ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56545— 2015

Защита информации

УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Правила описания уязвимостей

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. № 1180-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 1
4 Основные положения 2
5 Структура и содержание описания уязвимостей 2
Приложение А (рекомендуемое) Форма паспорта уязвимости с примером его заполнения 6
Библиография 8

Введение

Настоящий стандарт входит в комплекс стандартов, устанавливающих классификацию уязвимостей, правила описания уязвимостей, содержание и порядок выполнения работ по выявлению и оценке уязвимостей информационных систем (ИС).

Настоящий стандарт распространяется на деятельность по защите информации, связанную с выявлением, описанием, устранением или исключением возможности использования уязвимостей ИС при разработке, внедрении и эксплуатации ИС.

В настоящем стандарте приняты правила описания уязвимостей, которые могут быть использованы специалистами по информационной безопасности при создании и ведении базы данных уязвимостей ИС, разработке средств контроля (анализа) защищенности информации, разработке моделей угроз безопасности информации и проектировании систем защиты информации, проведении работ по идентификации, выявлению уязвимостей, их анализу и устранению.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Правила описания уязвимостей

Information protection. Vulnerabilities in information systems. Rules of vulnerabilities description

Дата введения — 2016—04—01

1 Область применения

Настоящий стандарт устанавливает общие требования к структуре описания уязвимости и правилам описания уязвимости информационной системы (ИС). В настоящем стандарте принята структура описания уязвимости, использование которой позволит обеспечить достаточность информации для идентификации уязвимости ИС и выполнения работ по анализу уязвимостей ИС.

Настоящий стандарт не распространяется на уязвимости ИС, связанные с утечкой информации по техническим каналам, в том числе уязвимости электронных компонентов технических (аппаратных и аппаратно-программных) средств информационных систем.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

ГОСТ Р 56546 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем

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 ежемесячного 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 следующие термины с соответствующими определениями:

3.1 **информационная система:** Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Примечание — Определение термина соответствует [1].

Издание официальное

3.2 **угроза безопасности информации:** Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

3.3 **уязвимость:** Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

3.4 **правила описания уязвимости:** Совокупность положений, регламентирующих структуру и содержание описания уязвимости.

3.5 **описание уязвимости:** Информация о выявленной уязвимости.

3.6 **паспорт уязвимости:** Документ (формализованное представление), содержащий(ее) описание уязвимости, определяющий(ее) характеристики уязвимости и выполненный(ое) в соответствии с правилами описания уязвимости.

3.7 **известная уязвимость:** Уязвимость, опубликованная в общедоступных источниках с описанием соответствующих мер защиты информации, исправлений недостатков или соответствующих обновлений.

3.8 **уязвимость нулевого дня:** Уязвимость, которая становится известной до момента выпуска разработчиком компонента информационной системы соответствующих мер защиты информации, исправлений недостатков или соответствующих обновлений.

3.9 **впервые выявленная уязвимость:** Уязвимость, не опубликованная в общедоступных источниках.

4 Основные положения

4.1 Описание уязвимости ИС выполняется в соответствии с правилами описания.

4.2 Правила описания уязвимостей ИС распространяются на известные уязвимости, уязвимости нулевого дня и впервые выявленные уязвимости.

4.3 Описание уязвимости ИС оформляется в виде паспорта уязвимости, форма которого и пример заполнения представлены в таблице А.1 (приложение А).

5 Структура и содержание описания уязвимостей

5.1 Общие требования к структуре описания уязвимости

5.1.1 Структура описания уязвимости должна обеспечивать достаточность информации для идентификации уязвимости ИС и выполнения работ по анализу уязвимостей ИС.

5.1.2 Для однозначной идентификации уязвимости описание должно включать следующие элементы:

- идентификатор уязвимости;
- наименование уязвимости;
- класс уязвимости;
- наименование программного обеспечения (ПО) и его версия.

5.1.3 Для обеспечения работ по анализу уязвимостей ИС описание должно включать следующие элементы:

- идентификатор типа недостатка;
- тип недостатка;
- место возникновения (проявления) уязвимости;
- способ (правило) обнаружения уязвимости;
- возможные меры по устранению уязвимости.

