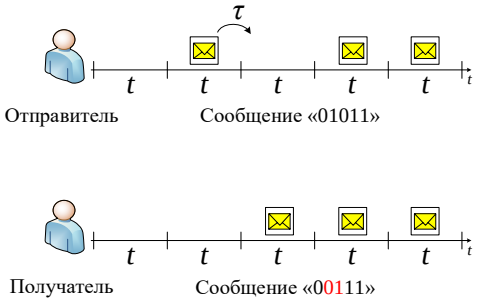

Рисунок 3 — Появление ошибок в ССК-1 из-за введения задержек перед отправкой пакетов

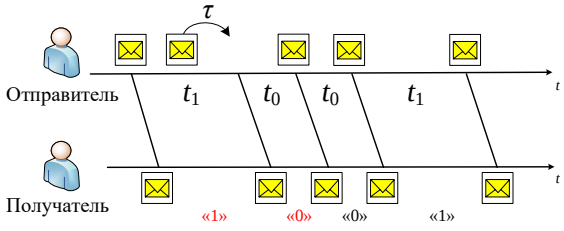

Рисунок 4 — Появление ошибок в ССК-2 из-за введения задержек перед отправкой пакетов

С целью повышения неопределенности для противника при попытке распознать фактическое время отправки пакета длину дополнительных временных задержек предлагается выбирать не постоянной, а распределенной по некоторому закону на интервале (0; *d*). Далее в работе исследовано два класса распределения значений задержек:

- равномерное распределение на интервале (0; *d*);
- распределение на интервале (0; *d*) с невозрастающей функцией плотности распределения.

Введение задержек с невозрастающей функцией плотности распределения может обеспечить снижение нагрузки на канал связи по сравнению со способом, когда значения задержек выбираются по равномерному закону распределения на некотором интервале, сохранив при этом значение остаточной пропускной способности ССКВ не выше допустимого. Это обуславливается тем, что малые величины задержек будут генерироваться чаще, таким образом, среднее время передачи пакетов от отправителя к получателю увеличится меньше.

С целью выработки рекомендаций по выбору значений количественных параметров предложенного метода противодействия утечке информации, заключающегося во введении дополнительных задержек перед отправкой IP-пакетов, были разработаны способы оценки пропускной способности ССКВ в условиях введения метода противодействия с учетом наиболее распространенных условий в СППД. Пропускная способность ССК-1 и ССК-2 представлена функцией от параметров скрытых каналов, метода противодействия и характеристик нагрузки на сеть. Так, например, в случае, когда ВСП распределено по нормальному и экспоненциальному законам распределения, условные вероятности распознавания символов в ССК-1 определяются по формулам

$$p(0\,|\,0) = (1-q)F(t+t_{\min}-\tau)+q \qquad (3)$$
$$p(0\,|\,1) = (1-q)F(t+t_{\min}-\tau)\left[1-F(t+t_{\min}-\tau)\right]+q\left[1-F(t+t_{\min}-\tau)\right],$$

г

д

е Полученные формулы позволяют определить значения параметров метода противодействия, при которых предельная пропускная способность соответствующих *C* скрытых каналов не превышает допустимого значения. Достигнутые результаты могут

–

быть использованы для различных видов функций распределения значений задержек, что предоставляет возможность сравнения нагрузки на канал связи.

В четвертом разделе описана методика противодействия утечке информации по ССК-1 и ССК-2. Методика позволяет определить необходимость введения метода противодействия утечке информации путем добавления задержек перед отправкой пакетов, а также понизить пропускную способность скрытого канала до заданного уровня, минимизировав дополнительную нагрузку на канал связи и снижение его эффективной пропускной способности.

На рисунке 5 представлена блок-схема методики противодействия утечке информации по рассматриваемым скрытым каналам. Методика состоит из шести этапов, которые подробно описаны в диссертационной работе. Четвертый этап методики включает в себя алгоритм выбора значения параметра метода противодействия утечке информации по ССКВ, который позволяет снизить пропускную способность скрытого канала до заданного уровня.

Для использования методики необходимы следующие входные данные:

- требования политики информационной безопасности, действующей на защищаемом объекте и определяющей величину допустимой пропускной способности скрытого канала $C_{доп}$;
- временные характеристики сетевого трафика в коммуникационном канале: набор величин, определяющих ВСП от устройства во внутренней сети до пограничного межсетевого экрана.

