ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ГОСТ Р 56546— 2015**

## Защита информации

# УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

## Классификация уязвимостей информационных систем

**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. № 1181-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ПЕРЕИЗДАНИЕ. Ноябрь 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, 2016, 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 Классификация . . . . . 3
Библиография . . . . . 6

## 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 и устранением уязвимостей ИС, при создании и эксплуатации ИС.

В настоящем стандарте принята классификация уязвимостей ИС исходя из области происхождения уязвимостей, типов недостатков ИС и мест возникновения (проявления) уязвимостей ИС.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Защита информации**

# УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

**Классификация уязвимостей информационных систем**

Information protection. Vulnerabilities in information systems.
The classification of vulnerabilities in information systems

**Дата введения — 2016—04—01**

## 1 Область применения

Настоящий стандарт устанавливает классификацию уязвимостей информационных систем (ИС). Настоящий стандарт направлен на совершенствование методического обеспечения определения и описания угроз безопасности информации при проведении работ по защите информации в 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 ИС.

## 2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:
ГОСТ Р 50922 Защита информации. Основные термины и определения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте национального органа Российской Федерации по стандартизации 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 документа с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого документа 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 50922, а также 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].

3.2 **компонент информационной системы:** Часть информационной системы, включающая некоторую совокупность информации и обеспечивающих ее обработку отдельных информационных технологий и технических средств.

**Издание официальное**

3.3 **признак классификации уязвимостей:** Свойство или характеристика уязвимостей, по которым производится классификация.

3.4 **информационная технология [технология обработки (передачи) информации в информационной системе]:** Процесс, метод поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов.

3.5 **конфигурация информационной системы:** Взаимосвязанные структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между компонентами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, а также с полномочиями субъектов доступа к объектам доступа информационной системы.

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

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

3.8 **уязвимость кода:** Уязвимость, появившаяся в процессе разработки программного обеспечения.

3.9 **уязвимость конфигурации:** Уязвимость, появившаяся в процессе задания конфигурации (применения параметров настройки) программного обеспечения и технических средств информационной системы.

3.10 **уязвимость архитектуры:** Уязвимость, появившаяся в процессе проектирования информационной системы.

3.11 **организационная уязвимость:** Уязвимость, появившаяся в связи с отсутствием (или недостатками) организационных мер защиты информации в информационной системе и(или) несоблюдением правил эксплуатации системы защиты информации информационной системы, требований организационно-распорядительных документов по защите информации и(или) несвоевременном выполнении соответствующих действий должностным лицом (работником) или подразделением, ответственным за защиту информации.

3.12 **многофакторная уязвимость:** Уязвимость, появившаяся в результате наличия нескольких недостатков различных типов.

3.13 **язык программирования:** Язык, предназначенный для разработки (представления) программного обеспечения.

3.14 **степень опасности уязвимости:** Мера (сравнительная величина), характеризующая подверженность информационной системы уязвимости и ее влияние на нарушение свойств безопасности информации (конфиденциальность, целостность, доступность).

## 4 Основные положения

4.1 В основе классификации уязвимостей ИС используются следующие классификационные признаки:

- область происхождения уязвимости;
- типы недостатков ИС;
- место возникновения (проявления) уязвимости ИС.

Примечание — В качестве уязвимых компонентов ИС рассматриваются общесистемное (общее), прикладное, специальное программное обеспечение (ПО), технические средства, сетевое (коммуникационное, телекоммуникационное) оборудование, средства защиты информации.

4.2 Помимо классификационных признаков уязвимостей ИС используются поисковые признаки (основные и дополнительные). Поисковые признаки предназначены для организации расширенного поиска в базах данных уязвимостей.

4.3 К основным поисковым признакам уязвимостей ИС относятся следующие:

- наименование операционной системы (ОС) и тип аппаратной платформы;
- наименование ПО и его версия;
- степень опасности уязвимости.

4.4 К дополнительным поисковым признакам уязвимостей ИС относятся следующие:
- язык программирования;
- служба (порт), которая(ый) используется для функционирования ПО.

## 5 Классификация

5.1 Уязвимости ИС по области происхождения подразделяются на следующие классы:
- уязвимости кода;
- уязвимости конфигурации;
- уязвимости архитектуры;
- организационные уязвимости;
- многофакторные уязвимости.

Примечание — В целях выявления и оценки уязвимостей информационных систем могут выделяться подклассы уязвимостей.

5.2 Уязвимости ИС по типам недостатков ИС подразделяются на следующие:
- недостатки, связанные с неправильной настройкой параметров ПО.

Примечание — Неправильная настройка параметров ПО заключается в отсутствии необходимого параметра, присвоении параметру неправильных значений, наличии избыточного числа параметров или неопределенных параметров ПО;

- недостатки, связанные с неполнотой проверки вводимых (входных) данных.

