ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53113.2— 2009

Информационная технология

ЗАЩИТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РЕАЛИЗУЕМЫХ С ИСПОЛЬЗОВАНИЕМ СКРЫТЫХ КАНАЛОВ

Часть 2

Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов

Издание официальное

Москва
Стандартинформ
2010

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «Криптоком»

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 841-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ПЕРЕИЗДАНИЕ. Октябрь 2018 г.

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Обозначения и сокращения 2
5 Механизм функционирования скрытого канала 2
6 Правила формирования модели угроз безопасности с учетом существования скрытых каналов 4
7 Порядок организации защиты информации, информационных технологий и автоматизированных систем от атак, реализуемых с использованием скрытых каналов 4
8 Анализ рисков 5
9 Рекомендации по порядку выявления скрытых каналов 5
10 Рекомендации по методам реализации защитных мероприятий по противодействию скрытым каналам 6
11 Рекомендации по организации контроля за противодействием скрытым каналам 7
Библиография 8

Введение

В настоящем стандарте установлены рекомендации по организации защиты информации (ЗИ), информационных технологий и автоматизированных систем от атак с использованием скрытых каналов (СК).

СК используются для систематического взаимодействия вредоносных программ (компьютерных вирусов) с нарушителем безопасности при организации атаки на автоматизированную систему (АС), которая не обнаруживается средствами контроля и защиты.

Опасность СК основана на предположении постоянного доступа нарушителя безопасности к информационным ресурсам организации и воздействии через эти каналы на информационную систему для нанесения максимального ущерба организации.

Настоящий стандарт разработан с учетом требований ГОСТ Р ИСО/МЭК 15408-3 и ГОСТ Р ИСО/МЭК 27002, в которых предусматривается осуществление мероприятий по противодействию угрозам безопасности организации, реализуемым с использованием СК. В данных стандартах мероприятия по противодействию угрозам ИБ с использованием СК представлены в общем виде, а их детализация представлена в настоящем стандарте.

Кроме этого, существует ряд технологий по обеспечению информационной безопасности и нормативных документов (НД) ФОИВ (ФСТЭК России, в которых рассматриваются отдельные аспекты этой проблемы).

Так ГОСТ Р 51188 устанавливает общие правила организации и проведения испытаний программных средств и их компонентов с целью обнаружения и устранения в них компьютерных вирусов. В данном стандарте также регламентирован порядок проверки компьютера на наличие компьютерных вирусов и их устранение. Такая проверка может выявить агента нарушителя безопасности, используемого им для организации скрытого канала, но только в том случае, если агент не является неотъемлемой частью операционной системы или аппаратной платформы проверяемого компьютера. Поскольку антивирусные проверки не способны выявить всех потенциальных агентов, возникает необходимость в противодействии СК, которые такие «невидимые» агенты могут использовать для взаимодействия с нарушителем безопасности.

НТД ФСТЭК России [1] установлена классификация программного обеспечения (как отечественного, так и зарубежного производства) для средств ЗИ, в том числе встроенных в общесистемное и прикладное программное обеспечение (ПО), по уровню контроля отсутствия в нем недекларированных возможностей. В процессе такой проверки недекларированные возможности, признанные неопасными, могут оказаться более опасными в процессе эксплуатации ПО в результате взаимодействия через СК с внешним нарушителем безопасности.

В НТД ФСТЭК России [2] установлена классификация межсетевых экранов по уровню защищенности от несанкционированного доступа к информации путем выбора соответствующих показателей защищенности. Данные показатели содержат требования, предъявляемые к средствам ЗИ, реализованным в виде межсетевых экранов, обеспечивающие безопасное взаимодействие сетей ЭВМ АС посредством управления межсетевыми потоками информации. Межсетевой экран реализует функции ограничения сетевого взаимодействия, а также требования принятой политики информационной безопасности организации. Взаимодействие с использованием СК осуществляется в рамках ограничений, вводимых межсетевым экраном, поэтому СК могут функционировать даже при использовании правильно настроенного межсетевого экрана, имеющего достаточный уровень защищенности.

Настоящий стандарт также устанавливает типовой порядок организации противодействия СК, который может уточняться с учетом условий и особенностей применения информационных технологий в АС. Кроме того, могут разрабатываться и применяться дополнительные меры защиты.