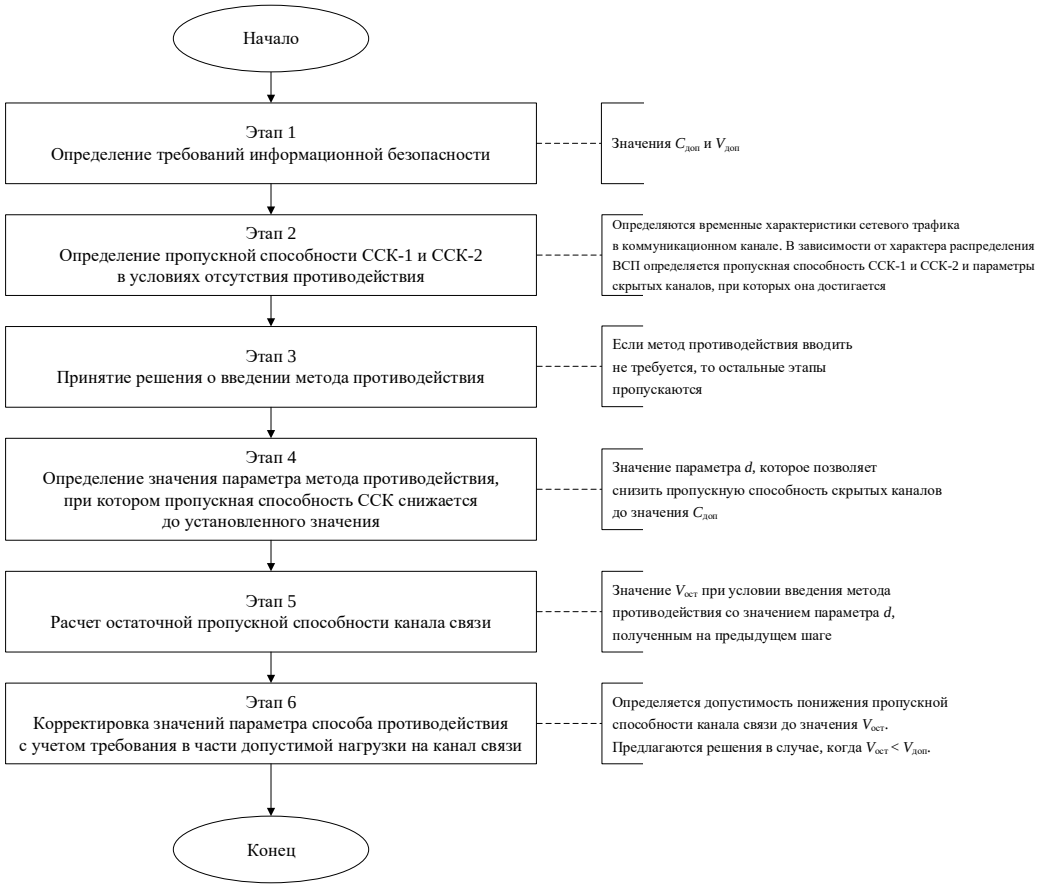

Рисунок 5 — Блок-схема методики противодействия утечке информации по сетевым скрытым каналам по времени

При использовании данной методики принимаются следующие допущения:

- рассматриваются ССК-1 и ССК-2;
- устройство (аппаратный / программный комплекс), при помощи которого злоумышленник передает информацию по скрытому каналу, находится в пределах контролируемой сетевой зоны, имеет доступ к защищаемой информации и способно модулировать длительность межпакетных интервалов в трафике, следуемом за границу контролируемой сетевой зоны;
- злоумышленник принимает информацию, передающуюся по скрытому каналу, после границы контролируемой сетевой зоны;
- величины, определяющие ВСП от устройства во внутренней сети до пограничного межсетевого экрана, подчиняются либо нормальному закону распределения (НЗР), либо экспоненциальному закону распределения (ЭЗР). Если такой набор величин не аппроксимируется НЗР или ЭЗР с заданной точностью, то считается, что ВСП определяется величиной, имеющей равномерное распределение на некотором интервале.