Примечание — Недостаточность проверки вводимых (входных) данных заключается в отсутствии проверки значений, избыточном количестве значений, неопределенности значений вводимых (входных) данных;

- недостатки, связанные с возможностью прослеживания пути доступа к каталогам.

Примечание — Прослеживание пути доступа к каталогам заключается в отслеживании пути доступа к каталогу (по адресной строке/составному имени) и получении доступа к предыдущему/корневому месту хранения данных;

- недостатки, связанные с возможностью перехода по ссылкам.

Примечание — Переход по ссылкам связан с возможностью внедрения нарушителем ссылки на сторонние ресурсы, которые могут содержать вредоносный код. Для файловых систем недостатками являются символьные ссылки и возможности прослеживания по ним нахождения ресурса, доступ к которому ограничен;

- недостатки, связанные с возможностью внедрения команд ОС.

Примечание — Внедрение команд ОС заключается в возможности выполнения пользователем команд ОС (например, просмотра структуры каталогов, копирование, удаление файлов и другие команды);

- недостатки, связанные с межсайтовым скриптингом (выполнением сценариев).

Примечание — Межсайтовый скриптинг обычно распространен в веб-приложениях и позволяет внедрять код в веб-страницы, которые могут просматривать нелегитимные пользователи. Примерами такого кода являются скрипты, выполняющиеся на стороне пользователя;

- недостатки, связанные с внедрением интерпретируемых операторов языков программирования или разметки.

Примечание — Недостатки связаны с внедрением интерпретируемых операторов языков программирования (например, операции выбора, добавления, удаления и другие) или разметки в исходный код веб-приложения;

- недостатки, связанные с внедрением произвольного кода.

Примечание — Недостатки связаны с внедрением произвольного кода и части кода, которые могут приводить к нарушению процесса выполнения операций;

- недостатки, связанные с переполнением буфера памяти.

Примечание — Переполнение буфера возникает в случае, когда ПО осуществляет запись данных за пределами выделенного в памяти буфера. Переполнение буфера обычно возникает из-за неправильной работы с данными, полученными извне, и памятью, при отсутствии защиты со стороны среды программирования и ОС. В результате переполнения буфера могут быть испорчены данные, расположенные следом за буфером или перед ним. Переполнение буфера может вызывать аварийное завершение или зависание ПО. Отдельные виды переполнений буфера (например, переполнение в стековом кадре) позволяют нарушителю выполнить произвольный код от имени ПО и с правами учетной записи, от которой она выполняется;

- недостатки, связанные с неконтролируемой форматной строкой.

Примечание — Форматная строка в языках С/С++ является специальным аргументом функции с динамически изменяемым числом параметров. Ее значение в момент вызова функции определяет фактическое количество и типы параметров функции. Ошибки форматной строки потенциально позволяют нарушителю динамически изменять путь исполнения программы, в ряде случаев — внедрять произвольный код;

- недостатки, связанные с вычислениями.

Примечание — К недостаткам, связанным с вычислениями, относятся следующие:

- некорректный диапазон, когда ПО использует неверное максимальное или минимальное значение, которое отличается от верного на единицу в большую или меньшую сторону;
- ошибка числа со знаком, когда нарушитель может вводить данные, содержащие отрицательное целое число, которые программа преобразует в положительное нецелое число;
- ошибка усечения числа, когда часть числа отсекается (например, вследствие явного или неявного преобразования или иных переходов между типами чисел);
- ошибка индикации порядка байтов в числах, когда в ПО смешивается порядок обработки битов (например, обратный и прямой порядок битов), что приводит к неверному числу в содержимом, имеющем критическое значение для безопасности;
- недостатки, приводящие к утечке/раскрытию информации ограниченного доступа.

Примечание — Утечка информации — преднамеренное или неумышленное разглашение информации ограниченного доступа (например, существуют утечки информации при генерировании ПО сообщения об ошибке, которое содержит сведения ограниченного доступа). Недостатки, приводящие к утечке/раскрытию информации ограниченного доступа, могут возникать вследствие наличия иных ошибок (например, ошибок, связанных с использованием скриптов);

- недостатки, связанные с управлением полномочиями (учетными данными).

Примечание — К недостаткам, связанным с управлением полномочиями (учетными данными) относятся, например, нарушение политики разграничения доступа, отсутствие необходимых ролей пользователей, ошибки при удалении ненужных учетных данных и другие;

- недостатки, связанные с управлением разрешениями, привилегиями и доступом.

Примечание — К недостаткам, связанным с управлением разрешениями, привилегиями и доступом, относятся, например, превышение привилегий и полномочий, необоснованное наличие суперпользователей в системе, нарушение политики разграничения доступа и другие;

- недостатки, связанные с аутентификацией.

Примечание — К недостаткам, связанным с аутентификацией, относятся возможность обхода аутентификации, ошибки логики процесса аутентификации, отсутствие запрета множественных неудачных попыток аутентификации, отсутствие требования аутентификации для выполнения критичных функций;

- недостатки, связанные с криптографическими преобразованиями (недостатки шифрования).

