На правах рукописи

Когос Константин Григорьевич

МЕТОД ПРОТИВОДЕЙСТВИЯ УТЕЧКЕ ИНФОРМАЦИИ ПО СКРЫТЫМ КАНАЛАМ, ОСНОВАННЫМ НА ИЗМЕНЕНИИ ДЛИН ПЕРЕДАВАЕМЫХ ПАКЕТОВ

Специальность: 05.13.19 — методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Автор: _____

Москва — 2015

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

Научный руководитель:

кандидат технических наук,
доцент кафедры
«Криптология и дискретная математика»
НИЯУ МИФИ — Епишкина Анна Васильевна

Официальные оппоненты:

доктор технических наук,
старший научный сотрудник,
ведущий научный сотрудник
Института проблем информационной
безопасности ФГБОУ ВО «МГУ имени
М. В. Ломоносова» — Казарин Олег Викторович

доктор технических наук,
доцент,
главный научный сотрудник
Управления перспективных
специальных средств и комплексов
обеспечения информационной
безопасности ФГАНУ «ЦИТиС» — Татузов Александр Леонидович

Ведущая организация: Федеральное государственное учреждение
«Федеральный исследовательский центр
«Информатика и управление»
Российской академии наук»

Защита состоится «16» декабря 2015 г. в 15:00 на заседании диссертационного совета Д 212.130.08 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 «___» октября 2015 г.

Ученый секретарь диссертационного совета Горбатов В.С.

Общая характеристика работы

Актуальность работы. На современном этапе развития информационных технологий и массового внедрения средств вычислительной техники в различные области и сферы деятельности человека постоянно возрастает актуальность проблем информационной безопасности, от качества решения которых во многом зависит успешное функционирование государственных и коммерческих организаций.

В настоящее время и на прогнозируемую перспективу сохранится тенденция широкого использования сетей пакетной передачи данных, что, в свою очередь, делает весьма значимой угрозу негласного использования нарушителем особенностей протокола IP для скрытой передачи информации ограниченного доступа по каналам связи, выходящим за пределы объектов информатизации, на которых она обрабатывается.

Необходимость создания и постоянного совершенствования способов противодействия утечке информации по так называемым скрытым каналам обусловлена и тем, что такие каналы могут быть построены в условиях применения традиционных способов сетевой защиты, заключающихся в межсетевом экранировании, туннелировании трафика и др. Исследования показывают, что данная угроза сохраняется даже при передаче информации в зашифрованном виде. Согласно отечественному стандарту ГОСТ Р 53113.2-2009, информация, связанная с размерами пакетов и временными интервалами между их появлением, может быть использована для организации скрытого канала в условиях туннелирования и шифрования трафика. Вопросами анализа скрытых каналов занимаются такие отечественные и зарубежные ученые, как Аникеев М.В., Грушо А.А., Матвеев С.В., Тимонина Е.Е., Зандер С., Кабук С., Кеммерер Р.А., Лэмпсон Б.В., Миллен Ж.К. и другие.

Значимость диссертационной работы подтверждена Перечнем приоритетных проблем научных исследований в области обеспечения информационной безопасности Российской Федерации (пункты 45, 48, 74), наличием в стандарте ГОСТ Р ИСО/МЭК 15408-2-2013 класса функциональных требований, касающихся ограничения и подавления скрытых каналов, а также регламентируемым ГОСТ Р 53113 подходом к противодействию утечке информации по скрытым каналам.

Особую актуальность рассматриваемой угрозе, связанной с утечкой информации по скрытым каналам, придают известные результаты исследований, согласно которым противник, который знает схему контроля в системе защиты, может создать невидимый для контролирующего субъекта скрытый канал как для управления программно-аппаратным агентом в компьютерной системе, так и для общения программно-аппаратных агентов в открытой среде между собой.

Метод, позволяющий гарантировать отсутствие в системе сетевых скрытых каналов, заключается в построении и поддержании замкнутых доверенных программно-аппаратных сред. Внедрение агента нарушителя в такие системы должно быть невозможно на любой стадии их жизненного цикла. При этом, ввиду повсеместного использования импортного оборудования и программного обеспечения, такой метод зачастую практически не реализуем, так как агент нарушителя может быть внедрен как на оконечных, так и на промежуточных узлах на пути следования трафика. Передача данных по каналам связи в зашифрованном виде не решает проблему утечки информации по некоторым классам сетевых скрытых каналов. Вместе с тем, исследование даже известного кода на предмет обнаружения программных закладок представляет собой трудоемкую научно-техническую задачу и становится практически невозможным при частом внесении изменений в программное обеспечение. Таким образом, реализация рассмотренного подхода, позволяющего предотвратить утечку информации по сетевым скрытым каналам, является нетривиальной задачей и не в любой системе может быть доведена до практического исполнения. Другой способ исключения условий функционирования сетевых скрытых каналов заключается в нормализации параметров пакетной передачи данных, то есть, в отправке пакетов фиксированной длины с фиксированными заголовками через равные промежутки времени, что приводит к существенному снижению эффективности использования пропускной способности каналов связи, увеличению стоимости их применения.

В силу отмеченных причин, в соответствии с ГОСТ Р 53113.1-2008, в случаях, когда регулирующие органы или собственник информации допускают возможность утечки некоторых объемов данных, рекомендуется использовать методы ограничения пропускной способности скрытых каналов. Такие методы применимы, если пропускная способность скрытого канала может быть ограничена до величины, меньшей установленного допустимого значения. Целесообразность использования указанных методов подтверждена данными компании IBM, согласно которым допустимо функционирование скрытых каналов с пропускной способностью до 0,1 бит/с, но в некоторых случаях возможно наличие потенциальных скрытых каналов с пропускной способностью до 100 бит/с. Применение рассмотренных методов на практике, в отличие от методов подавления скрытых каналов, позволяет обеспечивать высокую эффективную пропускную способность канала связи, гибко управлять эксплуатационными и стоимостными характеристиками телекоммуникационных систем. Данный подход позволяет гарантированно ограничить пропускную способность широкого класса скрытых каналов, независимо от способа их организации. Для построения таких методов необходимо получить и исследовать оценки пропускной способности скрытых каналов, функционирующих в условиях отсутствия и применения средств противодействия.

Кроме того, оценка пропускной способности скрытых каналов и оценка опасности, которую несет их скрытое функционирование, является одним из этапов по определению степени опасности скрытого канала в соответствии с ГОСТ Р 53113.1-2008.

В настоящей работе исследованы скрытые каналы, основанные на изменении длин передаваемых пакетов, так как, с одной стороны, такие каналы могут быть построены в условиях шифрования трафика, с другой стороны, их пропускная способность может быть значительно выше, чем пропускная способность каналов по времени. Несмотря на то, что известны способы реализации анализируемых методов противодействия утечке информации по скрытым каналам путем увеличения длин пакетов и генерации фиктивного трафика, отсутствуют рекомендации по выбору значений параметров данных методов, а также неизвестны оценки остаточной пропускной способности скрытых каналов в условиях противодействия. Поэтому настоящая работа, посвященная разработке и исследованию методов противодействия утечки информации по скрытым каналам, основанным на изменении длин передаваемых пакетов, является актуальной и представляет как научный, так и практический интерес.

Целью диссертационной работы является повышение защищенности информационных систем путем разработки метода ограничения пропускной способности скрытых каналов, основанных на изменении длин пакетов.

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

- анализ существующих способов построения скрытых каналов в сетях пакетной передачи данных и способов противодействия им;
- оценка максимальной пропускной способности скрытых каналов, основанных на изменении длин пакетов, при поточном и блочном шифровании трафика;
- разработка методики анализа и оценки пропускной способности скрытых каналов при применении методов противодействия;
- разработка и оценка количественных характеристик методов противодействия утечке информации по скрытым каналам, основанным на изменении длин пакетов, путем случайного увеличения длин пакетов, детерминированной и случайной генерации фиктивного трафика.

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

Научная новизна диссертационной работы заключается в следующем.

1. Предложена методика анализа и оценки пропускной способности скрытых каналов с использованием методов теории информации в условиях их ограничения, позволяющая, в

отличие от существующих подходов, исследовать зависимость характеристик скрытых каналов от параметров способа противодействия.

2. Разработаны методы противодействия утечке информации по скрытым каналам, основанным на изменении длин передаваемых пакетов, путем их случайного увеличения, детерминированной и случайной генерации фиктивного трафика, отличающиеся от известных тем, что они применимы в случае, когда допускается наличие в информационной системе скрытого канала с приемлемым значением пропускной способности.