Ниже на рисунках 6, 7 представлены графики зависимости пропускной способности ССК-1 от параметра *d* (левая ось ординат) и параметра скрытого канала *t* от параметра *d* (правая ось ординат), которые были построены таким образом, что для каждого значения параметра *d* было определено наилучшее значение параметра *t* и *q*. Здесь под «наилучшим» подразумевается набор параметров, обеспечивающих максимальную пропускную способность ССК-1 в заданных условиях противодействия. На рисунке 6 значения задержек генерируются согласно бета-распределению, на рисунке 7 — согласно равномерному распределению.

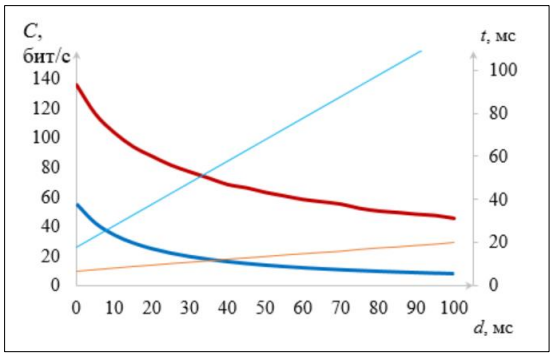

Рисунок 6 — График зависимости пропускной способности *C* ССК-1 от *d* и график зависимости *t* от *d* при нормальном распределении ВСП для ССК-1 без ошибок и с ошибками при генерации значений задержек по бета-распределению

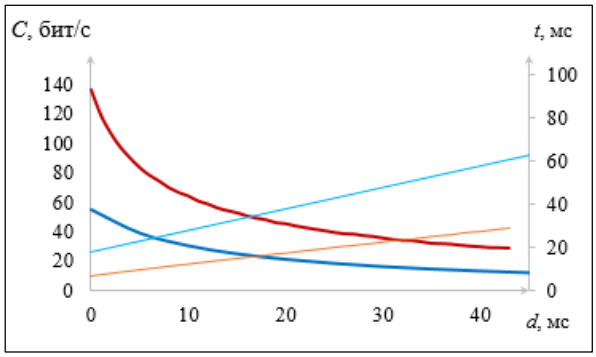

Рисунок 7 — График зависимости пропускной способности *C* ССК-1от *d* и график зависимости *t* от *d* при нормальном распределении ВСП для ССК-1 без ошибок и с ошибками при генерации значений задержек по равномерному распределению

На графиках изображены:

- значения пропускной способности ССК-1 без ошибок — синей линией;
- значения параметра *t* ССК-1 без ошибок — голубой линией;
- значения пропускной способности ССК-1 с ошибками — красной линией;
- значения параметра *t* ССК-1 с ошибками — оранжевой линией.

Как видно из графиков, при введении противодействия нарушителю целесообразнее незначительно увеличивать параметр скрытого канала *t*, чем устанавливать передачу по скрытому каналу без ошибок.

Также по результатам проведенных исследований апробирована методика противодействия утечке информации по ССК для пакетного трафика в локальной сети с ВСП, определяющимся НЗР. Была оценена пропускная способность ССК-1 и ССК-2, изучено влияние параметров скрытых каналов на его пропускную способность в условиях введения противодействия, в заключение даны рекомендации по выбору

параметров метода противодействия, позволяющие снизить пропускную способность ССК-1 и ССК-2 до допустимых величин. Некоторые результаты, полученные в ходе апробации методики противодействия утечки информации по ССК, приведены в таблице 1.

Таблица 1 — Сравнительная таблица для ССК-1 и ССК-2 в условиях нормального распределения времени следования пакетов в сети

	Пропускная способность ССК, бит/с	Пропускная способность ССК при противодействии, бит/с	*d*, мс
ССК-1	136,26	97,49	3
ССК-2	404,52	144,68	25

В таблице 1 представлены значения пропускной способности ССК-1 и ССК-2 в условиях отсутствия и введения противодействия, а также значение параметра *d*, которое следует устанавливать для снижения пропускной способности скрытых каналов.