5.1.4 Для обеспечения детальной информации об уязвимости описание может включать следующие элементы:

- наименование операционной системы и тип аппаратной платформы;
- язык программирования ПО;
- служба (порт), которую(ый) используют для функционирования ПО;
- степень опасности уязвимости.
- краткое описание уязвимости;
- идентификаторы других систем описаний уязвимостей;
- дата выявления уязвимости;
- автор, опубликовавший информацию о выявленной уязвимости;
- критерии опасности уязвимости.

5.1.5 Дополнительно описание уязвимости ИС может включать прочую информацию в составе следующих элементов:

- описание реализуемой технологии обработки (передачи) информации;
- описание конфигурации ПО, определяемой параметрами установки;
- описание настроек ПО, при которых выявлена уязвимость;
- описание полномочий (прав доступа) к ИС, необходимых нарушителю для эксплуатации уязвимости;
- описание возможных угроз безопасности информации, реализация которых возможна при эксплуатации уязвимости;
- описание возможных последствий от эксплуатации уязвимости ИС;
- наименование организации, которая опубликовала информацию о выявленной уязвимости;
- дата опубликования уведомления о выявленной уязвимости, а также дата устранения уязвимости разработчиком ПО;
- другие сведения.

5.2 Общие требования к содержанию описания уязвимости

5.2.1 Содержание описания уязвимости должно обеспечить однозначность и полноту информации об уязвимости.

5.2.2 Элемент «Наименование уязвимости» представляет собой текстовую информацию об уязвимости, на основе которой возможно установить причину и (или) последствия уязвимости. Наименование уязвимости должно быть представлено на русском языке (в скобках на английском языке — при необходимости).

Пример — Описание уязвимости в части элемента «Наименования уязвимости»: уязвимость, приводящая к переполнению буфера в службе RPC DCOM в операционных системах Microsoft Windows 4.0/2000/XP/2003 (Vulnerability Windows XP RPCSS DCOM Buffer Overflow).

5.2.3 Элемент «Идентификатор уязвимости» представляет собой алфавитно-цифровой код, включающий код базы данных уязвимостей, год выявления уязвимости и порядковый номер уязвимости, выявленной в текущем году. При определении идентификатора уязвимости код базы данных уязвимостей, год выявления уязвимости и порядковый номер уязвимости должны быть отделены друг от друга знаком «—», при этом знак пробела не ставится.

Пример — Описание уязвимости в части элемента «Идентификатор уязвимости»: XXX-2003-0813.

5.2.4 Элемент «Идентификаторы других систем описаний уязвимостей» представляет собой идентификаторы уязвимости в других системах описаний. Данный элемент включает идентификаторы уязвимости из общедоступных источников и содержит, как правило, цифровой или алфавитно-цифровой код. Описание может быть выполнено в виде гиперссылок в формате адресов URL.

Пример — Описание уязвимости в части элемента «Идентификаторы других систем описаний уязвимостей»: CVE ID: CVE-2003-0813; Bugtraq ID: 52018; OSVDB ID: 65465; Qualys ID: 90777; Secunia Advisory: SA48183; SecurityTracker Alert ID: 1025250; Nessus Plugin ID: 38099.

5.2.5 Элемент «Краткое описание уязвимости» представляет собой текстовую информацию об уязвимости и возможностях ее использования.

Пример — Описание уязвимости в части элемента «Краткое описание уязвимости»: уязвимость обнаружена в службе RPC DCOM. Нарушитель может вызвать отказ в обслуживании (аварийное завершение работы системы или перезагрузка), создавая два потока для одного и того же RPC-запроса. По сообщению разработчика, уязвимость может использоваться для выполнения произвольного кода в уязвимой системе. Разработчик оценил, что уязвимость имеет «критический» уровень опасности.

5.2.6 Элемент «Класс уязвимости» представляет собой текстовую информацию, которую определяют в соответствии с ГОСТ Р 56546.