Организация защиты ИТ и АС от атак с использованием СК включает в себя процедуры их выявления и подавления. Набор применяемых методов выявления и/или подавления СК должен определяться исходя из модели угроз безопасности организации.

Мероприятия по защите от атак с использованием СК должны быть интегрированы в систему информационной безопасности организации.

Настоящий стандарт применяется совместно с ГОСТ Р 53113.1.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

ЗАЩИТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РЕАЛИЗУЕМЫХ С ИСПОЛЬЗОВАНИЕМ СКРЫТЫХ КАНАЛОВ

Часть 2

Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов

Information technologies. Protection of information technology and automated systems against security threats posed by use of covert channels. Part 2. Recommendations on protecting information, information technologies and automated systems against covert channel attacks

Дата введения — 2009—12—01

1 Область применения

Настоящий стандарт предназначен для заказчиков, разработчиков и пользователей информационных технологий в процессе формирования требований по защите информации на стадиях разработки, приобретения и применения продуктов, информационных технологий и автоматизированных систем в соответствии с требованиями нормативных правовых документов ФОИВ (ФСТЭК России) [1], [2] или требованиями, устанавливаемыми обладателем информации.

Настоящий стандарт предназначен для органов сертификации, а также испытательных лабораторий при проведении подтверждения соответствия информационных технологий и автоматизированных систем требованиям к обеспечению безопасности информации, циркулирующей в этих системах, аналитических подразделений и служб безопасности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 7498-1—99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель

ГОСТ Р ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности

ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента

ГОСТ Р 51188 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

ГОСТ Р 53113.1—2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесяч-

Издание официальное

ного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 53113.1.

4 Обозначения и сокращения

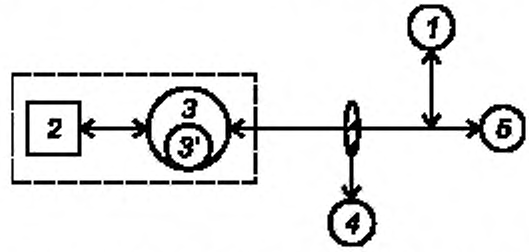
В настоящем стандарте использованы следующие обозначения и сокращения:
АБС — автоматизированная банковская система;
ВОС — взаимосвязь открытых систем;
ИБ — информационная безопасность;
ИТ — информационная технология;
НСД — несанкционированный доступ;
СУБД — система управления базами данных;
HTTP — (hypertext transfer protocol) протокол передачи гипертекста;
IP — (Internet protocol) протокол интернета;
VPN — (virtual private network) — виртуальная частная сеть.

5 Механизм функционирования скрытого канала

5.1 СК используются для систематического взаимодействия вредоносных программ (компьютерных вирусов) с нарушителем безопасности при организации атаки на АС, которая не обнаруживается средствами контроля и защиты.

Опасность СК основана на предположении постоянного доступа нарушителя безопасности к информационным ресурсам организации и воздействии через эти каналы на информационную систему для нанесения максимального ущерба организации.

5.2 Общая схема механизма функционирования СК в АС представлена на рисунке 1.



1 — нарушитель безопасности (злоумышленник), целью которого является НСД к информации ограниченного доступа либо несанкционированное влияние на АС, *2* — информация ограниченного доступа либо критически важная функция; *3* — субъект, имеющий санкционированный доступ к *2* и *5*; *3'* — агент нарушителя безопасности, находящийся в замкнутом контуре с *2* и взаимодействующий с *2* от имени субъекта *3*; *4* — инспектор (программное, программно-аппаратное, аппаратное средство или лицо), контролирующий(ее) информационное взаимодействие *3*, пересекающее замкнутый контур, отделяющий объект информатизации от внешней среды; *5* — субъект, находящийся вне замкнутого контура, с которым *3* осуществляет санкционированное информационное взаимодействие

Рисунок 1 — Общая схема механизма функционирования СК в АС

5.3 Взаимодействие между субъектами *3* и *5* является санкционированным и необходимым для правильной работы АС. Задача агента *3'* заключается в том, чтобы обеспечить регулярное интерактивное взаимодействие между агентом и злоумышленником. Агент должен передать информацию

ограниченного доступа *2* злоумышленнику *1* либо по команде злоумышленника *1* оказать воздействие на критически важную функцию *2*. Скрытность канала взаимодействия между злоумышленником *1* и агентом *3'* заключается в том, что субъект *3*, инспектор *4* и субъект *5* не обнаруживают факт передачи информации или команды.