3. Впервые получены оценки пропускной способности скрытых каналов, основанных на изменении длин передаваемых пакетов, в отсутствие противодействия и в условиях предотвращения утечки информации.

Теоретическую значимость представляют:

- методы противодействия утечке информации по скрытым каналам, основанным на изменении длин пакетов, путем случайного увеличения длин пакетов, подлежащих отправке, детерминированной и случайной генерации фиктивного трафика;
- методика анализа и оценки пропускной способности скрытых каналов при применении методов ограничения пропускной способности;
- формулы для расчета значений параметров предложенных методов противодействия, при которых пропускная способность скрытого канала не превышает заданного значения.

Практическую значимость представляют:

- методы ограничения пропускной способности скрытых каналов, основанных на изменении длин пакетов, путем случайного увеличения длин пакетов, подлежащих отправке, детерминированной и случайной генерации фиктивного трафика;
- оценка максимальной пропускной способности скрытого канала, основанного на изменении длин передаваемых пакетов, при отсутствии противодействия в условиях поточного и блочного шифрования трафика;
- методика анализа и оценки пропускной способности скрытого канала в условиях введения методов противодействия;
- программные средства для расчета значений параметров предложенных методов противодействия, позволяющих понизить остаточную пропускную способность скрытого канала до заданного значения.

Внедрение результатов исследований. Практическая значимость результатов диссертации подтверждена тремя актами о внедрении. Разработанные автором методы противодействия утечке информации по скрытым каналам внедрены в деятельность ЗАО «Голлард» по модернизации программного комплекса «Сито», предназначенного для

подавления функционирования скрытых логических каналов. Результаты диссертационной работы внедрены также в научно-исследовательские и опытно-конструкторские работы, выполняемые ООО «Защита информации». Теоретические результаты диссертации внедрены в образовательный процесс кафедры «Криптология и дискретная математика» НИЯУ МИФИ в рамках учебного курса «Криптографические протоколы и стандарты».

Публикации и апробация работы. Результаты диссертационной работы изложены в 15 опубликованных и приравненных к ним работах, в том числе в пяти научных статьях в изданиях, включенных в Перечень ведущих рецензируемых научных журналов, четырех научных статьях в журналах, индексируемых международной системой научного цитирования Scopus, из них одна в журнале, индексируемом международной системой научного цитирования Web of Science, также имеются два свидетельства о государственной регистрации программ для ЭВМ. Результаты работы докладывались на конференциях и семинарах различного уровня, в том числе на:

- 23-й и 24-й научно-технических конференциях «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2014, 2015 гг.);
- XXII Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы» (Москва, 2015 г.);
- научно-практическом семинаре в Центре специальных разработок Министерства обороны Российской Федерации (Москва, 2015 г.);
- 14-й Всероссийской конференции «Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» SIBECRYPT'15 (Новосибирск, 2015 г.);
- The International Conference on Open and Big Data OBD 2015 (Рим, Италия, 2015 г.);
- The 5th International Conference on IT Convergence and Security ICITCS 2015 (Куала Лумпур, Малайзия, 2015 г.);
- The 2nd Workshop on Emerging Aspects in Information Security EAIS'15 (Лодзь, Польша, 2015 г.);
- The 8th International Conference on Security of Information and Networks SIN 2015 (Сочи, 2015 г.).

Основные положения, выносимые на защиту:

- оценка максимальной пропускной способности скрытых каналов, основанных на изменении длин пакетов, при поточном и блочном шифровании трафика;
- методика анализа и оценки пропускной способности скрытых каналов при введении методов ограничения пропускной способности;

- методы противодействия утечке информации по скрытым каналам, основанным на изменении длин пакетов, путем случайного увеличения длин передаваемых пакетов, детерминированной и случайной генерации фиктивного трафика;
- выражения для расчета значений параметров предложенных методов противодействия утечке информации по скрытым каналам и рекомендации по их выбору.

Структура и объем работы. Диссертация состоит из введения, пяти разделов, заключения, списка литературы, включающего 148 наименований, и двух приложений. Диссертация изложена на 114 страницах с 27 рисунками и 12 таблицами, не включая приложения.

Содержание диссертации соответствует пунктам 5, 6, 13 паспорта специальности 05.13.19 — методы и системы защиты информации, информационная безопасность.

Общая характеристика работы

Во введении обосновывается актуальность диссертационной работы, определяется цель, формулируются задачи исследования, описываются структура и логика диссертации.

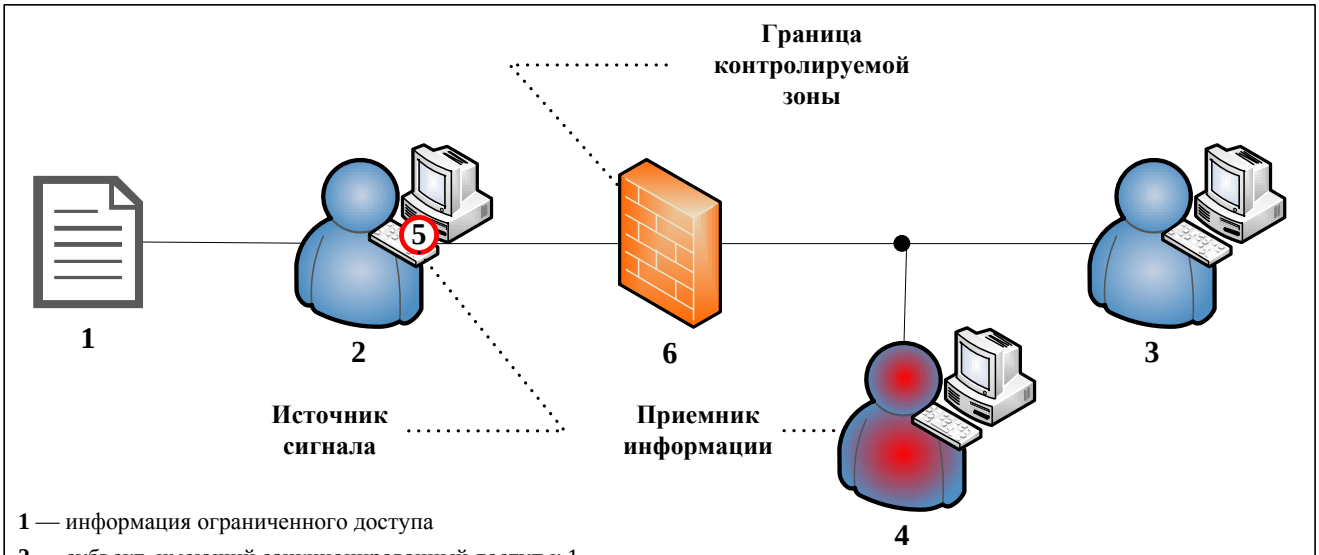
В первом разделе проанализированы существующие способы передачи информации по скрытым каналам в сетях пакетной передачи данных и методы противодействия им. В соответствии с ГОСТ Р 533113.1-2008, скрытый канал — непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности. Схема функционирования исследуемых скрытых каналов представлена на рисунке 1.

Согласно ГОСТ Р 53113.2-2009, защита информации, информационных технологий и автоматизированных систем от атак, реализуемых с использованием скрытых каналов, является циклическим процессом, включающим в себя следующие этапы:

- анализ рисков для активов организации, а именно выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов;
- идентификация скрытых каналов и оценка их опасности для активов организации;
- реализация защитных мер по противодействию скрытым каналам;
- организация контроля за противодействием скрытым каналам.

Так как доказано, что существуют необнаруживаемые скрытые каналы, а идентификацию способов построения потенциальных сетевых скрытых каналов, как правило, достаточно просто реализовать, то при оценке актуальности угрозы утечки информации по таким скрытым каналам, необходимо исследование следующих факторов:

- возможности встраивания агента нарушителя в автоматизированную систему;
- меры опасности, которую несет функционирование скрытых каналов.