Основные результаты работы

В работе проведён цикл исследований, посвящённых проблеме утечке информации по сетевым скрытым каналам по времени и способам ограничения их пропускной способности. В работе получены следующие основные результаты:

1. Проведенный анализ существующих способов построения скрытых каналов в сетях пакетной передачи данных и способов противодействия утечке информации по данным каналам выявил актуальную задачу оценки пропускной способности таких скрытых каналов и разработки рекомендаций по выбору количественных характеристик методов противодействия скрытым каналам, основанным на изменении интенсивности передачи пакетов и длин межпакетных интервалов.

2. Разработанный способ оценки пропускной способности рассматриваемых сетевых скрытых каналов при отсутствии противодействия подтвердил необходимость исследования способов противодействия, так как при помощи этого способа обосновано, что при варьировании злоумышленником параметров канала с учётом характера сетевого трафика (распределения длин межпакетных интервалов) пропускная способность скрытого канала возрастает.

3. Предложенный метод противодействия утечке информации по рассматриваемым сетевым скрытым каналам, заключающийся во введении

дополнительных случайных задержек перед отправкой пакетов, обеспечивает предотвращение несанкционированной передачи информации ограниченного доступа из информационных систем, для работы которых необходима сетевая связность с объектами, расположенными за пределами защищенного контура.

4. Разработанный способ оценки пропускной способности рассматриваемых сетевых скрытых каналов в условиях введения метода противодействия учитывает наиболее распространенные условиях в сети, позволяет оценить остаточную пропускную способность скрытого канала с учетом характера распределения времени следования IP-пакетов и сравнить её с допустимым значением пропускной способности скрытого канала в защищаемой системе.

5. Разработанная методика противодействия утечке информации по изучаемым сетевым скрытым каналам и алгоритм выбора значений параметров метода противодействия утечке информации по скрытым каналам ограничивают утечку информации по таким каналам.

6. Предложенный способ генерации значений задержек согласно закону распределения с невозрастающей функцией плотности распределения уменьшает нагрузку на канал связи, сохраняя при этом остаточную пропускную способность скрытого канала ниже установленного допустимого значения.

7. Реализованные программные средства для расчета значений параметров разработанного метода противодействия утечке информации по скрытым каналам автоматизируют выбор необходимых значений параметров данного метода. Получены четыре свидетельства о государственной регистрации программ для ЭВМ.

Публикации по теме диссертации в рецензируемом журнале из международной базы данных Scopus:

1. Belozubova, A. Historical notes on Russian cryptography // A. Belozubova, A. Epishkina, S. Zapechnikov // Journal of Computer Virology and Hacking Techniques — 2024. — Pp. 277–293. (*Scopus, Web of Science, Q1*)

Публикации по теме диссертации в рецензируемых журналах из Перечня ВАК:

1. Белозубова А.И. Ограничение пропускной способности сетевых скрытых каналов по времени путем введения дополнительных случайных задержек перед отправкой пакета / А. И. Белозубова, К. Г. Когос, Лебедев Ф. В. // Безопасность информационных технологий. — 2021. — №4. — С. 74–89 (специальность 2.3.6, К2)
2. Белозубова А.И. Пропускная способность бинарных скрытых каналов по времени в различных условиях распределения времени следования пакетов в сети / А. И. Белозубова, А.В. Епишкина, К. Г. Когос // Системы высокой доступности. — 2021. — №1. — С. 41–50 (специальность 2.3.6, К2)
3. Белозубова А.И. Анализ существующих способов противодействия утечке информации по скрытым каналам в IP-сетях / А. И. Белозубова, К. Г. Когос, М. А. Финошин // Безопасность информационных технологий. — 2015. — №3. — С. 10–16 (специальность 2.3.6, К2)
4. Белозубова А.И. Об ограничении пропускной способности скрытых каналов в IP-сетях / А. И. Белозубова, К. Г. Когос // Безопасность информационных технологий. — 2015. — №1. — С. 61–63 (специальность 2.3.6, К2)

Материалы международных конференций, рецензируемые в базе Scopus:

1. Belozubova, A. On Hybrid Network Covert Channel Capacity / A. Belozubova, K. Kogos // 2022 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: The 13th Annual Meeting of the BICA Society. — 2022. — Pp. 453–462.
2. Belozubova, A. How to Limit Capacity of Timing Covert Channel by Adding Extra Delays / A. Belozubova, A. Epishkina, K. Kogos // Procedia Computer Science. — 2021. — Pp. 64–70. (*Scopus, Web of Science, Q2*).