Примечание — К недостаткам, связанным с криптографическими преобразованиями, относятся ошибки хранения информации в незашифрованном виде, ошибки при управлении ключами, использование несертифицированных средств криптографической защиты информации;

- недостатки, связанные с подменой межсайтовых запросов.

Примечание — Подмена межсайтового запроса заключается в том, что используемое ПО не осуществляет или не может осуществить проверку правильности формирования запроса;

- недостатки, приводящие к «состоянию гонки».

Примечание — «Состояние гонки» — ошибка проектирования многопоточной системы или приложения, при которой функционирование системы или приложения зависит от порядка выполнения части кода. «Состояние гонки» является специфической ошибкой, проявляющейся в случайные моменты времени;

- недостатки, связанные с управлением ресурсами.

Примечание — К недостаткам управления ресурсами относятся недостаточность мер освобождения выделенных участков памяти после использования, что приводит к сокращению свободных областей памяти, и отсутствие очистки ресурса и процессов от сведений ограниченного доступа перед повторным использованием и другие;

- иные типы недостатков.

Примечание — По результатам выявления уязвимостей ИС перечень типов недостатков может дополняться.

5.3 Уязвимости ИС по месту возникновения (проявления) подразделяются на следующие:

- уязвимости в общесистемном (общем) ПО.

Примечание — К уязвимостям в общесистемном (общем) ПО относятся уязвимости ОС (уязвимости файловых систем, уязвимости режимов загрузки, уязвимости, связанные с наличием средств разработки и отладки ПО, уязвимости механизмов управления процессами и другие), уязвимости систем управления базами данных [уязвимости серверной и клиентской частей системы управления базами данных, уязвимости специального инструментария, уязвимости исполняемых объектов баз данных (хранимые процедуры, триггеры) и другие], уязвимости иных типов общесистемного (общего) ПО;

- уязвимости в прикладном ПО.

Примечание — К уязвимостям в прикладном ПО относятся уязвимости офисных пакетов программ и иных типов прикладного ПО (наличие средств разработки мобильного кода, недостатки механизмов контроля исполнения мобильного кода, ошибки программирования, наличие функциональных возможностей, способных оказать влияние на средства защиты информации, и другие уязвимости);

- уязвимости в специальном ПО.

Примечание — К уязвимостям в специальном ПО относятся уязвимости ПО, разработанного для решения специфических задач конкретной ИС (ошибки программирования, наличие функциональных возможностей, способных оказать влияние на средства защиты информации, недостатки механизмов разграничения доступа к объектам специального ПО и другие уязвимости);

- уязвимости в технических средствах.

Примечание — К уязвимостям в технических средствах относятся уязвимости ПО технических средств (уязвимости микропрограмм в постоянных запоминающих устройствах, уязвимости микропрограмм в программируемых логических интегральных схемах, уязвимости базовой системы ввода-вывода, уязвимости ПО контроллеров управления, интерфейсов управления и другие уязвимости), иные уязвимости технических средств;

- уязвимости в портативных технических средствах.

Примечание — К уязвимостям в портативных технических средствах относятся уязвимости ОС мобильных (портативных) устройств, уязвимости приложений для получения с мобильного устройства доступа к Интернет-сервисам, уязвимости интерфейсов беспроводного доступа, иные уязвимости портативных технических средств;

- уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании.

Примечание — К уязвимостям в сетевом (коммуникационном, телекоммуникационном) оборудовании относятся уязвимости маршрутизаторов, коммутаторов, концентраторов, мультиплексоров, мостов и телекоммуникационного оборудования иных типов (уязвимости протоколов и сетевых сервисов, уязвимости средств и протоколов управления телекоммуникационным оборудованием, недостатки механизмов управления потоками информации, недостатки механизмов разграничения доступа к функциям управления телекоммуникационным оборудованием, другие уязвимости);

- уязвимости в средствах защиты информации.

Примечание — К уязвимостям в средствах защиты информации относятся уязвимости в средствах управления доступом, средствах идентификации и аутентификации, средствах контроля целостности, средствах доверенной загрузки, средствах антивирусной защиты, системах обнаружения вторжений, средствах межсетевого экранирования, средствах управления потоками информации, средствах ограничения программной среды, средствах стирания информации и контроля удаления информации, средствах защиты каналов передачи информации, уязвимости в иных средствах защиты информации (ошибки программирования, недостатки, связанные с возможностью обхода, отключения, преодоления функций безопасности, другие уязвимости).

## Библиография

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

УДК 004: 006.354 ОКС 35.020

Ключевые слова: информационная система, программное обеспечение, защита информации, уязвимость, недостаток, классификация, угроза безопасности

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *А.А. Ворониной*

Сдано в набор 01.11.2018. Подписано в печать 12.11.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,12.

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