1 — информация ограниченного доступа

2 — субъект, имеющий санкционированный доступ к 1

3 — субъект, находящийся вне объекта информатизации, с которым 2 осуществляет санкционированное информационное взаимодействие

4 — нарушитель безопасности, имеющий пассивный несанкционированный доступ к каналу связи за пределами объекта информатизации

5 — агент нарушителя безопасности, взаимодействующий с 1 от имени 2

6 — средство, контролирующее информационное взаимодействие между 2 и 3, которое осуществляет, в частности, шифрование трафика, выходящего за пределы объекта информатизации

Рисунок 1 — Схема функционирования скрытого канала

На основании выполнения указанных этапов принимается решение о необходимости противодействия каждому потенциальному скрытому каналу. В связи с тем, что основная часть аппаратного и программного обеспечения компьютерных систем произведена за рубежом, в него потенциально могут быть внесены закладки, троянские кони и другие объекты, при определенных условиях индуцирующие реализацию недекларированных возможностей. Причем, это касается как конечного оборудования, так и промежуточных узлов на пути следования трафика. Поэтому наличие агента нарушителя в автоматизированной системе, как правило, считается возможным при использовании импортного оборудования или программного обеспечения.

Таким образом, важная задача заключается в оценке ущерба, который может нанести функционирование потенциального скрытого канала при отсутствии специальных методов его подавления, данная оценка включает в себя, согласно ГОСТ Р 53113.1-2008, расчет пропускной способности скрытого канала, то есть предельного объема информации, утечка которого возможна по скрытому каналу за единицу времени. Далее, с учетом определения объема активов организации, утечка которых возможна по потенциальному скрытому каналу, и

интервала времени, в течение которого данные активы сохраняют ценность, становится возможным отнесение угрозы утечки информации по скрытому каналу к актуальным либо неактуальным угрозам.

Если оценка пропускной способности показала, что опасность, которую несет функционирование потенциальных скрытых каналов, такова, что угроза актуальна, то необходимо применять средства и методы по противодействию выбранным скрытым каналам. Согласно ГОСТ Р 53113.1-2008, к ним относят:

- снижение пропускной способности скрытого канала с использованием специальных технических средств и организационно-технических мер;
- обнаружение функционирующих скрытых каналов с использованием программно-технических средств;
- архитектурные решения построения защищенных автоматизированных систем.

Механизм определения актуальности угрозы утечки информации по скрытому каналу и возможные меры противодействия обобщенно представлены на рисунке 2.

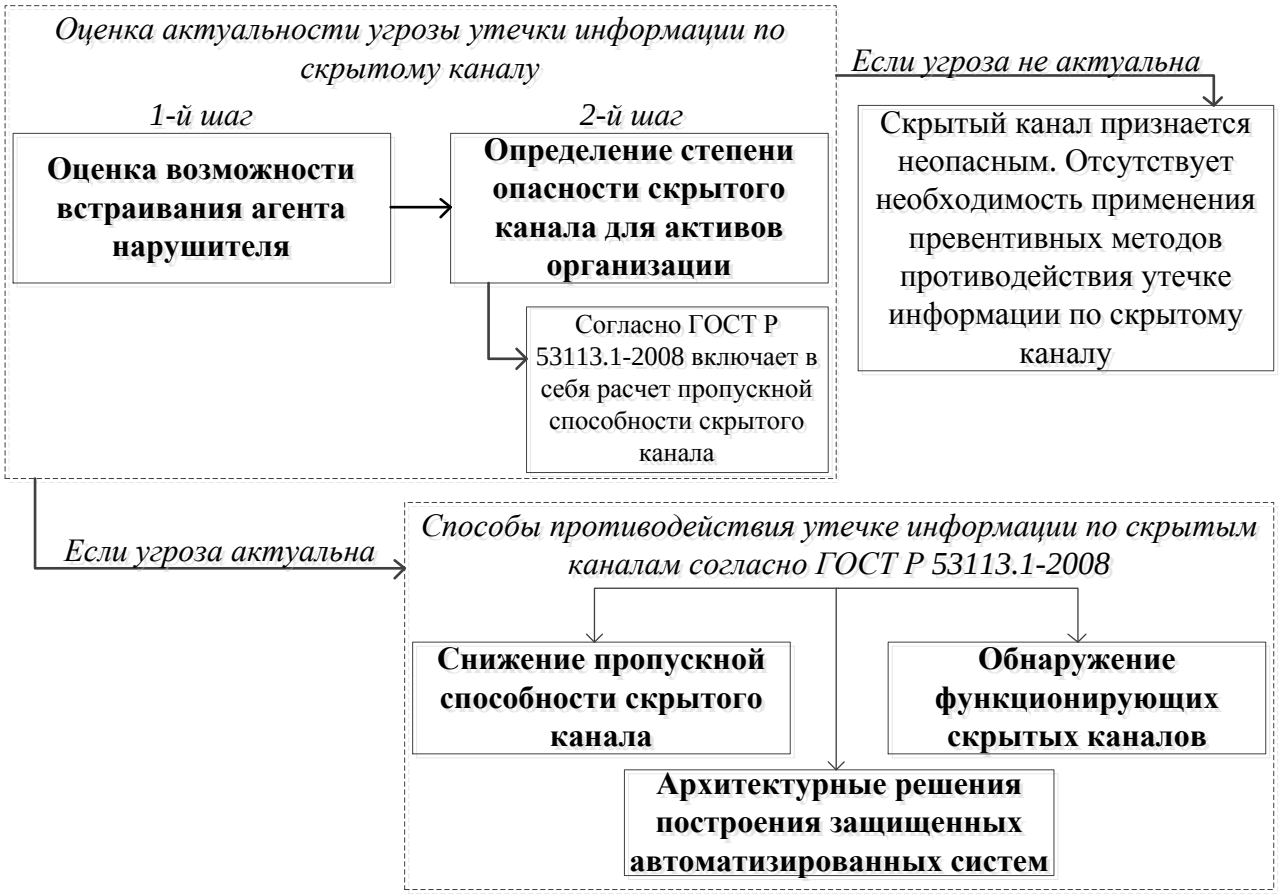


Рисунок 2 ─ Схема противодействия утечке информации по скрытым каналам

Зачастую не представляется возможным применять специальные архитектурные решения построения защищенных автоматизированных систем, в которых подавляется

возможность организации скрытых каналов. Например, при наличии каналов связи, выходящих за пределы объектов информатизации, на которых обрабатывается информация ограниченного доступа, необходимо использовать меры по понижению пропускной способности скрытых каналов.

Следовательно, принципиально важным является исследование методов, уменьшающих пропускную способность потенциального скрытого канала до такого значения, что утечка информации заданного объема за определенный интервал времени считается допустимой, что, как правило, приводит к понижению пропускной способности и самого канала связи и должно учитываться при выборе значений параметров таких методов противодействия.

Заметим, что несмотря на то, что проблема утечки информации по скрытым каналам поднимается в российских стандартах, а также в ряде исследований отечественных ученых, у государственных регуляторов в области информационной безопасности отсутствуют требования по защите информации, информационных технологий и автоматизированных систем от угроз, реализуемых с использованием скрытых каналов. Данное обстоятельство подтверждает важность настоящего исследования ввиду того, что необходимость применения и выбор конкретных методов противодействия скрытым каналам не регламентированы нормативными документами.

На рисунке 3 представлена систематизация скрытых каналов в сетях пакетной передачи данных.

Рисунок 3 — Систематизация скрытых каналов в сетях пакетной передачи данных

К скрытым каналам, возможность построения которых остается в условиях туннелирования и шифрования трафика, относят каналы по времени и каналы, основанные на

изменении длин передаваемых пакетов. Поскольку указанный тип скрытых каналов, как правило, имеет более высокую пропускную способность, настоящее исследование посвящено разработке и анализу методов противодействия утечке информации по таким каналам. Для их построения агент нарушителя должен обладать одной или несколькими следующими возможностями:

- изменять длины передаваемых пакетов;
- формировать фиктивные пакеты;
- переупорядочивать пакеты, подлежащие отправке.

Метод подавления исследуемых каналов заключается в приведении длин всех пакетов к фиксированному значению и их последующему зашифрованию, что в некоторых случаях приводит к недопустимому понижению эффективной пропускной способности и увеличению стоимости использования канала связи.

Второй раздел посвящен оценке максимальной пропускной способности скрытого канала, основанного на изменении длин пакетов, в условиях шифрования трафика, разработке методики анализа и оценки пропускной способности скрытых каналов в условиях противодействия.