3. Belozubova, A. On/Off Covert Channel Capacity Limitation by Adding Extra Delays / A. Belozubova, A. Epishkina, K. Kogos // ElConRus 2021. — 2021. — Pp. 2318–2322. (*Scopus, Web of Science, материалы конференции*).

4. Belozubova, A. Dummy Traffic Generation to Limit Timing Covert Channels / A. Belozubova, A. Epishkina, K. Kogos // IEEE Russia Section Young Researchers in Electrical and Electronic Engineering Conference, ElConRus. — 2018. — Pp. 1472–1476. (*Scopus, Web of Science, материалы конференции*).

5. Belozubova, A. Random Delays to Limit Timing Covert Channel / A. Belozubova, A. Epishkina, K. Kogos // Proceedings of the European Intelligence and Security Informatics Conference (EISIC) 2016. — 2016. — Pp. 188–191. (*Scopus, Web of Science, материалы конференции*).

6. Belozubova, A. Random delays to Limit On/Off covert channel / A. Belozubova, A. Epishkina, K. Kogos // Proceedings of the 18-th Mediterranean Electrotechnical Conference MELECON 2016. — 2016. — Pp. 915–919. (*Scopus, Web of Science, материалы конференции*).

Печатные работы в сборниках трудов всероссийских конференций, индексируемые в РИНЦ:

1. Белозубова А.И. Ограничение пропускной способности сетевого скрытого канала по времени с учетом распределения времени следования пакетов в сети / А. И. Белозубова, А.В. Епишкина, К. Г. Когос // Сборник научных трудов по материалам всероссийской научно-теоретической конференции «Теория и практика обеспечения информационной безопасности». — 2021. — №1. — С. 318–327. *(В рамках работы по гранту аспирантам и молодым ученым на исследования, направленные на обеспечение ИБ для задач цифровой экономики).*

2. Белозубова А. И. О введении задержек для противодействия утечке информации по скрытым каналам в IP-сетях / А. И. Белозубова, К. Г. Когос // Материалы 28-ой научно-технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург. — 2019. — С. 81–82. (*Всероссийская конференция*).

3. Белозубова, А. И. Об одном способе ограничения пропускной способности скрытых каналов в IP-сетях / А. И. Белозубова, К. Г. Когос // Материалы 24-ой научно-

технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург. — 2015. — С. 35–37. (*Всероссийская конференция*).

Свидетельства о государственной регистрации программ для ЭВМ:

1. Свидетельство о государственной регистрации программы для ЭВМ. Заявка 2021617417. Российская Федерация. Оценка объема информации, утечка которой возможна по скрытому каналу по времени, основанному на изменении длин межпакетных интервалов, в условиях нормального распределения длин межпакетных интервалов при введении противодействия путем генерации дополнительных случайных задержек / Автор и правообладатель Белозубова А.И. — №.2021617417; заявл. 29.04.21; опубл. 14.05.21.

2. Свидетельство о государственной регистрации программы для ЭВМ. Заявка 2021661048. Российская Федерация. Оценка объема информации, утечка которой возможна по скрытому каналу по времени, основанному на изменении скорости передачи пакетов, в условиях нормального распределения длин межпакетных интервалов при введении противодействия путем генерации дополнительных случайных задержек / Автор и правообладатель Белозубова А.И. — №.2021661048; заявл. 29.04.21; опубл. 05.07.21.

3. Свидетельство о государственной регистрации программы для ЭВМ. Заявка 2019666544. Российская Федерация. Оценка объема информации, утечка которой возможна по скрытому каналу по времени в условиях нормального распределения длин межпакетных интервалов / Автор и правообладатель Белозубова А.И. — №.2019666544; заявл. 29.11.19; опубл. 11.12.19.

4. Свидетельство о государственной регистрации программы для ЭВМ. Заявка 2019666545. Российская Федерация. Оценка объема информации, утечка которой возможна по скрытому каналу по времени в условиях равномерного распределения длин межпакетных интервалов / Автор и правообладатель Белозубова А.И. — №.2019666545; заявл. 29.11.19; опубл. 11.12.19.