ГОСТ Р 53113.1-2008

Группа Т00

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

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

Часть 1

Общие положения

Information technology. Protection of information technologies and automated systems against security threats posed by use of covert channels. Part 1. General principles

ОКС 35.040

Дата введения 2009-10-01

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании", а правила применения национальных стандартов Российской Федерации - ГОСТ Р 1.0-2004 "Стандартизация в Российской Федерации. Основные положения"

Сведения о стандарте

1 РАЗРАБОТАН Обществом с ограниченной ответственностью "Криптоком"

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. N 531-ст

4 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе "Национальные стандарты", а текст изменений и поправок - в ежемесячно издаваемых информационных указателях "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе "Национальные стандарты". Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

Введение

Развитие, внедрение и использование распределенных информационных систем и технологий, использование импортных программно-аппаратных платформ без конструкторской документации привели к появлению класса угроз информационной безопасности (ИБ), связанных с использованием так называемых скрытых информационных каналов, "невидимых" для традиционных средств защиты информации.

Традиционные средства обеспечения ИБ такие, как средства разграничения доступа, межсетевые экраны, системы обнаружения вторжений, контролируют только информационные потоки, которые проходят по каналам, предназначенным для их передачи. Возможность обмена информацией вне этих рамок посредством скрытых каналов (СК) не учитывается.

В системах, требующих обеспечения повышенного уровня доверия, должны учитываться угрозы безопасности, возникающие вследствие наличия возможности несанкционированного действия с помощью СК.

Опасность СК для информационных технологий (ИТ) и автоматизированных систем (АС) и других активов организации связана с отсутствием контроля средствами защиты информационных потоков, что может привести к утечке информации, нарушить целостность информационных ресурсов и программного обеспечения в компьютерных системах или создать иные препятствия по реализации ИТ.

Для обеспечения защиты информации, обрабатываемой в АС, необходимо выявлять и нейтрализовывать все возможные информационные каналы несанкционированного действия - как традиционные, так и скрытые.

Настоящий стандарт входит в серию взаимосвязанных стандартов, объединенных общим наименованием "Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов", включающий в себя:

- общие положения;

- рекомендации по организации защиты информации, ИТ и АС от атак с использованием СК.

В общих положениях определены задачи, решаемые при проведении анализа СК, описана классификация СК и приведена классификация активов по степени опасности атак с использованием СК.

Существенным моментом защищенности систем ИТ и АС является доверие к системам защиты. Обеспечение доверия осуществляется путем глубокого анализа или экспертизы программно-аппаратных продуктов с точки зрения их защищенности. Во многих случаях этот анализ затруднен в силу отсутствия исходных данных для его проведения, то есть исходных кодов, конструкторской и тестовой документации, в результате чего создаются угрозы информационным ресурсам, которые могут быть реализованы с помощью неизвестных программно-аппаратных систем и через интерфейсы взаимодействующих программно-аппаратных продуктов.

Требования доверия к безопасности информации установлены в ГОСТ Р ИСО/МЭК 15408-3, в соответствии с которым для систем с оценочным уровнем доверия (ОУД), начиная с ОУД5, предусмотрено проведение обязательного анализа СК. При использовании аппаратно-программных продуктов иностранных производителей в условиях отсутствия на них конструкторской, тестовой документации и исходных кодов невозможно гарантировать отсутствие в них потенциально вредоносных компонентов, включенных специально или возникших случайно (например, программной уязвимости). Таким образом, требование анализа СК в Российской Федерации является необходимым условием безопасного функционирования систем, обрабатывающих ценную информацию или использующих импортное аппаратно-программное обеспечение, в том числе и для систем с ОУД ниже ОУД5.

В рекомендациях по организации защиты информации, ИТ и АС от атак с использованием СК определен порядок поиска СК и противодействия СК.

Настоящий стандарт разработан в развитие ГОСТ Р ИСО/МЭК 15408-3, ГОСТ Р ИСО/МЭК 17799 (в части мероприятий по противодействию угрозам ИБ, реализуемым с использованием СК) и [1].