При поточном шифровании пакетов предложено исследовать скрытый канал, построенный следующим образом. Пусть длины пакетов принимают значения на множестве $N_{l_{фикс}+L-1} \setminus N_{l_{фикс}-1}$, где N_x — множество натуральных чисел от 1 до x, $l_{фикс}$, $L \in N$, где $l_{фикс}$, как правило, определяет размер заголовка пакета, $L-1$ — максимальный размер информационного наполнения пакета. Тогда для передачи символа «i» отправитель посылает пакет длины $l_{фикс}+i$, $i \in N_{n-1} \bigcup \{0\}$, n — параметр скрытого канала. Если β — пропускная способность канала связи, то при равновероятном выборе передаваемых символов пропускная способность скрытого канала ν принимает наибольшее значение, равное

$$\nu \approx \frac{2\left(\log_2\left(2l_{фикс}-1\right)-\log_2\left(W\left(\frac{2l_{фикс}-1}{e}\right)\right)\right)}{2l_{фикс}+\frac{2l_{фикс}-1}{W\left(\frac{2l_{фикс}-1}{e}\right)}-1}\beta, \qquad (1)$$

где $W(y)$ — функция Ламберта, определяемая как корень уравнения $xe^x = y$.

При блочном шифровании пакетов предложено исследовать скрытый канал, организованный следующим образом. Для передачи символа «0» отправитель посылает пакет длины $l \in V_0$, где $V_0 = N_{\left\lceil \frac{l_{фикс}}{l_ш} \right\rceil l_ш} \setminus N_{l_{фикс}-1}$; для передачи символа «$i$» — пакет длины $l \in V_i$, $i \in N_{n-1}$,

где $V_i = N_{\left\lceil \frac{l_{фикс}}{l_ш} \right\rceil l_ш + il_ш} \setminus N_{\left\lceil \frac{l_{фикс}}{l_ш} \right\rceil l_ш + (i-1)l_ш}$, n — параметр скрытого канала, $l_ш$ — длина блока. Тогда при равновероятном выборе передаваемых символов пропускная способность скрытого канала ν принимает наибольшее значение, равное

$$\nu \approx \frac{2\left(\log_2\left(2\left\lceil \frac{l_{фикс}}{l_ш} \right\rceil - 1\right) - \log_2 W\left(e^{-1}\left(2\left\lceil \frac{l_{фикс}}{l_ш} \right\rceil - 1\right)\right)\right)}{l_ш\left(\left(2\left\lceil \frac{l_{фикс}}{l_ш} \right\rceil - 1\right)\left(1 + W^{-1}\left(e^{-1}\left(2\left\lceil \frac{l_{фикс}}{l_ш} \right\rceil - 1\right)\right)\right)\right)} \beta. \quad (2)$$

В таблице 1 приведены значения пропускных способностей скрытых каналов при использовании протоколов IPv4 и IPv6 в качестве протоколов сетевого уровня модели взаимосвязи открытых систем. Полученные результаты подтверждают актуальность исследования методов противодействия утечке информации по скрытым каналам, так как показывают, что при пропускной способности канала связи 1 Гбит/с может быть построен скрытый канал с пропускной способностью более 1 Мбит/с при блочном и 10 Мбит/с при поточном шифровании пакетов.

Таблица 1 — Отношение пропускной способности скрытого канала к пропускной способности канала связи при шифровании трафика

Протокол сетевого уровня	**Оцениваемая величина**	**Блочное шифрование пакетов**			**Поточное шифрование пакетов**
		Длина блока $l_ш$, бит			
		64	**128**	**256**	
IPv4 ($l_{фикс} = 34$ байта)	n	9	7	5	138
	$\frac{\nu}{\beta}10^3$	5,77	3,94	2,28	20,9
IPv6 ($l_{фикс} = 54$ байта)	n	10	8	5	201
	$\frac{\nu}{\beta}10^3$	4,52	3,30	2,28	14,4

При исследовании методов противодействия утечке информации по скрытым каналам сделаны следующие допущения:

- противнику известна вся необходимая для организации скрытого канала информация о характеристиках сети пакетной передачи данных, в которой планируется его построение: топология сети, применяемое сетевое оборудование, пропускная способность каналов связи и так далее;
- противнику известны значения всех статических параметров метода противодействия;
- противнику неизвестны значения всех динамических параметров метода противодействия;

- задано значение пропускной способности скрытого канала v_0, такое что функционирование скрытых каналов с пропускной способностью, не превосходящей v_0, является допустимым.

Пропускную способность v скрытого канала при введении способов противодействия предлагается оценивать методами теории информации как максимум по всевозможным значениям параметров скрытого канала отношения средней взаимной информации $I(X,Y)$ случайных величин, описывающих входные и выходные характеристики скрытого канала соответственно, к среднему времени τ передачи пакета.

Выбранный подход к оценке пропускной способности скрытых каналов методами теории информации, с одной стороны, позволяет находить пропускную способность скрытых каналов с шумом, который может быть вызван введением методов противодействия, с другой стороны, полученное выражение пропускной способности имеет размерность «бит/с», что важно для практических приложений. Заметим, таким образом находится максимальная пропускная способность скрытого канала: предполагается, что нарушитель выбирает параметры, при которых величина $\frac{I(X,Y)}{\tau}$ принимает наибольшее значение.

Этапы предложенной методики анализа и оценки пропускной способности скрытых каналов при введении методов противодействия схематично изображены на рисунке 4.

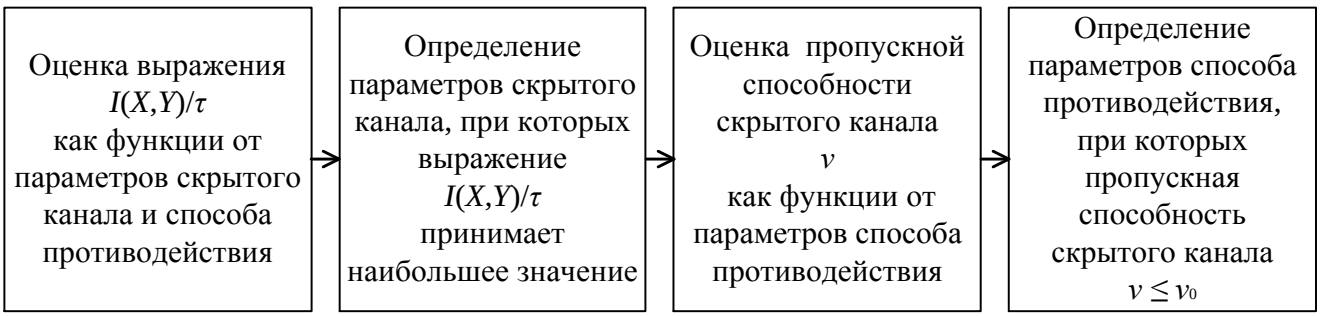


Рисунок 4 — Основные этапы предложенной методики

Разработанная методика применена для анализа и оценки пропускной способности исследуемых скрытых каналов при введении предложенных в последующих разделах методов противодействия.

Третий раздел посвящен разработке метода ограничения пропускной способности скрытых каналов для противодействия утечке информации ограниченного доступа путем увеличения длин пакетов: длина каждого пакета, подлежащего отправке, увеличивается на количество битов, определяемое значениями случайной величины, имеющей равномерное распределение на множестве $N_\alpha \bigcup \{0\}$, где α — параметр метода противодействия.

Равномерное распределение представляет наибольшую неопределенность в распознавании получателем переданного символа, а выбор множества $N_\alpha \bigcup \{0\}$ продиктован уменьшением дополнительной нагрузки на канал связи.

Первым исследован скрытый канал, имеющий наибольшую пропускную способность в условиях данного метода противодействия: для передачи символа «i» отправитель посылает пакет длины $l_{фикс} + i(\alpha+1)$, $i \in N_{n-1} \bigcup \{0\}$, n — параметр скрытого канала. При равновероятном выборе передаваемых символов пропускная способность скрытого канала ν принимает наибольшее значение, равное

$$\nu \approx \frac{2\left(\log_2\left(\frac{2l_{фикс}-1}{\alpha+1}\right)-\log_2\left(W\left(\frac{2l_{фикс}-1}{e(\alpha+1)}\right)\right)\right)}{2l_{фикс}+\frac{2l_{фикс}-1}{W\left(\frac{2l_{фикс}-1}{e(\alpha+1)}\right)}-1}\beta. \qquad (3)$$

Отметим, что длины передаваемых пакетов принимают лишь некоторые из возможных значений, что делает сложным построение канала при ограниченных возможностях агента нарушителя. Если необходимым условием для построения канала является равномерное распределение на множестве длин передаваемых пакетов, то канал может быть построен следующим образом: для передачи символа «i» отправитель посылает пакет длины $l \in W_i$, $i \in N_{n-1} \bigcup \{0\}$, где $W_i = N_{l_{фикс}+(i+1)b-1} \setminus N_{l_{фикс}+ib-1}$, n, b — параметры скрытого канала. Тогда пропускная способность скрытого канала определяется по формуле (3), если $l_{фикс}$ положить равным $l_{фикс} + \alpha/2$.