СК позволяют злоумышленнику регулярно интерактивно осуществлять взаимодействие со своим агентом, внедренным в АС.

5.4 В АС взаимодействие между агентом *3* и субъектом *5* может быть как сетевым, так и происходить внутри одной АС (см. 5.6).

5.5 Классификация СК по различным признакам приведена в ГОСТ Р 53113.1.

5.6 Примеры СК, поясняющие механизм их функционирования представлены ниже.

Пример 1 — Нарушитель безопасности (злоумышленник), сотрудничающий с конкурирующей организацией, в процессе внедрения (ввода в эксплуатацию) установил в АБС программного агента. Взаимодействуя с АБС в качестве клиента этого банка, злоумышленник передает программному агенту команды, закодированные в последовательностях его действий, каждое из которых не вызывает подозрений (проверка состояния счета, управление счетом, временные интервалы между операциями и др.). В ответ на команды, полученные по СК, агент по тем же СК возвращает злоумышленнику интересующие конкурента сведения об атакуемом банке (информацию о счетах других клиентов, объемах активов банков, любую другую инсайдерскую информацию, к которой агент имеет доступ) либо вносит изменения в базу данных о счетах клиентов или любую другую информацию, к которой он имеет доступ. Выявление существования такого агента может произойти только по косвенным признакам, которые могут возникнуть в результате появления изменений в базах данных. Скрытая утечка информации из базы данных, происходящая по такому СК, будет оставаться незамеченной. В этом случае в соответствии со схемой на рисунке 1:3' — программный агент, 3 — АБС, 2 — база данных, 4 — служба безопасности банка, 1 — злоумышленник, действующий в интересах конкурента, 5 — клиент банка.

Пример 2 — Злоумышленник, имеющий целью получение служебной информации с компьютера сотрудника, может действовать по следующему сценарию. Пусть ПК, защищенный межсетевым экраном, заражен троянской программой. Троянская программа получает от злоумышленника команды и отправляет в ответ на них информацию о зараженном ПК и хранящуюся на нем информацию ограниченного доступа, маскируя обмен как протокол HTTP, разрешенный межсетевым экраном. В этом случае в соответствии со схемой на рисунке 1:3' — троянская программа, 3 — программа, имеющая санкционированный доступ в Интернет, 2 — документ ограниченного распространения, 4 — межсетевой экран, 5 — узел сети Интернет, 1 — промежуточный узел сети, контролируемый злоумышленником.

Пример 3 — При использовании VPN также возможно построение СК взаимодействия агента со злоумышленником. Пусть пользователь использует свое рабочее место в качестве терминала удаленного доступа к серверу АС, т. е. информация о каждом нажатии клавиши отправляется терминалом на сервер. Злоумышленник установил на рабочее место пользователя атакуемой АС клавиатуру, содержащую агента. Агент перехватывает нажатия клавиш, а затем передает их по СК по времени, задерживая срабатывание некоторых клавиш по схеме, известной злоумышленнику. Злоумышленник, наблюдая поток пакетов между терминалом и сервером, выделяет из него информацию, передаваемую агентом по СК. Выделение скрытой информации возможно даже в случае использования криптографически защищенного канала между терминалом и сервером, так как для работы СК важно не содержимое пакетов, которыми терминал и сервер обмениваются друг с другом, а длительность временных интервалов между соседними пакетами.

В данном случае в соответствии со схемой на рисунке 1:3' — аппаратный агент, 3 — клавиатура, 2 — информация, вводимая с клавиатуры (например, пароль), 4 — любые средства обеспечения безопасности АС, не обнаруживающие закономерностей в потоках сетевых пакетов; 5 — терминальный сервер, 1 — злоумышленник.