1 Область применения

Настоящий стандарт устанавливает классификацию СК и определяет задачи, решаемые при проведении анализа СК, что является необходимой составляющей для определения дальнейшего порядка организации защиты информации от атак с использованием СК, а также устанавливает порядок проведения анализа СК для продуктов и систем ИТ и АС, результаты которого используются при оценке доверия к мерам защиты информационных систем и ИТ.

Настоящий стандарт предназначен для заказчиков, разработчиков и пользователей ИТ при формировании ими требований к разработке, приобретению и применению продуктов и систем ИТ, которые предназначены для обработки, хранения или передачи информации, подлежащей защите в соответствии с требованиями нормативных документов или требованиями, устанавливаемыми собственником информации. Настоящий стандарт предназначен также для органов сертификации и испытательных лабораторий при проведении оценки безопасности и сертификации безопасности ИТ и АС, а также для аналитических подразделений и служб безопасности для сопоставления угроз ценным информационным активам с потенциальной возможностью ущерба через СК.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

ГОСТ Р ИСО/МЭК 17799-2006* Информационная технология. Практические правила управления информационной безопасностью

_____

* Вероятно ошибка оригинала. Следует читать ГОСТ Р ИСО/МЭК 17799-2005. - Примечание изготовителя базы данных.

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 ежегодно издаваемому информационному указателю "Национальные стандарты", который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **автоматизированная система:** Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

3.2 **агент нарушителя:** Лицо, программное, программно-аппаратное или аппаратное средство, действующие в интересах нарушителя.

3.3 **активы** (assets): Все, что имеет ценность для организации и находится в ее распоряжении.

Примечание - К активам организации могут относиться:

- вычислительные, телекоммуникационные и прочие ресурсы;

- информационные активы, в т.ч. различные виды информации на следующих фазах их жизненного цикла: генерация (создание), обработка, хранение, передача, уничтожение;

- продукты и услуги, предоставляемые сторонним организациям.

3.4 **блокирование доступа (к информации):** Прекращение или затруднение доступа законных пользователей к информации.

3.5 **вредоносная программа:** Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

3.6 **глубина анализа скрытого канала:** Степень варьирования применяемых средств по сложности для идентификации скрытого канала и его характеристик.

3.7 **доверие** (assurance): Основание для уверенности в том, что объект соответствует целям безопасности.

3.8 **идентификация скрытого канала:** Выявление возможности существования скрытого канала и определение его места в классификации.

3.9 **информация ограниченного доступа:** Вид сведений, доступ к которым ограничен и разглашение которых может нанести ущерб интересам других лиц, общества и государства.

3.10 **информационная безопасность** (information security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

3.11 **информационная система:** Организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Примечание - Информационные системы предназначены для хранения, обработки, поиска, распространения, передачи и предоставления информации.

3.12 **информационная технология:** Приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных.

3.13 **информационный объект:** Элемент программы, содержащий фрагменты информации, циркулирующей в программе.

Примечание - В зависимости от языка программирования в качестве информационных объектов могут выступать переменные, массивы, записи, таблицы, файлы, фрагменты оперативной памяти и т.п.

3.14 **информационный поток** (information flow): Процесс взаимодействия источника информации и ее получателя.

Примечание - Информационный поток может быть разрешенным и неразрешенным. Информационный поток между объектами X и Y существует, если средняя взаимная информация I (X, Y) больше 0. Математическая модель информационного потока может определяться как конечный автомат, в котором источник сообщения посылает входное слово на вход автомата, а получатель сообщения видит выходную последовательность автомата.

3.15 **исчерпывающий анализ скрытых каналов** (exhaustive covert channel analysis): Анализ, при котором требуется представление дополнительного свидетельства, показывающего, что план идентификации скрытых каналов достаточен для утверждения того, что были испробованы все возможные пути исследования скрытых каналов.

3.16 **ключ:** Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

3.17 **коммуникационный канал:** Совокупность носителей информации, доставляющих сообщение от источника к приемнику.