Однако при таком построении скрытого канала вероятность верного распознавания переданного символа равна $\frac{1}{\alpha+1}$. Пусть задан допустимый уровень ошибок при передаче данных по скрытому каналу $p_{ош} \le \frac{1}{2}$. Тогда пропускная способность скрытого канала принимает наибольшее значение, равное

$$\nu \approx \frac{2\left(\log_2\left(\frac{2p_{ош}\left(2l_{фикс}+\alpha-1\right)}{\alpha}\right)-\log_2\left(W\left(\frac{2^{1-H(\zeta)}p_{ош}\left(2l_{фикс}+\alpha-1\right)}{e\alpha}\right)\right)-H(\zeta)\right)}{2l_{фикс}+\alpha-1+\left(2l_{фикс}+\alpha-1\right)W^{-1}\left(\frac{2^{1-H(\zeta)}p_{ош}\left(2l_{фикс}+\alpha-1\right)}{e\alpha}\right)}\beta, \qquad (4)$$

где ζ — случайная величина, имеющая распределение Бернулли с вероятностью успеха $p_{ош}$.

Необходимо заметить, что пропускная способность рассмотренных выше скрытых каналов максимальна при данном методе противодействия и некоторых дополнительных ограничениях. Однако при случайном увеличении длин пакетов, подлежащих отправке, подавляется возможность построения класса скрытых каналов, в которых длины пакетов, соответствующие символам скрытно передаваемого сообщения, выбираются случайным образом из множества возможных длин пакетов.

В четвертом разделе разработан метод противодействия утечке информации по скрытым каналам путем генерации фиктивного трафика. Предложено два способа генерации фиктивных пакетов: детерминированным и случайным образом. При детерминированной генерации фиктивного трафика количество пакетов между фиктивными равно k, при случайной — определяется значениями случайной величины, имеющей равномерное распределение на множестве $N_{\tilde{k}}$. Таким образом, k и $\tilde{k}$ — параметры соответствующих методов противодействия.

После отправки фиктивного пакета происходит рассинхронизация отправителя и получателя. В качестве механизма восстановления синхронизма предложена отправка пакетов специального вида. Получатель фиксирует $T-1$ пакет после получения пакета специального вида, восстанавливает переданные символы и ожидает прибытия следующего пакета специального вида, T — параметр скрытого канала, определяющий частоту синхронизации отправителя и получателя.

Так как длины передаваемых пакетов не изменяются, а отправка фиктивных пакетов приводит к нарушению синхронизма, то исследуется пропускная способность в бит/пакет бинарного скрытого канала, построенного следующим образом. Пусть даны равномощные непересекающиеся множества L_0, L_1, такие что $L_0 \bigcup L_1 = N_{l_{фикс}+L-1} \setminus N_{l_{фикс}-1}$. Тогда для отправки «0» отправитель посылает пакет длины $l \in L_0$, для отправки «1» — длины $l \in L_1$. Рисунки 5, 6 иллюстрируют передачу данных по бинарному скрытому каналу при детерминированной ($k=5,\ T=3$) и случайной ($\tilde{k}=5,\ T=3$) генерации фиктивного трафика соответственно, отправлено сообщение: 1000011011, получено сообщение: 1100001011.

Для повышения стойкости скрытого канала к обнаружению могут быть приняты следующие меры:

- периодическое изменение отправителем и получателем множеств L_0, L_1;
- выбор в качестве L_0, L_1 мультимножеств таким образом, чтобы при случайном равновероятном выборе длин пакетов из мультимножеств L_0, L_1 распределение на множестве

длин передаваемых пакетов совпадало с эмпирически полученным распределением длин пакетов, характерным для отсутствия скрытого канала.

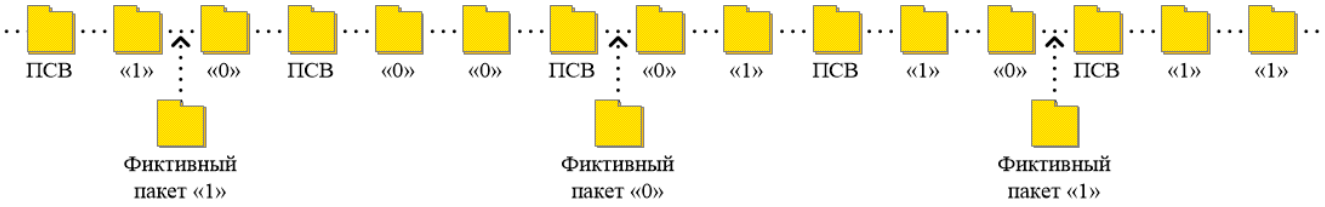


Рисунок 5 — Передача данных по бинарному скрытому каналу при детерминированной генерации фиктивного трафика

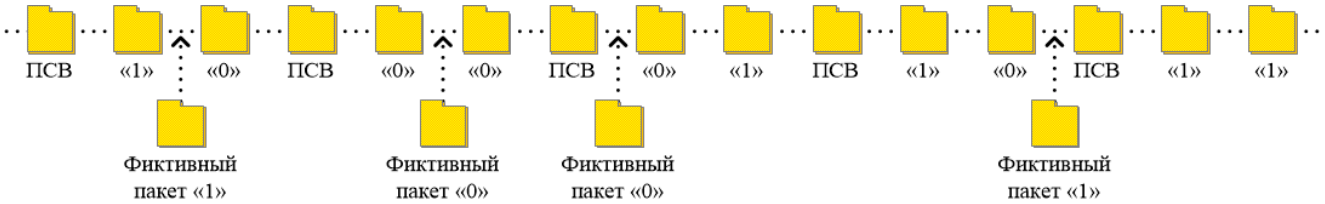


Рисунок 6 — Передача данных по бинарному скрытому каналу при случайной генерации фиктивного трафика

При таком способе построения скрытого канала средняя длина передаваемых пакетов не зависит от значения параметра скрытого канала T, а взаимную информацию $I(X,Y)$ предлагается оценить как $\frac{T-1}{T} I^*(X,Y)$, где $I^*(X,Y)$ — взаимная информация случайных величин, описывающих входные и выходные характеристики скрытого канала при исключении пакетов специального вида.

Значения условных вероятностей $p(s|r)$, $s,r \in \{0,1\}$ распознавания получателем символа «s» при отправке символа «r» зависят от числа пакетов, переданных по скрытому каналу от момента синхронизации до прихода фиктивного пакета, поэтому пропускную способность скрытого канала ν при детерминированной генерации фиктивного трафика предлагается оценить как

$$\nu = \max_T \left\{ \frac{T-1}{kT} \left(k - (T-1) + \sum_{i=0}^{T-2} \left(1 - H_i(Y \mid X)\right) \right) \right\}, \quad (5)$$

где $H_i(Y \mid X)$ — условная энтропия случайной величины Y относительно случайной величины X, когда количество пакетов, переданных между пакетом специального вида и фиктивным пакетом, равно i.

Пропускная способность ν при случайной генерации фиктивного трафика равна

$$\nu = \max_{T} \left\{ \frac{(T-1)\left(\binom{\tilde{k}-T+2}{2} + \sum_{i=0}^{T-2} \left(\binom{\tilde{k}-i}{2} \left(1 - H_i(Y \mid X)\right) \right) \right)}{T \binom{\tilde{k}+1}{2}} \right\}. \quad (6)$$

На рисунках 7, 8 представлены графики зависимости взаимной информации $I(X,Y)$ от параметров методов противодействия k и $\tilde{k}$ при детерминированной ($T \in \{2,3,4,5\}$) и случайной ($T \in \{2,3,4\}$) генерациях фиктивного трафика соответственно. При заданных значениях $k, \tilde{k}$ выбор параметра скрытого канала T однозначен, с увеличением значений параметров $k, \tilde{k}$ значение параметра T либо не изменяется, либо увеличивается на единицу.