Пример — Описание уязвимости в части элемента «Класс уязвимости»: уязвимость кода.

5.2.7 Элемент «Наименование программного обеспечения и его версия» представляет собой информацию о наименовании ПО и его версии.

Пример — Описание уязвимости в части элемента «Наименование программного обеспечения и его версия»: RPC/DCOM Microsoft Windows 4.0/2000/XP/2003.

5.2.8 Элемент «Служба (порт), которую(ый) используют для функционирования ПО», представляет собой комбинированную информацию о службе (системной или сетевой), о сетевом порте, который используют для функционирования ПО, и о наименовании сетевого протокола передачи данных. Номер сетевого порта и наименование сетевого протокола передачи данных отделяют друг от друга знаком «/».

Примечание — Служба (порт), которую(ый) используют для функционирования ПО, может не иметь постоянного значения. ПО может быть назначен порт по умолчанию, но практически любое ПО может быть переконфигурировано на другой порт.

Пример — Описание уязвимости в части элемента «Служба (порт), которую(ый) используют для функционирования ПО»: RPC 139/tcp.

5.2.9 Элемент «Язык программирования ПО» представляет собой наименование языка программирования, используемого при разработке (представлении) ПО. Современное ПО, как правило, разрабатывают с использованием семейства языков программирования, поэтому данный элемент может включать информацию о технологии (среде) программирования.

Пример — Описание уязвимости в части элемента «Язык программирования ПО»: C++.

5.2.10 Элемент «Тип недостатка» представляет собой текстовую информацию, которую определяют в соответствии с ГОСТ Р 56546.

Пример — Описание уязвимости в части элемента «Тип недостатка»: недостатки, связанные с переполнением буфера памяти.

5.2.11 Элемент «Идентификатор типа недостатка» представляет собой уникальный идентификатор типа недостатка и содержит алфавитно-цифровой код. Идентификатор может быть взят (и при необходимости дополнен) из общедоступных источников.

Пример — Описание уязвимости в части элемента «Идентификатор типа недостатка»: CWE-119.

5.2.12 Элемент «Место возникновения (проявления) уязвимости» представляет собой текстовую информацию о компонентах информационной системы, которые содержат рассматриваемую уязвимость.

Пример — Описание уязвимости в части элемента «Место возникновения (проявления) уязвимости»: уязвимость в общесистемном (общем) ПО.

5.2.13 Элемент «Наименование операционной системы и тип аппаратной платформы» представляет собой информацию об операционной системе и типе аппаратной платформы. Типами аппаратной платформы являются: IA-32, IA-64, X86, ARM, PA-RISC, SPARC, System z и другие.

Пример — Описание уязвимости в части элемента «Наименование операционной системы и тип аппаратной платформы»: Microsoft Windows 4.0/2000/XP/2003 (×32).

5.2.14 Элемент «Дата выявления уязвимости» представляет собой информацию о дате выявления уязвимости в формате ДД/ММ/ГГГГ. Дата выявления уязвимости в случае фактической невозможности ее установления считается совпадающей с датой регистрации сообщения об уязвимости в базе данных уязвимостей.

Пример — Описание уязвимости в части элемента «Дата выявления уязвимости»: 23/12/2004.

5.2.15 Элемент «Автор, опубликовавший информацию о выявленной уязвимости» представляет собой информацию об авторе, который обнаружил и опубликовал уязвимость первым.

Примечание — Элемент является необязательным к заполнению. Размещение информации об авторе осуществляется с учетом [2].

5.2.16 Элемент «Способ (правило) обнаружения уязвимости» представляет собой формализованное правило определения уязвимости. Способ (правило) обнаружения уязвимости позволяет при помощи специальной процедуры проводить проверку наличия уязвимости.