3.18 **критически важные объекты:** Объекты, нарушение или прекращение функционирования которых приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению или разрушению экономики страны, субъекта или административно-территориальной единицы или к существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях длительный период времени.

3.19 **механизм передачи информации:** Реализованный способ передачи информации от отправителя к получателю.

3.20 **модификация информации:** Целенаправленное изменение формы представления и содержания информации.

3.21 **нарушитель безопасности информации** (adversary): Физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.

3.22 **несанкционированный доступ к информации** (unauthorized access to information): Доступ к информации или действия с информацией, нарушающие правила разграничения доступа

с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Примечание - Доступ к объекту подразумевает и доступ к содержащейся в нем информации.

3.23 **объект** (object): Пассивный компонент системы, хранящий, принимающий или передающий информацию.

3.24 **оценка опасности:** Определение степени возможного деструктивного воздействия.

3.25 **оценочный уровень доверия** (evaluation assurance level): Пакет компонентов доверия, представляющий некоторое положение на предопределенной в нем шкале доверия.

Примечание - Пакет компонентов доверия определяется в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3.

3.26 **пароль доступа** (password): Идентификатор субъекта доступа, который является его (субъекта) секретом.

3.27 **персональные данные:** Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Примечание - В качестве персональных данных могут использоваться фамилия, имя, отчество, год, месяц, дата и место рождения субъекта персональных данных, а также адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация.

3.28 **политика безопасности информации** (information security policy): Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности .

3.29 **продукт** (product): Совокупность программных, программно-аппаратных и/или аппаратных средств информационных технологий, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы.

3.30 **пропускная способность скрытого канала** (covert channel capacity): Количество информации, которое может быть передано по скрытому каналу в единицу времени или относительно какой-либо другой шкалы измерения.

3.31 **система** (system): Специфическое воплощение информационных технологий с конкретным назначением и условиями эксплуатации.

3.32 **систематический анализ скрытых каналов** (systematic covert channel analysis): Анализ,

при котором разработчик системы информационных технологий и автоматизированных систем должен идентифицировать скрытые каналы структурированным и повторяемым образом в противоположность идентификации скрытых каналов частным методом, применимым для конкретной ситуации.

Примечание - Идентификация скрытых каналов осуществляется, как правило, в соответствии с планом обеспечения безопасности.

3.33 **скрытый канал** (covert channel): Непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности.

3.34 **среда передачи:** Физическая реализация процесса передачи информации.

3.35 **субъект** (subject): Активный компонент системы, обычно представленный в виде пользователя, процесса или устройства, которые могут явиться причинами потока информации от объекта к объекту или изменения состояния системы.

3.36 **угроза безопасности** (threat): Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

3.37 **уполномоченный пользователь** (authorised user): Пользователь, которому в соответствии с политикой безопасности разрешено выполнять какую-либо операцию.

3.38 **ущерб:** Отрицательные последствия, возникающие вследствие причинения вреда активам .

3.39 **уязвимость:** Свойство системы, которое можно использовать для нарушения информационной безопасности системы информационных технологий и автоматизированных систем.

4 Общие положения

4.1 Настоящий стандарт определяет следующий порядок действий по определению степени опасности СК для активов организации, выявлению и противодействию СК:

- проведение классификации активов в зависимости от степени опасности атак с использованием СК с учетом возможных угроз безопасности активам;

- определение необходимой глубины анализа СК в зависимости от типа активов;

- проведение анализа СК, включающее в себя выполнение следующих задач:

идентификация (выявление) СК,

оценка пропускной способности СК и оценка опасности, которую несет их скрытое функционирование;

- мероприятия по защите от угроз, реализуемых с использованием СК, и включающие в себя выполнение следующих задач:

принятие решений о внедрении защитных мер для противодействия указанным угрозам безопасности,

противодействие реализации СК вплоть до его уничтожения.

4.2 Классификация защищаемых активов в зависимости от степени опасности атак с использованием СК приведена в разделе 7.

4.3 Глубину анализа СК определяют ценностью активов, то есть ущербом, который может быть причинен в результате реализации угроз безопасности, реализуемых с использованием СК, то есть рисков, возникающих вследствие наличия этих угроз. Классификация таких угроз приведена в разделе 6.