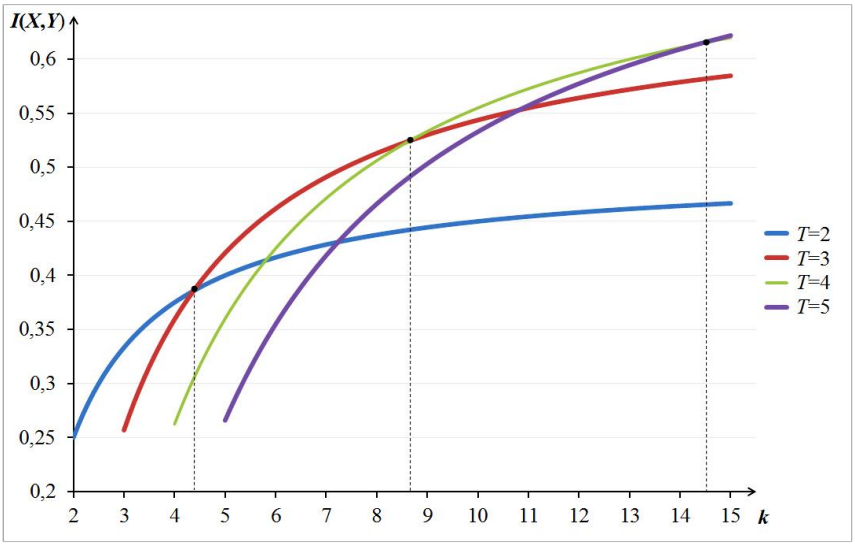


Рисунок 7 — Взаимная информация случайных величин X, Y при детерминированной генерации фиктивного трафика

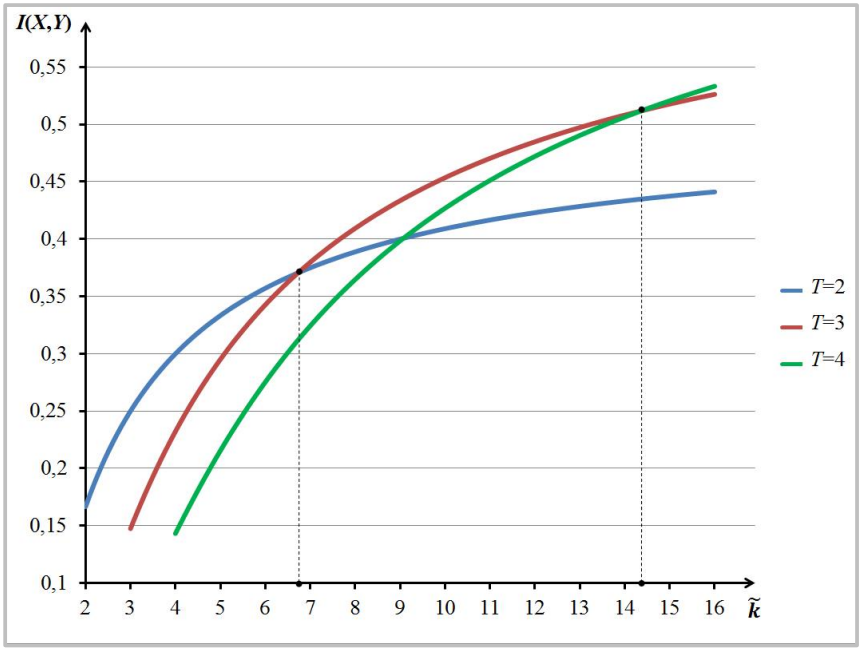


Рисунок 8 — Взаимная информация случайных величин X, Y при случайной генерации фиктивного трафика

Из рисунка 7 следует, что при $k \in \{2,3,4\}$ параметр T следует выбирать равным двум, при $k \in \{5,6,7,8\}$ — трем, при $k \in \{9,...,14\}$ — четырем. Из рисунка 8 следует, что при $\tilde{k} \in \{2,...,6\}$ параметр T следует выбирать равным двум, при $\tilde{k} \in \{7,...,14\}$ — трем.

Таким образом, определены наилучшие, с точки зрения величины остаточной пропускной способности скрытого канала, значения его параметров, отвечающих за частоту синхронизации, при детерминированной и случайной генерации фиктивного трафика. Также получено выражение пропускной способности скрытого канала при введении противодействия.

Пятый раздел посвящен разработке рекомендаций по практической применимости полученных результатов.

Особенностью предложенной обобщенной методики анализа и оценки пропускной способности скрытых каналов в условиях противодействия является исследование скрытого канала с наибольшим значением остаточной пропускной способности при некоторых ограничениях. Таким образом, пропускная способность скрытого канала может быть значительно ниже в условиях противодействия при, например, ограничениях на возможности агента нарушителя, однако важна оценка именно максимальной остаточной пропускной способности скрытого канала при отсутствии достоверных предположений о возможностях агента. Заметим, методика может быть применена к анализу пропускной способности не только скрытых каналов в условиях предложенных методов противодействия, но и иных классов скрытых каналов и способов противодействия.

Ввиду того, что в ряде случаев определять значения параметров разработанных методов противодействия для ограничения пропускной способности скрытого канала необходимо расчетным способом с использованием сложных аналитических зависимостей, реализованы программные средства по расчету необходимых значений параметров предложенных методов противодействия, позволяющих предотвратить утечку информации ограниченного доступа, понизив дополнительную нагрузку на канал связи. Получены два свидетельства о государственной регистрации программ для ЭВМ, касающихся оценки параметров методов противодействия путем случайного увеличения длин пакетов и генерации фиктивного трафика.

В таблице 2 представлена зависимость между значениями параметров скрытого канала b, n, пропускной способности скрытого канала v и параметра метода противодействия α. Результаты приведены для трех типов скрытых каналов, исследованных в третьем разделе:

- канала, имеющего наибольшую пропускную способность при введении противодействия (K_1);
- канала, имеющего наибольшую пропускную способность при введении противодействия и условии, что длины передаваемых пакетов принимают равномерно распределенные значения (K_2);
- канала, имеющего наибольшую пропускную способность при введении противодействии, и условиях, что длины передаваемых пакетов принимают равномерно распределенные значения и уровень ошибок не превышает заданного значения (K_3).

Таблица 2 — Пропускная способность скрытого канала при увеличении длин пакетов

Протокол сетевого уровня	α	K_1		K_2		K_3					
						$p_{ош}$=0,25			$p_{ош}$=0,1		
		n	$\frac{v}{\beta}\times10^3$	n	$\frac{v}{\beta}\times10^3$	b	n	$\frac{v}{\beta}\times10^3$	b	n	$\frac{v}{\beta}\times10^3$
IPv4 ($l_{фикс}$=34 байта)	10	23	11,40	257	11,20	20	20	7,37	50	11	5,42
	50	9	6,33	479	6,03	100	9	3,16	250	6	2,02
	100	6	4,50	694	4,16	200	7	1,95	500	5	1,18
	200	5	3,00	1084	2,66	400	6	1,13	1000	4	0,65
	500	4	1,57	2192	1,32	1000	6	0,50	2500	4	0,28
IPv6 ($l_{фикс}$=54 байта)	10	32	8,23	353	8,16	20	26	5,58	50	14	4,24
	50	12	4,86	614	4,70	100	11	2,63	250	7	1,76
	100	8	3,60	851	3,39	200	8	1,71	500	5	1,07
	200	6	2,50	1266	2,28	400	7	1,03	1000	5	0,61
	500	4	1,40	2402	1,20	1000	6	0,48	2500	4	0,27

На рисунках 9, 10 проиллюстрировано сравнение количественных характеристик бинарного скрытого канала при детерминированной (П1) и случайной (П2) генерации фиктивного трафика. С целью корректного сравнения методов противодействия при одинаковой нагрузке на канал связи параметр $\tilde{k} = 2k - 1$.

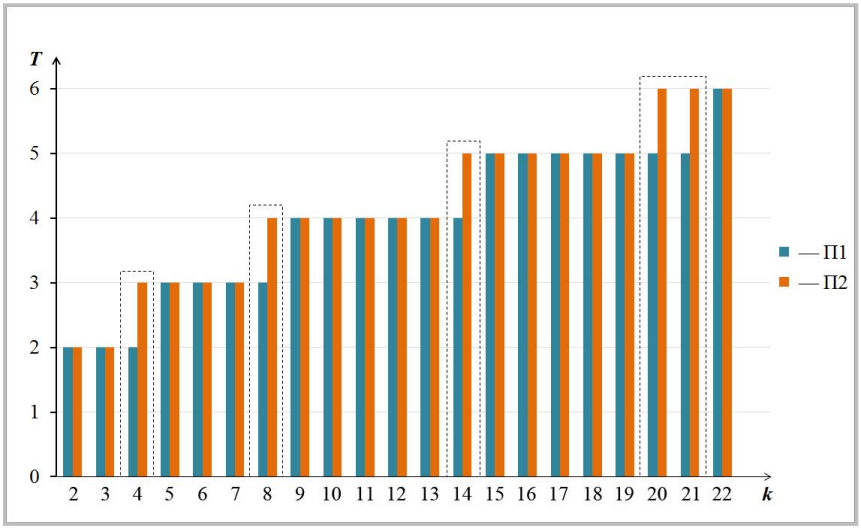


Рисунок 9 — Частота синхронизации в скрытом канале

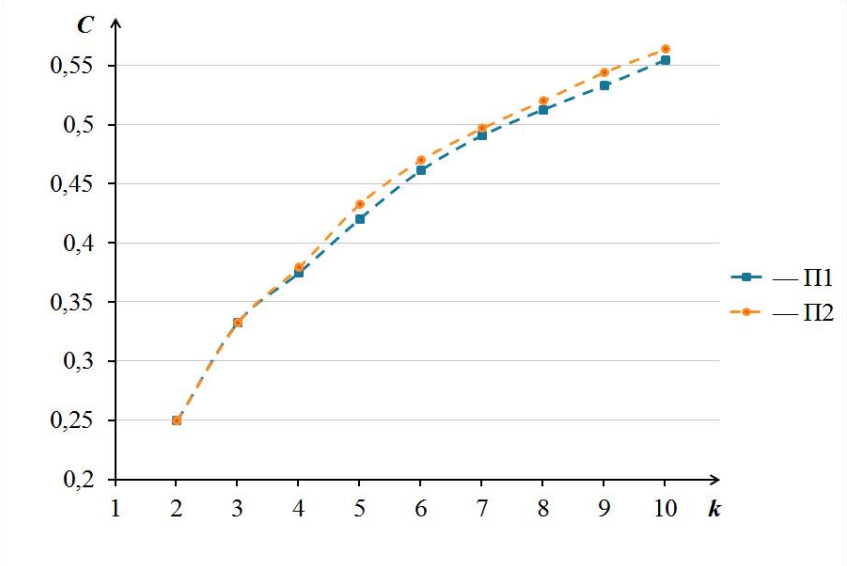


Рисунок 10 — Пропускная способность скрытого канала

При некоторых значениях k, как следует из рисунка 9, синхронизацию в случае П2 необходимо проводить реже, чем в случае П1. Как видно из рисунка 10, при k>3 пропускная способность скрытого канала выше при П2, чем при П1.

При этом метод детерминированной генерации фиктивного трафика подвержен атаке по отслеживанию фиктивных пакетов: противнику необходимо единожды обнаружить фиктивный пакет, после чего вся дальнейшая передача данных по скрытому каналу будет без ошибок и необходимости поддержки синхронизма. Данные выводы позволяют сделать следующие рекомендации по выбору способа генерации фиктивного трафика.

Если возможна атака по отслеживанию фиктивных пакетов, необходимо применять случайную генерацию фиктивного трафика, в противном случае необходимо генерировать фиктивные пакеты детерминированным образом.

На рисунке 11 представлена обобщенная блок-схема, иллюстрирующая применение предложенных методов противодействия утечке информации по скрытым каналам в системах защиты информации, на которой красным цветом выделены этапы, выполняемые автоматически при помощи разработанных программных средств, а также данные, получаемые в результате их работы.

В приведенной блок-схеме под логическим устройством понимается блок управления, осуществляющий выбор необходимых методов противодействия утечке информации по скрытым каналам и их количественных характеристик, а также определяющий необходимые действия, применительно к каждому обрабатываемому пакету. Результаты диссертации позволяют определить логику работы данного блока управления, предотвратив утечку информации ограниченного доступа по скрытым каналам, основанным на изменении длин пакетов, и уменьшив дополнительную нагрузку на канал связи.

Практическая значимость результатов диссертации подтверждена тремя актами о внедрении. Разработанные автором методы противодействия утечке информации по скрытым каналам внедрены в деятельность ЗАО «Голлард» по модернизации программного комплекса «Сито», предназначенного для подавления функционирования скрытых логических каналов. Результаты диссертационной работы внедрены в научно-исследовательские и опытно-конструкторские работы, выполняемые ООО «Защита информации», применены в образовательном процессе кафедры «Криптология и дискретная математика» НИЯУ МИФИ в рамках учебного курса «Криптографические протоколы и стандарты». Имеются три акта о внедрении результатов диссертационной работы.

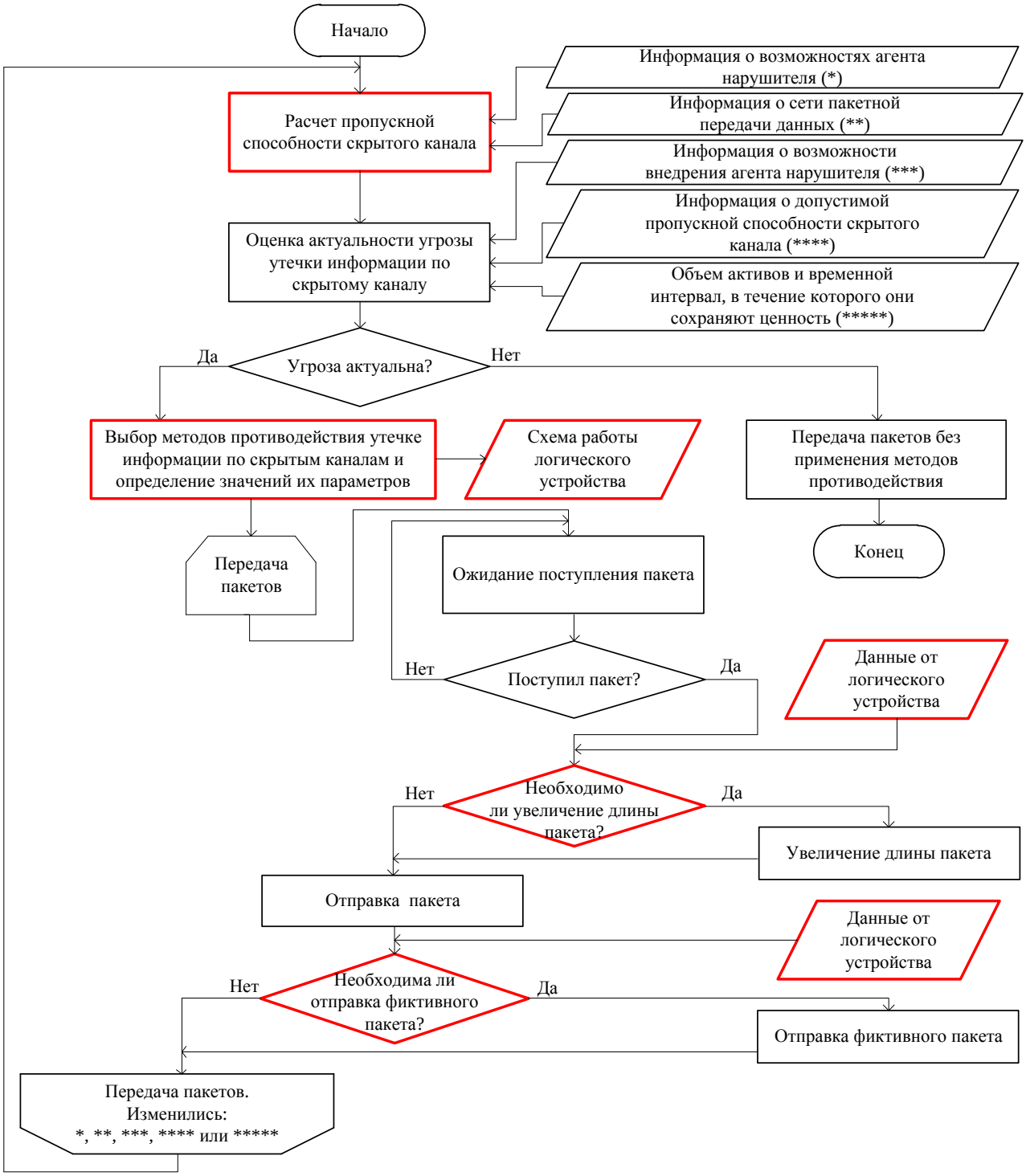


Рисунок 11 — Блок-схема применения методов противодействия утечке информации по скрытым каналам

Основные результаты работы

1. Проведенный анализ существующих способов построения скрытых каналов в сетях пакетной передачи данных и способов противодействия утечке информации по данным каналам выявил актуальную задачу разработки и оценки количественных характеристик превентивных методов противодействия скрытым каналам, основанным на изменении длин передаваемых пакетов.

2. Оценка максимальной пропускной способности скрытых каналов, основанных на изменении длин пакетов, при поточном и блочном шифровании трафика подтвердила необходимость исследования и применения превентивных методов противодействия, так как показано, что при их отсутствии пропускная способность скрытого канала может превышать 1% пропускной способности канала связи.

3. Разработанная методика анализа и оценки пропускной способности скрытых каналов при применении методов противодействия, включающая в себя построение наилучшего, с точки зрения величины остаточной пропускной способности, скрытого канала и оценку значений параметров способа противодействия, при которых пропускная способность скрытого канала не превышает заданного значения, позволила оценить количественные характеристики предложенных методов противодействия.

4. Разработанные методы противодействия утечке информации по скрытым каналам, основанным на изменении длин пакетов, путем их случайного увеличения перед отправкой, детерминированной и случайной генерации фиктивного трафика, позволили повысить защищенность информационных систем, для функционирования которых необходимо обеспечение функционирования каналов связи, выходящих за пределы объектов информатизации, на которых обрабатывается информация ограниченного доступа.

5. Оценена остаточная пропускная способность многосимвольного и бинарного скрытых каналов в условиях случайного увеличения длин пакетов и генерации фиктивного трафика соответственно. Полученные результаты позволили выбирать необходимые методы противодействия и их количественные характеристики для предотвращения утечки информации ограниченного доступа.

6. Разработанные рекомендации по выбору значений параметров методов противодействия утечке информации по скрытым каналам путем случайного увеличения длин передаваемых пакетов, детерминированной и случайной генерации фиктивного трафика позволили ограничить утечку информации по таким каналам, уменьшив дополнительную нагрузку на канал связи.

7. Созданы программные средства для расчета значений параметров разработанных методов противодействия скрытым каналам, позволившие автоматизировать выбор необходимых значений параметров данных методов для предотвращения утечки информации ограниченного доступа. Получены два свидетельства о государственной регистрации программ для ЭВМ.

8. Основные результаты диссертационной работы, касающиеся разработки и оценки количественных характеристик методов противодействия утечке информации по скрытым каналам, используются в научно-исследовательских и опытно-конструкторских работах, проводимых ЗАО «Голлард», ООО «Защита информации». Аналитические результаты применены в образовательном процессе кафедры «Криптология и дискретная математика» НИЯУ МИФИ в рамках учебного курса «Криптографические протоколы и стандарты». Имеются три акта о внедрении результатов диссертационной работы.

Публикации по теме диссертации

1. Архангельская, А.В. О подходе к противодействию утечке информации по скрытым каналам / А.В. Архангельская, **К.Г. Когос** // Безопасность информационных технологий. — 2013. — №4. — С. 10–20 (Перечень ВАК).

2. Архангельская, А.В. О пропускной способности скрытых каналов, основанных на модуляции длин передаваемых пакетов / А.В. Архангельская, **К.Г. Когос** // Сборник материалов 23-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»: сб. науч. тр. / Санкт-Петербургский политехнический университет Петра Великого. — СПб., 2014. — С. 40–42.

3. Епишкина, А.В. Исследование методов организации и противодействия скрытым каналам в IP-сетях / А.В. Епишкина, **К.Г. Когос** // Проблемы информационной безопасности. Компьютерные системы. — 2014. — №4. — С. 36–42 (Перечень ВАК).

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 (Перечень ВАК).

5. **Когос, К.Г.** Обнаружение скрытых каналов по времени в IP-сетях / К.Г. Когос, М.А. Финошин // Безопасность информационных технологий. — 2015. — №1. — С. 95–97 (Перечень ВАК).

6. Epishkina, A.V. The capacity of the packet length covert channel / A.V. Epishkina, **K.G. Kogos** // Прикладная дискретная математика. Приложение. — 2015. — №8. — С. 96–99 (Перечень ВАК).

7. Епишкина, А.В. Максимальная пропускная способность скрытых каналов, основанных на изменении длин передаваемых пакетов / А.В. Епишкина, **К.Г. Когос** // Сборник материалов 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»: сб. науч. тр. / Санкт-Петербургский политехнический университет Петра Великого. — СПб., 2015. — С. 39–41.

8. Белозубова, А.И. Об одном способе ограничения пропускной способности скрытых каналов по времени в IP-сетях / А.И. Белозубова, **К.Г. Когос** // Сборник материалов 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»: сб. науч. тр. / Санкт-Петербургский политехнический университет Петра Великого. — СПб., 2015. — С. 35–37.

9. Когос, К.Г. Генерация фиктивного трафика как метод повышения стойкости скрытых каналов по времени в IP-сетях / **К.Г. Когос**, М.А. Финошин // Сборник материалов 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»: сб. науч. тр. / Санкт-Петербургский политехнический университет Петра Великого. — СПб., 2015. — С. 46–48.

10. Epishkina, A. A random traffic padding to limit packet size covert channels / A. Epishkina, **K. Kogos** // Proceedings of the 2015 Federated Conference on Computer Science and Information Systems. — 2015. — С. 1119–1123 (Scopus, Web of Science).

11. Epishkina, A. Covert channels parameters evaluation using the information theory statements / A. Epishkina, **K. Kogos** // Proceedings of the 5th International Conference on IT convergence and security. — 2015. — С. 395–399 (Scopus).

12. Epishkina, A. A traffic padding to limit packet size covert channels / A. Epishkina, **K. Kogos** // Proceedings of the International Conference on open and big data. — 2015. — С. 519–525 (Scopus).

13. Epishkina, A. Protection from binary and multi-symbol packet length covert channels / A. Epishkina**, K. Kogos** // Proceedings of the 8th International Conference on security of information and networks. — 2015. — С. 196–202 (Scopus).

14. Свидетельство о государственной регистрации программы для ЭВМ. Заявка 2015617148. Российская Федерация. Оценка объема информации, утечка которой возможна по многосимвольному скрытому каналу при случайном увеличении длин передаваемых пакетов [Текст] / Автор и правообладатель **Когос К.Г.** — №.2015619945; заявл. 24.07.15; опубл. 17.09.15 (приравнивается к публикации в журнале из Перечня ВАК).

15. Свидетельство о государственной регистрации программы для ЭВМ. Заявка 2015617168. Российская Федерация. Оценка объема информации, утечка которой возможна по бинарному скрытому каналу при генерации фиктивного трафика [Текст] / Автор и правообладатель **Когос К.Г.** — №.2015619957; заявл. 24.07.15; опубл. 17.09.15 (приравнивается к публикации в журнале из Перечня ВАК).

Личный вклад автора. Все основные результаты работы получены автором единолично. В работах, опубликованных в соавторстве, автору принадлежат: анализ методов идентификации и ограничения пропускной способности скрытых каналов [1]; метод противодействия утечке информации по скрытым каналам путем случайного увеличения длин передаваемых пакетов [2]; методика анализа и оценки пропускной способности скрытых каналов в условиях противодействия [3]; взаимосвязь между способами подавления, ограничения пропускной способности и механизмами построения скрытых каналов в IP-сетях [4]; сравнительный анализ методов обнаружения скрытых каналов по времени в IP-сетях [5]; метод противодействия утечке информации по скрытым каналам путем детерминированной генерации фиктивного трафика [6]; оценка максимальной пропускной способности скрытого канала при отсутствии противодействия [7]; метод противодействия утечке информации по скрытым каналам по времени в IP-сетях путем введения случайных задержек [8]; метод генерации фиктивного трафика для повышения стойкости скрытых каналов по времени [9]; метод противодействия утечке информации по скрытым каналам путем случайной генерации фиктивного трафика [10]; формулы для расчета и рекомендации по выбору значения параметра метода противодействия утечке информации по скрытым каналам путем случайной генерации фиктивного трафика [11]; формулы для расчета и рекомендации по выбору значения параметра метода противодействия утечке информации по скрытым каналам путем детерминированной генерации фиктивного трафика [12]; оценка остаточных пропускных способности многосимвольного и бинарного скрытых каналов в условиях случайного увеличения длин пакетов и генерации фиктивного трафика соответственно [13].