Пример — Описание уязвимости в части элемента «Способ (правило) обнаружения уязвимости» на языке описания OVAL:

```
AND Software section
  Criterion: Windows XP is installed
    registry_test (oval:org.mitre.oval:tst:2838): check_existence = at_least_one_exists,
    check = at least one
```

registry_object (oval:org.mitre.oval:obj:419): hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Microsoft\Windows NT\CurrentVersion
name: CurrentVersion
registry_state (oval:org.mitre.oval:ste:2657):
value: 5.1
OR a vulnerable version of rpcrt4.dll exists on XP
AND 32-bit version of Windows and a vulnerable version of rpcrt4.dll exists
Criterion: 32-Bit version of Windows is installed
registry_test (oval:org.mitre.oval:tst:2748): check_existence = at_least_one_exists,
check = at least one
registry_object (oval:org.mitre.oval:obj:1576): hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Control\Session Manager\Environment
name: PROCESSOR_ARCHITECTURE
registry_state (oval:org.mitre.oval:ste:2569):
value: x86

Примечание — OVAL (Open Vulnerability and Assessment Language) — открытый язык описания уязвимостей и проведения оценок. OVAL детально описывает метод проверки параметров конфигурации для определения наличия уязвимости.

5.2.17 Элемент «Критерии опасности уязвимости» представляет собой совокупность информации о критериях, используемых при оценке степени опасности уязвимости, и о их значениях. Каждый критерий может принимать значения согласно следующей номенклатуре:

- критерий «тип доступа» (локальный, удаленный, другой тип доступа);
- критерий «условия доступа» (управление доступом, другие условия, управление доступом не применяется);
- критерий «требования аутентификации» [однократная аутентификация, использование (многократный ввод) различной аутентификационной информации, аутентификация не требуется];
- критерий «влияние на конфиденциальность» (не оказывает влияния, нарушение конфиденциальности);
- критерий «влияние на целостность» (не оказывает влияния, нарушение целостности);
- критерий «влияние на доступность» (не оказывает влияния, нарушение доступности).

Примечание — Примером описания критериев опасности уязвимости является базовый вектор уязвимости в соответствии с Common Vulnerability Scoring System[1)].

5.2.18 Элемент «Степень опасности уязвимости» представляет собой текстовую информацию, которая может принимать одно из четырех значений: критический, высокий, средний и низкий уровень опасности. Степень опасности определяют в соответствии с отдельной методикой.

Пример — Описание уязвимости в части элемента «Степень опасности уязвимости»: высокий уровень опасности.

5.2.19 Элемент «Возможные меры по устранению уязвимости» включает в себя предложения и рекомендации по устранению выявленных уязвимостей или исключению возможности использования нарушителем выявленных уязвимостей. Предложения и рекомендации должны содержать ссылки на необходимое ПО и (или) описание конфигураций ПО, для которых угрозы безопасности информации, использующие данную уязвимость, не являются актуальными.

Пример — Описание уязвимости в части элемента «Возможные меры по устранению уязвимости»:
Установите соответствующее обновление:
Microsoft Windows NT Server 4.0 Service Pack 6a;
Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6;
Microsoft Windows XP and Microsoft Windows XP Service Pack 1;
Microsoft Windows XP 64-Bit Edition Service Pack 1;
Microsoft Windows XP 64-Bit Edition Version 2003;
Microsoft Windows Server 2003 64-Bit Edition.

5.2.20 Элементы описания уязвимости с прочей информацией представляют собой текстовую информацию, которая позволяет дополнить общую информацию об уязвимости (см. 5.1.5).

Пример — Описание уязвимости в части элемента «Прочая информация»: специальных полномочий (прав доступа) по отношению к ИС нарушителю не требуется.