Пример 4 — Генерация искусственных сбоев и ограничений на доступность может проводиться по СК. Например, агент, внедренный в один из ключевых компонентов АС, ожидает получения от злоумышленника некоторого условного сигнала. Получив этот сигнал, агент нарушает работу компонента АС, в которой он расположен. В результате происходит временная потеря работоспособности АС или ослабление ее защиты (если агент внедрен в средство обеспечения ИБ). Например, условным сигналом для активизации агента в общедоступном сетевом ресурсе может являться попытка аутентификации с некоторым фиксированным именем пользователя и паролем. Система разграничения доступа к сетевому ресурсу 4 не обнаружит данную атаку, поскольку попытка аутентификации является разрешенным действием. В данном случае в соответствии со схемой на рисунке 1:2 — критически важная функция, выполняемая компонентом АС (3), в который встроен агент 3'; 1 — злоумышленник, подающий агенту условный сигнал, который, с точки зрения 4, не является опасным, и поэтому не блокируется, 5 — АС.

Пример 5 — В соответствии со схемой на рисунке 1: операционная система 4 обеспечивает изоляцию программы 3, которая имеет доступ к конфиденциальной информации 2, от программы 1, выполняющейся в этой же операционной системе, но не имеющей такого доступа. Для передачи 1 информации ограниченного доступа агент нарушителя 3' организует СК по времени, производя фиктивные обращения к ресурсу 5, например, жесткому диску. Агент модулирует частоту обращений содержимым информации ограниченного доступа, которую ему необходимо передать. Программа 1, наблюдая за общесистемной нагрузкой на этот же ресурс, обнаруживает интенсивность воздействия на этот ресурс со стороны агента и может извлечь передаваемую агентом информацию из характера изменения этой интенсивности.

6 Правила формирования модели угроз безопасности с учетом существования скрытых каналов

6.1 Модель угроз безопасности формируется с учетом угроз, реализуемых с использованием СК. Эти угрозы должны учитываться при оценке рисков ИБ.

6.2 Угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя:

- внедрение вредоносных программ и данных;
- подачу злоумышленником команд агенту для выполнения;
- утечку криптографических ключей или паролей;
- утечку отдельных информационных объектов.

6.3 Угроза внедрения вредоносных программ и данных заключается в том, что, обладая возможностью интерактивно взаимодействовать с атакуемой АС, злоумышленник может передать в нее посредством СК вредоносные программы, обладающие необходимой ему функциональностью. Внедрение ложных данных в атакуемую АС может осуществлять непосредственно агент, с которым злоумышленник взаимодействует по СК. Например, если агент внедрен в СУБД банка, злоумышленник может передать ему команду на изменение хранящихся в базе данных сведений о счетах клиентов либо подменить хранящуюся в этой базе процедуру, оперирующую с данными о счетах, ложной, вредоносной процедурой, действующей в интересах злоумышленника.

6.4 Угроза подачи злоумышленником команд агенту для выполнения его функций заключается в том, что агент может оказывать влияние на АС, в которую он внедрен, по команде злоумышленника. Эти команды могут быть как простыми (например, заблокировать работу АС на некоторое время), так и более сложными (например, передать злоумышленнику по СК содержимое файла, хранящегося в атакуемой системе).

6.5 Угроза утечки криптографических ключей или паролей, отдельных информационных объектов возникает, если злоумышленнику удалось внедрить своего агента в АС так, чтобы агент имел доступ к ценным информационным активам (например, криптографическим ключам, паролям). СК могут быть использованы для несанкционированной передачи такой информации злоумышленнику. Поскольку ключи имеют сравнительно небольшой объем, даже канал с низкой пропускной способностью способен обеспечить их утечку.

7 Порядок организации защиты информации, информационных технологий и автоматизированных систем от атак, реализуемых с использованием скрытых каналов

7.1 ЗИ, ИТ и АС от атак, реализуемых с использованием СК, является циклическим процессом, включающим в себя следующие этапы, повторяющиеся на каждой из итераций процесса:

- анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием СК (см. раздел 8);
- выявление СК и оценка их опасности для активов организации (см. раздел 9);
- реализация защитных мер по противодействию СК (см. раздел 10);
- организация контроля за противодействием СК (см. раздел 11).

7.2 Цикличность процесса защиты от угроз ИБ, реализуемых с использованием СК, определяется появлением новых способов построения СК, неизвестных на момент предыдущих итераций.

8 Анализ рисков

8.1 Выбор мер противодействия угрозам ИБ, реализуемым с использованием СК, должен основаться на технико-экономической оценке или других методах оценки ценности информации. Кроме того, должны учитываться такие последствия, как утрата доверия к организации или подрыв деловой репутации организации и ее руководителя.

8.2 Следует выявить, какие из защищаемых информационных активов могут быть интересны потенциальному злоумышленнику, обладающему возможностью:

- встроить своего агента в АС в процессе ее разработки, развертывания, внедрения или эксплуатации;
- обнаружить в АС уязвимость (или встроенного агента), которая может быть использована для организации СК и получения доступа к защищаемым активам.

8.3 Для анализа рисков можно применять методологию по ГОСТ Р 51901.1.

8.4 С целью снижения информационных рисков до приемлемого уровня должны быть выбраны и внедрены мероприятия по организации ЗИ от атак с использованием СК.

9 Рекомендации по порядку выявления скрытых каналов

9.1 Порядок выявления СК включает в себя:

- оценку архитектуры АС и имеющихся в ней коммуникационных каналов;
- выявление возможных путей обмена скрытой информацией между злоумышленником и его предполагаемым агентом в АС;
- оценку опасности выявленных СК для защищаемых активов организации;
- принятие решения о целесообразности противодействия каждому из выявленных СК.

9.2 Оценка архитектуры АС подразумевает выявление всех имеющихся в ней коммуникационных каналов и анализ взаимодействия ее компонентов на предмет потенциального использования их для организации СК. В результате проведения такого анализа должны быть выявлены компоненты АС, в которых потенциально могут быть использованы СК.

9.3 Выявление возможных путей обмена скрытой информацией между злоумышленником и его предполагаемым агентом в АС проводится на основании общей схемы механизма функционирования СК (см. раздел 6). Следует для каждого из защищаемых активов *2* (см. схему на рисунке 1) выявить, какие субъекты *3* имеют к ним доступ и при этом изолированы от внешней среды, но имеют возможность взаимодействовать с отдельными субъектами из внешней среды *5*. При этом взаимодействие контролируется *4* и может также наблюдаться потенциальным злоумышленником *1*. При наличии этих элементов должен рассматриваться вопрос о возможном наличии потенциального СК между агентом *3'*, встроенным в *3*, и субъектами во внешней среде *1* или *5*. В качестве примера такого СК может рассматриваться возможность злоумышленника наблюдать интервалы времени, формируемые компонентом АС, потенциально содержащим агента злоумышленника *1*.

9.4 С точки зрения злоумышленника использовать СК для нарушения ИБ в тех сегментах АС, где он может обмениваться информацией со своим агентом, используя канал, не контролируемый средствами ЗИ, является нецелесообразным. В этом случае нет необходимости в скрытии факта обмена информацией, потому что такой обмен защитными средствами не контролируется.

9.5 При оценке возможности взаимодействия посредством СК следует учитывать «непрозрачность» для определенных типов СК отдельных сегментов АС.

9.6 После выявления СК следует оценить, насколько они реализуемы и опасны для защищаемых активов организации. Эта оценка определяется объемом активов, пропускной способностью СК и временным интервалом, в течение которого активы сохраняют ценность. На основании этой оценки каналы, не представляющие реальной опасности для активов, признаются неопасными.

9.7 На основании оценки опасности СК с учетом результатов проведенного анализа рисков делается вывод о целесообразности или нецелесообразности противодействия таким каналам.

9.8 В качестве примера на рисунке 2 представлена семиуровневая модель взаимодействия открытых систем, определенная в подпункте 6.1.5 ГОСТ Р ИСО/МЭК 7498-1—99.

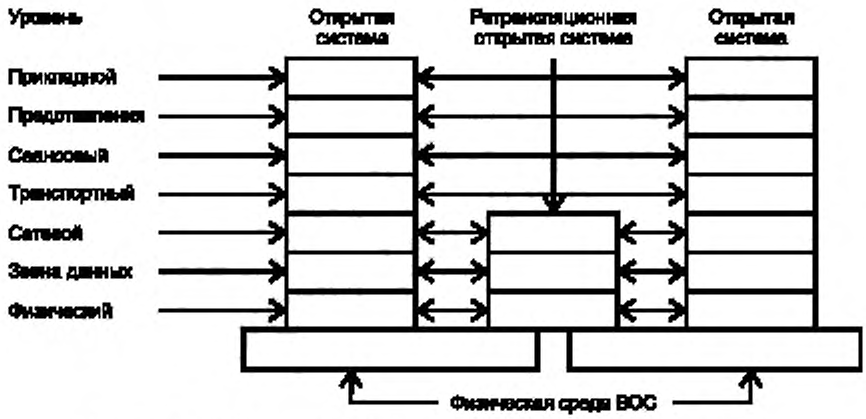


Рисунок 2 — Обмен данными через ретрансляционную открытую систему

9.9 Каждый из уровней данной модели взаимодействует только с нижестоящим и вышестоящим уровнями, при этом верхние уровни открытой системы изолированы от нижних. Эта особенность может быть использована для маскировки СК, действующих на низком уровне, от контролера, находящегося на высоком уровне.

9.10 В случае если специальные средства обнаружения СК не применяются, наличие СК может обнаружить пользователь какой-либо из взаимодействующих систем, наблюдая изменение поведения этих систем или частичную потерю их работоспособности.

9.11 Ограничивающим фактором при выборе злоумышленником уровня модели взаимодействия открытых систем в качестве среды для организации скрытой передачи является «непрозрачность» ретранслирующих систем. Ретранслирующие системы не содержат исходного отправителя и конечного получателя данных, а лишь передают данные от одних систем другим, если они не соединены единой физической средой в соответствии с ГОСТ Р ИСО/МЭК 7498-1.

9.12 При осуществлении ретрансляции в такой системе проводят интерпретацию полученной информации на всех уровнях модели, начиная с нижнего (физического) уровня, до уровня, на котором осуществляется ретрансляция данных. Затем, для передачи данных далее по сети, они вновь «спускаются» до физического уровня сети-получателя. В результате этого процесса, СК по памяти (см. подраздел 5.2 ГОСТ Р 53113.1—2008), использующие особенности протоколов, относящихся к более низким уровням, чем тот, на котором осуществляется ретрансляция, могут уничтожаться или ограничивать возможности скрытой передачи информации сквозь такую ретранслирующую систему.

10 Рекомендации по методам реализации защитных мероприятий по противодействию скрытым каналам

10.1 По результатам выявления СК формируется план мероприятий по противодействию угрозам, реализуемым с их использованием. Данные мероприятия могут включать в себя реализацию одного из уже известных (либо усовершенствование уже существующих) методов противодействия угрозам ИБ, реализуемым с использованием СК.

10.2 В качестве защитных мероприятий целесообразно использовать:

- снижение пропускной способности канала передачи информации;
- архитектурные решения построения АС;
- мониторинг эффективности защиты АС.

10.3 Выбор методов противодействия угрозам ИБ, реализуемым с использованием СК и формирование плана по их реализации определяется экспертами, исходя из индивидуальных особенностей защищаемой АС.

10.4 Примеры методов противодействия СК

Пример 1 — Противодействием угрозам, связанным с СК, является, в частности, нормализация трафика, заключающаяся в изменении значений полей сетевых пакетов так, чтобы исключить не-

однозначность, которую потенциально можно использовать для организации СК. При этом разрушаются СК, использующие для своей работы такую неоднозначность. В результате нормализации трафика должно обеспечиваться сохранение функциональности исходного протокола, необходимой для выполнения возложенной на него задачи. Нормализация полей пакетов информации может заключаться в приведении значений полей в соответствие со спецификациями протоколов, помещении в поля пакетов фиксированных значений или записи в поля произвольных значений.

Пример 2 — Использование посредника (прокси-сервера), т. е. устройства, имеющего доступ к двум или более сетям, принимающего запросы от приложений, выполняющихся на узлах одной из доступных ему сетей, к приложениям, выполняющимся на узлах другой сети, а затем передающего ответы на эти запросы в обратном направлении. Применение посредника позволяет предотвратить использование для организации СК особенностей протоколов, обеспечивающих работу сети. Детали реализации этих протоколов (например, значений отдельных служебных полей пакетов этих протоколов) при использовании посредника не передаются напрямую из одной сети в другую, а формируются посредником заново. Таким образом, СК по памяти, использующие в качестве среды передачи сетевые протоколы, не будут обеспечивать скрытый обмен информацией между абонентами, разделенными посредником. Работоспособность приложений, взаимодействующих не напрямую, а «сквозь» (через) посредника, не будет нарушена, поскольку посредник учитывает особенности работы этих приложений. Это позволяет без принятия дополнительных мер перекрыть многие СК, связанные с синтаксисом и семантикой сетевого, а также транспортного протоколов. Тем не менее перекрыть каналы, работающие на уровне приложений, таким способом не удастся, так как скрытая информация будет проходить через посредника без изменений вместе с данными приложения. Применяемое приложение-посредник должно учитывать специфику используемых приложений и транспортных протоколов, чтобы полностью сохранить все их функции и не привести к потере производительности сети. В свою очередь, приложения могут быть разработаны с учетом использования посредника.

Пример 3 — Инкапсуляция трафика Интернет («туннелирование») — транзитная передача пакетов из одной подсети в другую подсеть через третью сеть, при которой исходные пакеты «упаковываются» в пакеты туннельного протокола, передаваемые через третью сеть, представлена на рисунке 3

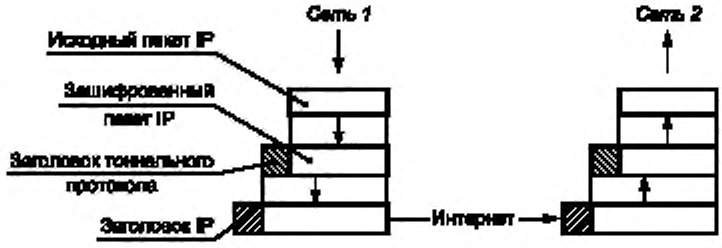


Рисунок 3 — Инкапсуляция IP-пакетов

10.5 При использовании инкапсуляции с шифрованием и подтверждением целостности пакета возможно перекрытие СК по памяти между узлами, «внутренними» по отношению к шлюзу (т. е. теми узлами, которые формируют пакеты, проходящие по тоннелю), и «внешними» (шлюзы Интернет, через которые проходит маршрут, по которому отправляются пакеты тоннельного протокола). СК по времени (см. подраздел 5.3 ГОСТ Р 53113.1—2008), оперирующие с моментами времени, в которые происходит передача пакетов, не могут быть полностью перекрыты таким способом. Информация, связанная с размерами пакетов и временными интервалами между их появлением, также сохраняется при инкапсуляции, и может быть использована для работы СК.

11 Рекомендации по организации контроля за противодействием скрытым каналам

11.1 Контроль за противодействием СК заключается в выявлении фактов использования СК в защищаемой АС. Такое выявление может проводиться непрерывно либо по факту обнаружения признаков ущерба от использования СК. Для выявления использования СК могут применяться статистический или сигнатурный методы.

11.2 Статистический метод выявления СК подразумевает сбор статистических данных о пакетах, проходящих через защищаемый участок сети, без внесения в них каких-либо изменений. Выявление СК может проводиться как в режиме реального времени (что позволяет быстро реагировать на инциденты), так и автономно, используя данные, накопленные за предыдущие отрезки времени, что делает возможным проведение более глубокого их анализа.

11.3 Метод выявления СК на основе сигнатурного анализа аналогичен способу, используемому антивирусными программами для поиска вредоносных программ. При наличии набора известных реализаций СК, для каждой из них формируется сигнатура, представляющая собой набор признаков, которые свидетельствуют о том, что используется данная реализация СК. Затем инспектор *4* (см. рисунок 1) проводит поиск таких сигнатур в просматриваемом потоке данных в сети и делает вывод о наличии или отсутствии в нем действующего СК в той или иной реализации. Для эффективной работы такого метода необходимо постоянное обновление базы сигнатур, т. е. включение в нее сигнатур для ранее неизвестных реализаций СК.

11.4 При выявлении признаков (в том числе косвенных) использования СК или появлении новых способов построения СК анализ рисков проводят повторно.

Библиография

[1] Руководящий документ. Гостехкомиссия России, 1999 г. — Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей

[2] Руководящий документ. Гостехкомиссия России, 1998 г. — Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации

УДК 351.864.1:004:006.354 ОКС 35.040 Т00

Ключевые слова: скрытые каналы, анализ скрытых каналов, порядок организации защиты информации

Редактор *Н.В. Таланова*
Технический редактор *И.Е. Черепкова*
Корректор *Р.А. Ментова*
Компьютерная верстка *Е.Е. Кругова*

Сдано в набор 10.10.2018. Подписано в печать 29.10.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,20.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru

gost.e-ecolog.ru

gost.e-ecolog.ru