4.4 Идентификация СК определяет субъекты (источник и получателя), между которыми потенциально может существовать СК, параметры, при манипулировании которыми происходит передача информации, параметры, за счет вариации которых происходит чтение информации, среду передачи информации, логические условия, при которых возможна передача информации. Идентификация СК может проводиться как при разработке системы путем исследования потенциальных каналов утечки или каналов воздействия, так и в режиме эксплуатации системы путем наблюдения признаков, идентифицирующих наличие СК. В последнем случае СК выявляются с помощью наблюдения за параметрами системы. В документации по безопасности информации должно быть отражено, какие классы СК могут быть выявлены с помощью используемой системы наблюдения.

4.5 Оценку пропускной способности идентифицированных СК проводят формальными, техническими методами или методами моделирования.

4.6 При принятии решений о внедрении защитных мер для противодействия угрозам безопасности, реализуемым с использованием СК, необходимо учитывать возможный риск нанесения ущерба активам организации, который связан в том числе с пропускной способностью СК.

4.7 Противодействие опасным СК может осуществляться с помощью следующих средств и методов:

- построение архитектуры ИТ или АС, позволяющей перекрыть СК или сделать их пропускную способность настолько низкой, что каналы становятся неопасными. Этот метод применяется на этапе проектирования ИТ или АС;

- использование технических средств, позволяющих перекрывать СК или снижать их пропускную способность ниже заданного уровня;

- использование программно-технических средств, позволяющих выявлять работу опасных СК в процессе эксплуатации системы. Выявление признаков работы СК может позволить блокировать их воздействие на информационные ресурсы;

- применение организационно-технических мер, позволяющих ликвидировать СК или уменьшить их пропускную способность до безопасного значения.

5 Классификация скрытых каналов

5.1 СК по механизму передачи информации подразделяют на:

- СК по памяти;

- СК по времени;

- скрытые статистические каналы.

5.2 СК по памяти основаны на наличии памяти, в которую передающий субъект записывает информацию, а принимающий - считывает ее.

Скрытость каналов по памяти определяется тем, что сторонний наблюдатель не знает того места в памяти, где записана скрываемая информация.

СК по памяти предполагают использование ресурсов памяти, однако способ использования памяти не учитывается разработчиками системы защиты и поэтому не может выявляться используемыми средствами защиты.

5.3 СК по времени предполагают, что передающий информацию субъект модулирует с помощью передаваемой информации некоторый изменяющийся во времени процесс, а субъект, принимающий информацию, в состоянии демодулировать передаваемый сигнал, наблюдая несущий информацию процесс во времени. Например, в многозадачной операционной системе (ОС) центральный процессор является разделяемым информационно-вычислительным ресурсом для прикладных программ. Модулируя время занятости процессора, приложения могут передавать друг другу нелегальные данные.

5.4 Скрытый статистический канал использует для передачи информации изменение параметров распределений вероятностей любых характеристик системы, которые могут рассматриваться как случайные и описываться вероятностно-статистическими моделями.

Скрытость таких каналов основана на том, что получатель информации имеет меньшую неопределенность в определении параметров распределений наблюдаемых характеристик системы, чем наблюдатель, не имеющий знаний о структуре СК.

Например, появление реальной, но маловероятной комбинации в присланном пакете в заданный промежуток времени может означать сигнал к сбою в компьютерной системе.

5.5 СК по памяти, в свою очередь, подразделяют на:

- СК, основанные на сокрытии информации в структурированных данных;

- СК, основанные на сокрытии информации в неструктурированных данных.

5.6 СК, основанные на сокрытии информации в структурированных данных, используют встраивание данных в информационные объекты с формально описанной структурой и формальными правилами обработки. Например, внутренний формат файлов, используемых современными текстовыми процессами, содержит ряд полей, не отображаемых при редактировании файла, поэтому они могут быть использованы для вставки скрытой информации.

5.7 СК, основанные на сокрытии информации в неструктурированных данных, используют встраивание данных в информационные объекты без учета формально описанной структуры (например, запись скрытой информации в наименее значимые биты изображения, не приводящая к видимым искажениям изображения).

5.8 СК по пропускной способности подразделяют на:

- канал с низкой пропускной способностью;

- канал с высокой пропускной способностью.

5.9 СК является каналом с низкой пропускной способностью, если его пропускной способности достаточно для передачи ценных информационных объектов минимального объема (например, криптографические ключи, пароли) или команд за промежуток времени, на протяжении которого данная передача является актуальной.

5.10 СК является каналом с высокой пропускной способностью, если его пропускная способность позволяет передавать информационные объекты среднего и большого размера (например, текстовые файлы, изображения, базы данных) за промежуток времени, на протяжении которого данные информационные объекты являются ценными.

Для решения сложных задач может использоваться комбинация СК, опирающихся на различные механизмы передачи.

6 Классификация угроз безопасности, реализуемых с использованием скрытых каналов

6.1 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.

6.2 Реализация данных угроз может привести к:

- нарушению конфиденциальности информационных активов;

- нарушению работоспособности ИТ и АС;

- блокированию доступа к ресурсам;

- нарушению целостности данных и ПО.

6.3 Системами, наиболее подверженным атакам с использованием СК, являются:

- многопользовательские распределенные системы;

- системы с выходом в глобальные сети;

- системы, использующие криптографические средства защиты;

- системы, использующие многоуровневую (мандатную) политику разграничения доступа;

- системы, программно-аппаратные агенты в которых не могут быть обнаружены (в связи с использованием программного и аппаратного обеспечения с недоступным исходным кодом и в связи с отсутствием конструкторской документации).

6.4 Взаимосвязь угроз, реализуемых с помощью СК, с типами СК в зависимости от их пропускной способности приведена в таблице 1.

Таблица 1 - Взаимосвязь угроз, реализуемых с помощью скрытых каналов, с типами скрытых каналов в зависимости от их пропускной способности

Угроза	Тип скрытых каналов	
	Скрытые каналы с низкой пропускной способностью	Скрытые каналы с высокой пропускной способностью

Внедрение вредоносных программ и данных	+	+
Подача злоумышленником команд агенту для выполнения	+	+
Утечка криптографических ключей или паролей	+	+
Утечка отдельных информационных объектов	-	+

Примечание - знак "+" - означает, что имеется связь угрозы с соответствующим типом скрытого канала; знак "-" - означает, что связи не существует.

7 Классификация активов по степени опасности атак с использованием скрытых каналов

7.1 В зависимости от степени опасности атак с использованием СК защищаемые активы организации подразделяют на следующие классы:

1-й класс - активы, содержащие информацию, степень подверженности которой атакам, реализуемым с использованием СК, определяет собственник.

2-й класс - активы, содержащие информацию ограниченного доступа или персональные данные и обрабатываемые в системах, имеющих технические интерфейсы с открытыми сетями или компьютерными системами общего доступа, а также компьютерными системами, не предполагающими защиту от утечки по техническим каналам.

3-й класс - активы, содержащие сведения, составляющие государственную тайну.

7.2 Кроме того, существует особый класс активов, которые уязвимы с точки зрения угроз, реализуемых с использованием СК с низкой пропускной способностью. К этой группе относятся:

Класс А - активы, связанные с функционированием критически важных объектов. Например, передача команды, способной инициализировать деструктивное воздействие на объект такого типа, может быть осуществлена по СК с низкой пропускной способностью.

Класс Б - активы, содержащие ключевую/парольную информацию, в том числе ключи криптографических систем защиты информации и пароли доступа к иным активам. Например, утечка ключевой/парольной информации по СК может поставить под угрозу функционирование всей информационной системы.

Библиография

[1] Руководящий документ. Гостехкомиссия России — Безопасность информационных технологий. Руководство по формированию семейств профилей защиты

Электронный текст документа
подготовлен ЗАО "Кодекс" и сверен по:
официальное издание
М.: Стандартинформ, 2009