---

1) Common Vulnerability Scoring System (CVSS) — общая система оценки уязвимости опубликована на официальном сайте сообщества FIRST по адресу URL: gost.e-ecolog.ru

Приложение А
(рекомендуемое)

Форма паспорта уязвимости с примером его заполнения

Таблица А.1 — Форма паспорта уязвимости с примером его заполнения

Элемент описания уязвимости	Пример заполнения описания уязвимости
Наименование уязвимости	Уязвимость, приводящая к переполнению буфера в службе RPC DCOM в операционных системах Microsoft WIndows 4.0/2000/XP/2003 (Vulnerability Windows XP RPCSS DCOM Buffer Overflow)
Идентификатор уязвимости	XXX-2003-0813
Идентификаторы других систем описаний уязвимостей	CVE ID: CVE-2003-0813 Bugtraq ID: 52018 OSVDB ID: 65465 Qualys ID: 90777 Secunia Advisory: SA48183 SecurityTracker Alert ID: 1025250 Nessus Plugin ID: 38099
Краткое описание уязвимости	Уязвимость обнаружена в службе RPC DCOM. Нарушитель может вызвать отказ в обслуживании (аварийное завершение работы системы или перезагрузка), создавая два потока для одного и того же RPC-запроса. По сообщению разработчика, уязвимость может использоваться для выполнения произвольного кода в уязвимой системе. Разработчик оценил, что уязвимость имеет «критический» уровень опасности
Класс уязвимости	Уязвимость кода
Наименование ПО и его версия	RPC DCOM Microsoft WIndows 4.0/2000/XP/2003
Служба (порт), которая(ый) используется для функционирования ПО	RPC 139/tcp
Язык программирования ПО	C++
Тип недостатка	Недостатки, связанные с переполнением буфера памяти
Место возникновения (проявления) уязвимости	Уязвимость в общесистемном (общем) ПО
Идентификатор типа недостатка	CWE-119
Наименование операционной системы и тип аппаратной платформы	Microsoft Windows 4.0/2000/XP/2003 (×32)
Дата выявления уязвимости	10/03/2003
Автор, опубликовавший информацию о выявленной уязвимости	—

Окончание таблицы А.1

Элемент описания уязвимости	Пример заполнения описания уязвимости
Способ (правило) обнаружения уязвимости	**AND** Software section **Criterion:** Windows XP is installed **registry_test** (oval:org.mitre.oval:tst:2838): check_existence = at_least_one_exists, check = at least one registry_object (oval:org.mitre.oval:obj:419): hive: *HKEY_LOCAL_MACHINE* key: *SOFTWARE\Microsoft\Windows NT\CurrentVersion* name: *CurrentVersion* registry_state (oval:org.mitre.oval:ste:2657): value: *5.1* **OR** a vulnerable version of rpcrt4.dll exists on XP **AND** 32-bit version of Windows and a vulnerable version of rpcrt4.dll exists **Criterion:** 32-Bit version of Windows is installed **registry_test** (oval:org.mitre.oval:tst:2748): check_existence = at_least_one_exists, check = at least one registry_object (oval:org.mitre.oval:obj:1576): hive: *HKEY_LOCAL_MACHINE* key: *SYSTEM\CurrentControlSet\Control\Session Manager\Environment* name: *PROCESSOR_ARCHITECTURE* registry_state (oval:org.mitre.oval:ste:2569): value: *x86*
Критерии опасности уязвимости	Например, в соответствии с CVSS - AV:N/AC:L/Au:N/C:C/I:C/A:C
Степень опасности уязвимости	Высокий уровень опасности
Возможные меры по устранению уязвимости	Установите соответствующее обновление: Microsoft Windows NT Server 4.0 Service Pack 6a Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6 Microsoft Windows XP and Microsoft Windows XP Service Pack 1 Microsoft Windows XP 64-Bit Edition Service Pack 1 Microsoft Windows XP 64-Bit Edition Version 2003 Microsoft Windows Server 2003 64-Bit Edition
Прочая информация	Специальных полномочий (прав доступа) по отношению к ИС нарушителю не требуется

Библиография

[1] Федеральный закон Российской Федерации — «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ

[2] Федеральный закон Российской Федерации — «О персональных данных» от 27 июля 2006 г. № 152-ФЗ

УДК 004: 006.354 ОКС 35.020

Ключевые слова: информационная система, программное обеспечение, защита информации, уязвимость, правила описания

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *Е.Е. Кругова*

Сдано в набор 31.10.2018. Подписано в печать 19.11.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,24.
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.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru