ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58142— 2018

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045

Часть 1

Использование доступных источников для идентификации потенциальных уязвимостей

(ISO/IEC TR 20004:2015, NEQ)

Издание официальное

Москва
Стандартинформ
2018

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 24 мая 2018 г. № 273-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта ISO/IEC TR 20004:2015 «Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ИСО/МЭК 15408 и ИСО/МЭК 18045» (ISO/IEC TR 20004:2015 «Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

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 (www.gost.ru)

Содержание

Введение

Настоящий стандарт входит в комплекс стандартов, устанавливающих детализацию анализа уязвимостей программного обеспечения в части использования доступных источников для идентификации потенциальных уязвимостей и тестирования проникновения.

Настоящий стандарт уточняет и детализирует действия оценщика (испытательной лаборатории), изложенные в ГОСТ Р ИСО/МЭК 18045, выполняемые при анализе уязвимостей. Стандарт предназначен для совместного использования или в дополнение к ГОСТ Р ИСО/МЭК 18045. Уточнение, детализация и руководства, представленные в настоящем стандарте, не предназначены для выполнения всех требований, предъявляемых семейством AVA_VAN ГОСТ Р ИСО/МЭК 18045, и не ограничивают деятельность, осуществляемую оценщиком, но обеспечивают согласованность посредством детализации минимальных базовых действий оценки выполнения требований семейства AVA_VAN.

Настоящий стандарт распространяется на деятельность оценщиков (испытательных лабораторий), использующих ГОСТ Р ИСО/МЭК 18045, экспертов органов по сертификации, проверяющих выполнение шагов оценивания, а также заявителей на сертификацию, разработчиков средств защиты информации и программного обеспечения и другие группы пользователей, участвующих в процессе оценки средств защиты информации и программного обеспечения по требованиям безопасности информации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045

Часть 1

Использование доступных источников для идентификации потенциальных уязвимостей

Information technology. Security techniques. Refining software vulnerability analysis under GOST R ISO/IEC 15408 and GOST R ISO/IEC 18045. Part 1. Using of available information for identification of potential vulnerabilities

Дата введения — 2018—11—01

1 Область применения

Настоящий стандарт уточняет действия оценщика, определенные семейством доверия AVA_VAN ГОСТ Р ИСО/МЭК 18045, и представляет детализированное руководство по идентификации актуальных потенциальных уязвимостей при проведении оценки объекта оценки в соответствии с ГОСТ Р ИСО/МЭК 15408. В настоящем стандарте используется классификация уязвимостей в соответствии с ГОСТ Р 56546 и описание уязвимостей в соответствии с ГОСТ Р 56545.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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 18045 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий

ГОСТ Р 56545 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей

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

ГОСТ Р 58143—2018 Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения

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 документа 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

Издание официальное

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 **верифицировать:** Провести строгую детальную проверку с независимым определением ее достаточности.

Примечание — См. также термин «подтвердить». Термин «верифицировать» имеет более глубокий смысл. Он используется в контексте действий оценщика, когда требуются независимые усилия оценщика.

3.2 **подтвердить:** Декларировать, что что-то детально проверено с независимым определением достаточности.

Примечание — Требуемый уровень строгости зависит от типа рассматриваемого предмета. Данный термин применим только к действиям оценщика.

3.3 **делать заключение:** Подтвердить некоторое заключение, основанное на независимом анализе для достижения этого заключения.

Примечание — Использование данного термина подразумевает выполнение действительно независимого анализа, обычно в условиях отсутствия какого бы то ни было предшествующего анализа. Термин «делать заключение» отличается от терминов «подтвердить» или «верифицировать», которые предполагают необходимость проверки ранее выполненного анализа.

3.4 **выбор:** Выделение одного или нескольких пунктов из перечня в компоненте требований.

3.5 **объект оценки:** Совокупность программного, программно-аппаратного и/или аппаратного обеспечения, сопровождаемая руководствами.

3.6 **потенциал нападения:** Мера усилий, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя.

3.7 **шаблон атаки:** Способ (модель) использования уязвимости для реализации компьютерной атаки.

3.8 **уязвимость:** Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации.

3.9 **недостаток:** Характеристика или свойство объекта оценки, которое при определенных условиях может способствовать внесению уязвимости в объект оценки.

3.10 **обнаруженные потенциальные уязвимости:** Потенциально уязвимые места объекта оценки, идентифицированные оценщиком при выполнении видов деятельности по оценке, которые могли бы быть использованы для нарушения функциональных требований безопасности.

3.11 **пригодная для использования уязвимость:** Уязвимое место объекта оценки, которое может быть использовано для нарушения функциональных требований безопасности в среде функционирования объекта оценки.

3.12 **потенциальная уязвимость:** Предполагаемый, но не подтвержденный недостаток объекта оценки.

Примечание — Предположение основывают на теоретически допустимой схеме нападения с целью нарушения функциональных требований безопасности.

3.13 **остаточная уязвимость:** Уязвимое место объекта оценки, которое не может быть использовано в среде функционирования объекта оценки, но которое может быть использовано для нарушения функциональных требований безопасности нарушителем с более высоким потенциалом нападения, чем предполагается в среде функционирования объекта оценки.

3.14 **профиль защиты:** Независимое от реализации изложение потребностей в обеспечении безопасности для некоторого типа объекта оценки.

3.15 **задание по безопасности:** Зависимое от реализации изложение потребностей в обеспечении безопасности для конкретного идентифицированного объекта оценки.

4 Обозначения и сокращения

В настоящем стандарте применены следующие обозначения:
ЗБ — задание по безопасности;
ИТ — информационная технология;
ОО — объект оценки;
ТДБ — требование доверия к безопасности;
ТОО — технический отчет по оценке;
ФТБ — функциональное требование безопасности.

5 Общие положения

Подраздел 15.1 ГОСТ Р ИСО/МЭК 15408-3 определяет «уязвимости, возникающие при разработке», как уязвимости, внесенные в ходе процесса разработки ОО, связанные с возможностью преодоления некоторых его свойств. В том же подразделе ГОСТ Р ИСО/МЭК 15408-3 определяется, что оценка уязвимостей, возникающих при разработке, охвачена семейством доверия «Анализ уязвимостей» (AVA_VAN). В соответствии с ГОСТ Р ИСО/МЭК 15408-3 ожидается, что данный анализ определит, могут ли идентифицированные потенциальные уязвимости нарушить выполнение ФТБ; при анализе учитывается угроза того, что нарушитель может выполнять поиск недостатков [как идентифицированных потенциальных уязвимостей] (ГОСТ Р ИСО/МЭК 15408-3, пункт 15.2.1).

Компоненты семейства доверия AVA_VAN ранжированы следующим образом:

- AVA_VAN.1 «Обзор уязвимостей» (ГОСТ Р ИСО/МЭК 15408-3, пункт 15.2.3);
- AVA_VAN.2 «Анализ уязвимостей» (ГОСТ Р ИСО/МЭК 15408-3, пункт 15.2.4);
- AVA_VAN.3 «Фокусированный анализ уязвимостей» (ГОСТ Р ИСО/МЭК 15408-3, пункт 15.2.5);
- AVA_VAN.4 «Методический анализ уязвимостей» (ГОСТ Р ИСО/МЭК 15408-3, пункт 15.2.6);
- AVA_VAN.5 «Усиленный методический анализ» (ГОСТ Р ИСО/МЭК 15408-3, пункт 15.2.7).

Компонент AVA_VAN.1 — младший по иерархии компонент в семействе доверия AVA_VAN, компонент AVA_VAN.5 — старший.

Текущая редакция ГОСТ Р ИСО/МЭК 15408 не предъявляет требований к заявителю (разработчику, производителю) по проведению анализа уязвимостей.

«AVA_VAN.4 Методический анализ уязвимостей

...

Элементы действий заявителя (разработчика, производителя)

AVA_VAN.4.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления документированной информации (свидетельств)

AVA_VAN.4.1C ОО должен быть пригоден для тестирования.

...»

Для обеспечения преемственности требований и сохранения принятой технологии сертификации в профилях защиты, утвержденных ФСТЭК России, требования по проведению анализа уязвимостей заявителем (разработчиком, производителем) определяются путем выполнения уточнения над соответствующими компонентами ТДБ из семейства AVA_VAN:

«AVA_VAN.4 Методический анализ уязвимостей

...

Элементы действий заявителя (разработчика, производителя)

AVA_VAN.X.1D Заявитель (разработчик, производитель) должен **выполнить анализ уязвимостей ОО**.

Элементы содержания и представления документированной информации (свидетельств)

AVA_VAN.X.1C **Документация анализа уязвимостей должна:**

- содержать результаты анализа, выполненного для поиска способов, которыми потенциально может быть нарушена реализация ФТБ;

- идентифицировать проанализированные предполагаемые уязвимости;

- демонстрировать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде функционирования ОО.

...».

Детализация проверки указанных требований приводится в настоящем стандарте в рамках выполнения действий AVA_VAN.X.1E в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045.

Кроме того, в настоящем стандарте приводится детализация действий AVA_VAN.X.2E в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045 по поиску и идентификации потенциальных уязвимостей на основе доступных источников для анализа:

- в AVA_VAN.1.2E (ГОСТ Р ИСО/МЭК 15408-3, подпункт 15.2.3.4.2);
- в AVA_VAN.2.2E (ГОСТ Р ИСО/МЭК 15408-3, подпункт 15.2.4.4.2);
- в AVA_VAN.3.2E (ГОСТ Р ИСО/МЭК 15408-3, подпункт 15.2.5.4.2);
- в AVA_VAN.4.2E (ГОСТ Р ИСО/МЭК 15408-3, подпункт 15.2.6.4.2);
- в AVA_VAN.5.2E (ГОСТ Р ИСО/МЭК 15408-3, подпункт 15.2.7.4.2).

ГОСТ Р ИСО/МЭК 18045 устанавливает конкретные шаги оценивания, связанные с действием «Идентификации потенциальной уязвимости в доступных источниках» (в подпунктах 14.2.1.5, 14.2.2.5, 14.2.3.5, 14.2.4.5) следующим образом.

AVA_VAN.1-3, AVA_VAN.2-3, AVA_VAN.3-3, AVA_VAN.4-3

Оценщик (испытательная лаборатория) должен исследовать доступные источники информации, чтобы идентифицировать потенциальные уязвимости ОО.

Возможность простого доступа нарушителя к информации, которая помогает идентифицировать уязвимости и облегчить нападение, существенно увеличивает потенциал нападения данного нарушителя. Доступность в сети Интернет информации об уязвимостях и современных средствах реализации атак позволяет с высокой степенью вероятности предположить, что данная информация будет использоваться при попытках идентифицировать потенциальные уязвимости в ОО и использовать их. Современные поисковые системы делают такую информацию легкодоступной оценщику, и заключение о стойкости ОО к нападениям с использованием опубликованных потенциальных уязвимостей, а также к хорошо известным типовым нападениям (атакам) может быть дано в терминах «эффективность-стоимость».

Поиск доступной информации необходимо сосредоточить на источниках, относящихся к конкретному продукту ИТ, на основании которого получен ОО. При определении требуемой широты поиска необходимо рассмотреть следующие факторы: тип ОО, опыт оценщика для проверки данного типа ОО, ожидаемый потенциал нападения и уровень доступных свидетельств по классу ADV «Разработка».

AVA_VAN.1-4, AVA_VAN.2-5, AVA_VAN.3-5, AVA_VAN.4-5

Оценщик должен привести в ТОО идентифицированные потенциальные уязвимости, которые являются предметом тестирования и применимы к данному ОО в среде его функционирования.

Может быть установлено, что не требуется дальнейшее рассмотрение конкретной потенциальной уязвимости, если оценщик идентифицирует, что использующихся в среде функционирования мер защиты, относящихся или не относящихся к ИТ, достаточно для предотвращения возможности использования потенциальной уязвимости в данной среде функционирования.

Оценщик фиксирует любые причины исключения потенциальных уязвимостей из дальнейшего рассмотрения, если он сделает заключение, что потенциальная уязвимость не применима в среде функционирования. В ином случае оценщик фиксирует выявленную потенциальную уязвимость для дальнейшего рассмотрения.

Оценщик должен привести в ТОО перечень потенциальных уязвимостей, применимых к ОО в его среде функционирования, который может использоваться в качестве исходных данных для действий по тестированию проникновения.

Как указано в пункте 14.2.5 ГОСТ Р ИСО/МЭК 18045, ГОСТ Р ИСО/МЭК 18045 не определяет шаги оценивания для компонента AVA_VAN.5.

Краткое изложение содержания действия оценщика «Идентификация потенциальной уязвимости в доступных источниках» приведено на рисунке 1.

Детализация действий, предусмотренных компонентами ТДБ семейства AVA_VAN, связанных с тестированием проникновения, в части поиска способов и методов тестирования приведена в ГОСТ Р 58143—2018.

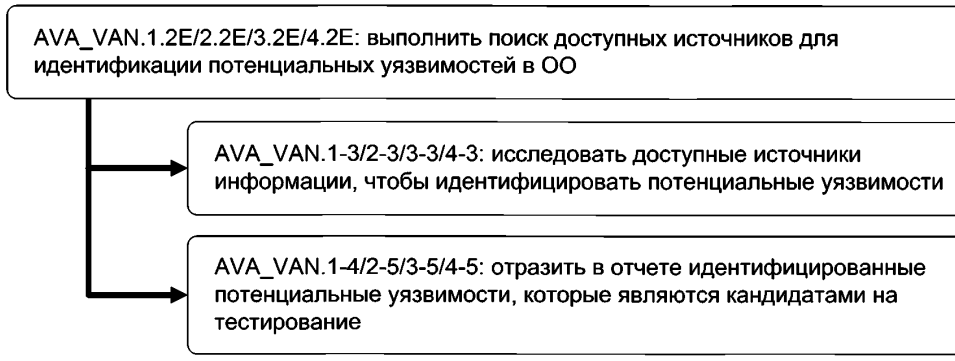

Рисунок 1 — Описание действия оценщика «Идентификация потенциальной уязвимости в доступных источниках»

6 Действия по оценке уязвимостей

ГОСТ Р ИСО/МЭК 18045 определяет шаги оценивания и документирования для определения актуальных потенциальных уязвимостей:

6.1 Подвид деятельности по оценке (AVA_VAN.1)

Действие AVA_VAN.1.2E

AVA_VAN.1.2E Оценщик должен выполнить поиск информации в доступных источниках, чтобы идентифицировать потенциальные уязвимости в ОО.

Шаг оценивания AVA_VAN.1-3

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен исследовать доступные источники информации, чтобы идентифицировать потенциальные уязвимости в ОО.

Оценщик исследует доступные источники информации в целях идентификации возможных потенциальных уязвимостей в ОО. Существует множество доступных источников информации, которые необходимо рассмотреть оценщику. Например, списки рассылки и форумы безопасности в сети Интернет, в которых публикуется информация об известных уязвимостях конкретных ИТ.

Оценщик не должен ограничиваться рассмотрением доступной информации из вышеупомянутых источников: необходимо рассмотреть любую другую доступную информацию, имеющую отношение к уязвимостям ОО.

В процессе исследования предоставленных заявителем (разработчиком, производителем) свидетельств, оценщиком должна использоваться доступная информация для дальнейшего поиска потенциальных уязвимостей. Оценщику также необходимо особо рассмотреть всю доступную информацию, имеющую отношение к идентифицированным уязвимостям ОО.

Поиск доступной информации необходимо сосредоточить на тех источниках, которые относятся к конкретному продукту ИТ, принятому в качестве ОО. При определении требуемой области этого поиска необходимо рассмотреть следующие факторы: тип ОО, опыт оценщика для данного типа ОО, ожидаемый потенциал нападения и уровень (степень детализации) доступных свидетельств по классу ADV «Разработка».

Процесс идентификации является итерационным (повторяющимся), т. е. идентификация одной потенциальной уязвимости может привести к идентификации иных потенциальных недостатков, которые требуют дальнейшего исследования.

Оценщик приводит в отчете (сообщении) информацию о действиях, предпринятых им для идентификации потенциальных уязвимостей на основе доступной информации. Однако, осуществляя поиск уязвимостей на основе доступной информации, оценщик может не иметь возможности до начала анализа изложить шаги, которые он предпримет при идентификации потенциальных уязвимостей, поскольку подход к анализу может изменяться в зависимости от информации, выявленной в процессе поиска.

Оценщик приводит в отчете свидетельства, исследованные в процессе поиска потенциальных уязвимостей.

Детализация в соответствии с ИСО/МЭК ТО 20004

Оценщик должен провести анализ информации об уязвимостях, полученной:

а) из банка данных угроз безопасности информации (базы данных уязвимостей);

б) от уполномоченных федеральных органов исполнительной власти;

в) из иных источников (например, CVE, CWE).

Банк данных угроз безопасности информации размещен на официальном сайте ФСТЭК России (www.bdu.fstec.ru) и содержит информацию об уязвимостях различных классов (типов), выявленных в программном обеспечении (включая программное обеспечение средств защиты информации), применяемом в информационных системах.

Примечание — В ЗБ при изложении угроз безопасности информации, которым противостоит продукт ИТ, описываются используемые уязвимости на уровне классов (типов) уязвимостей. Оценщик, используя Банк данных угроз безопасности информации ФСТЭК России, осуществляет фильтрацию уязвимостей по наименованию (или типу программного обеспечения) и классу (типу) уязвимостей из ЗБ. Полученные описания уязвимостей используются оценщиком для дальнейшего анализа.

Уполномоченные федеральные органы исполнительной власти могут предоставить в испытательную лабораторию описание уязвимостей, характерных для типа изделия ИТ, заявленного на сертификацию, с учетом предполагаемой среды функционирования. Информацию об уязвимостях уполномоченный федеральный орган исполнительной власти может предоставить при выпуске решения на сертификацию или в процессе проведения сертификационных испытаний.

В качестве иных источников информации об уязвимостях могут выступать имеющиеся доступные источники (такие, например, как CVE, CWE).

Примечание — Общий перечень уязвимостей и рисков (Common Vulnerabilities and Exposures, CVE) является справочником общеизвестных уязвимостей программного обеспечения. Перечень CVE является широко применяемым индустриальным стандартом описания уязвимостей и рисков. Основу справочника составляют CVE-идентификаторы, которые обеспечивают основу баз данных уязвимостей инструментальных средств и сервисов, используемых для оценки защищенности систем.

Кроме того, существует независимый стандартизованный перечень потенциальных уязвимостей (недостатков) программного обеспечения в виде Общего перечня недостатков (Common Vulnerabilities and Exposures, CWE). Общий перечень недостатков CWE является разрабатываемым международным сообществом формализованным перечнем общих недостатков программного обеспечения. Перечень CWE обеспечивает наличие общего языка для описания недостатков программного обеспечения, стандартных единиц измерения инструментальных средств оценки защищенности, выявляющих эти уязвимости, основу для идентификации, уменьшения и предотвращения уязвимостей. Содержание перечня CWE пополняется для формирования стандартизированного механизма идентификации, сбора, совершенствования и распространения перечня недостатков программного обеспечения среди сообщества разработчиков.

Оценщик должен задокументировать идентифицированные при анализе уязвимости. Описание идентифицированных уязвимостей рекомендуется выполнять с учетом ГОСТ Р 56545 и ГОСТ Р 56546.

Для выполнения данного шага оценивания оценщик должен определить перечень уязвимостей, полученный из банка данных угроз безопасности информации (базы данных уязвимостей) и идентифицировать уязвимости для проведения анализа. Оценщик должен определить (в случае применимости) те уязвимости, которые он получил от уполномоченных федеральных органов исполнительной власти. Оценщик должен определить те уязвимости, которые он идентифицировал для проведения анализа из иных источников (например, CVE, CWE).

Примечание — При поиске информации оценщик должен учитывать, что ОО может быть продуктом ИТ, частью продукта ИТ, набором продуктов ИТ. Таким образом должен быть осуществлен сбор информации о продукте ИТ (продуктах ИТ), который (которые) частично или полностью охвачен (охвачены) объектом оценки. Более подробно принципы соотнесения понятий «объект оценки» и «продукт ИТ» приведены в ГОСТ Р ИСО/МЭК 15408-1.

Шаг оценивания AVA_VAN.1-4

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен привести в ТОО идентифицированные потенциальные уязвимости, которые подлежат тестированию и применимы к данному ОО в среде его функционирования.

Может быть установлено, что не требуется дальнейшее рассмотрение конкретной потенциальной уязвимости, если оценщик идентифицирует, что использующихся в среде функционирования мер за-

щиты, относящихся или не относящихся к ИТ, достаточно для предотвращения возможности использования потенциальной уязвимости в данной среде функционирования. Например, ограничение физического доступа к ОО и предоставление такого доступа только уполномоченным пользователям может значительно снизить вероятность использования потенциальной уязвимости для несанкционированного вмешательства в процесс функционирования ОО.

Оценщик фиксирует любые причины исключения потенциальных уязвимостей из дальнейшего рассмотрения, если он делает заключение, что потенциальная уязвимость не применима в среде функционирования. Иначе оценщик фиксирует выявленную потенциальную уязвимость как уязвимость, предназначенную для дальнейшего рассмотрения.

Оценщик должен привести в ТОО перечень потенциальных уязвимостей, применимых к ОО в его среде функционирования, который может использоваться в качестве исходных данных для проведения тестирования проникновения.

Детализация в соответствии с ИСО/МЭК ТО 20004

Целью использования большого количества источников информации об уязвимостях является эксплуатация уязвимостей, которые могут быть актуальными для различных условий функционирования ОО. Для того чтобы ограничить множество потенциальных уязвимостей, используемых при оценке по требованиям безопасности информации, исходное множество потенциально актуальных уязвимостей должно быть отсортировано методом исключения уязвимостей, которые не являются актуальными из-за применяемых в среде функционирования ОО мер безопасности, предотвращающих наличие потенциальных уязвимостей в данной среде функционирования. Оценщик должен задокументировать обоснование каждого исключения уязвимости.

Используя указанные выше действия для сортировки уязвимости, уточняются шаги оценивания AVA_VAN.1-3 в части рассмотрения уязвимостей для ОО и формируется актуальный перечень уязвимостей.

Детализация шагов AVA_VAN.1-4 — AVA_VAN.1-10 — в соответствии с ГОСТ Р 58143—2018. С учетом выполнения шагов AVA_VAN.1-4 - AVA_VAN.1-10 выполняется шаг AVA_VAN.1-11. Шаг оценивания AVA_VAN.1-11

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен привести в ТОО информацию обо всех пригодных для использования уязвимостях и остаточных уязвимостях, детализируя для каждой:

а) источник уязвимости (например, стала известна при выполнении действий ГОСТ Р ИСО/МЭК 18045, известна оценщику, прочитана в публикации);

б) связанные с уязвимостью невыполненные ФТБ;

в) описание уязвимости;

г) пригодна ли уязвимость для использования в среде функционирования (т. е. пригодна ли уязвимость для использования или является остаточной уязвимостью);

д) количество времени, уровень компетентности, уровень знания ОО, необходимый уровень доступа к ОО, оборудование, требуемые для использования идентифицированных уязвимостей, а также соответствующие значения, полученные на основе таблиц В.2 и В.3 приложения В.4 ГОСТ Р ИСО/МЭК 18045.

Детализация в соответствии с ИСО/МЭК ТО 20004

В дополнение к информации, изложенной в подпункте 14.2.1.6.7 ГОСТ Р ИСО/МЭК 18045, оценщик должен включить в ТОО следующую подробную информацию обо всех пригодных для использования уязвимостях и остаточных уязвимостях:

а) соответствующие идентификаторы уязвимостей (идентификатор, наименование, краткое описание);

б) идентификаторы шаблонов атак (идентификатор, наименование), используемые для доказательства подтверждения уязвимости.

Примечание — Оценщик (а также заявитель сертификации при разработке свидетельств) при определении количества времени, уровня компетентности, уровня знания ОО, уровня возможности доступа, оборудования, требуемых для использования идентифицированных уязвимостей, должен стремиться к сокращению субъективизма.

Могут существовать иные (по отношению к ГОСТ Р ИСО/МЭК 18045) методики определения потенциала нарушителя, необходимого для использования уязвимостей, результаты применения которых (при наличии соответствующих исходных данных) можно сравнивать с результатами по ГОСТ Р ИСО/МЭК 18045 для повышения объективности оценки.

Например, может применяться некоторая методика вычисления потенциала нарушителя, базирующаяся на показателях опасности уязвимости, изложенных в «Паспорте уязвимости» в соответствии с ГОСТ Р 56545.

6.2 Подвиды деятельности по оценке (AVA_VAN.2 — AVA_VAN.5)

Действие AVA_VAN.X.1E

AVA_VAN.X.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

Проверка выполнения требования AVA_VAN.X.1C

AVA_VAN.X.1C Документация анализа уязвимостей должна:

содержать результаты анализа, выполненного для поиска способов, которыми потенциально может быть нарушена реализация ФТБ;

идентифицировать проанализированные предполагаемые уязвимости;

демонстрировать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде функционирования ОО.

В соответствии с ГОСТ Р ИСО/МЭК 18045

Шаги оценивания не определены.

Детализация в соответствии с ИСО/МЭК ТО 20004

Шаг оценивания AVA_VAN.X-1

Оценщик должен исследовать материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, вся ли информация рассмотрена при поиске уязвимостей.

Оценщик должен убедиться, что разработчик провел анализ информации об уязвимостях, полученной из банка данных угроз безопасности информации (базы данных уязвимостей) и идентифицировал уязвимости для проведения анализа.

Оценщик должен определить (в случае применимости) те уязвимости, информацию о которых разработчик получил от уполномоченных федеральных органов исполнительной власти.

Оценщик должен определить те уязвимости, которые разработчик идентифицировал для проведения анализа из иных источников (например, CVE, CWE).

Для определения актуальных потенциальных уязвимостей оценщик должен **самостоятельно** изучить доступные источники для идентификации потенциальных уязвимостей.

Для выполнения данного шага оценивания оценщик должен провести исследование материалов анализа уязвимостей, выполненного разработчиком, а также самостоятельно определить перечень уязвимостей, полученный из банка данных угроз безопасности информации (базы данных уязвимостей) и идентифицировать уязвимости для проведения анализа.

Оценщик должен определить (в случае применимости) те уязвимости, информацию о которых он получил от уполномоченных федеральных органов исполнительной власти.

Оценщик должен определить те уязвимости, которые он идентифицировал для проведения анализа из иных источников (например, CVE, CWE).

Замечания по применению

По факту прохождения ОО сертификации, а также в процессе проведения сертификационных испытаний уполномоченный федеральный орган исполнительной власти может потребовать проверку отсутствия в ОО дополнительных уязвимостей, описание которых отсутствует в базе данных уязвимостей. При этом уполномоченный федеральный орган исполнительной власти предоставляет в испытательную лабораторию описание данных уязвимостей.

Шаг оценивания AVA_VAN.X-2

Оценщик должен исследовать материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, описана ли каждая идентифицированная уязвимость и дано ли обоснование того, почему она является непригодной для использования в предопределенной среде ОО.

Для выполнения данного шага оценивания оценщик должен провести исследование материалов анализа уязвимостей, выполненного разработчиком, и удостовериться в непригодности уязвимостей для использования.

Уязвимость считается непригодной для использования, если выполняется одно или более из следующих условий:

- уязвимость является пригодной для использования только нарушителями, обладающими высоким потенциалом нападения;

- в ЗБ либо не утверждается о противостоянии соответствующей угрозе, либо не утверждается о следовании политике безопасности организации, которая может быть нарушена.

Действие AVA_VAN.X.2E

Оценщик должен выполнить поиск информации в доступных источниках, чтобы идентифицировать потенциальные уязвимости в ОО.

Шаг оценивания AVA_VAN.X-3

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен исследовать доступные источники информации, чтобы идентифицировать потенциальные уязвимости в ОО.

Оценщик исследует доступные источники информации, в целях идентификации возможных потенциальных уязвимостей в ОО. Существует множество доступных источников информации, которые необходимо рассмотреть оценщику. Например, доступные источники информации в сети Интернет, включая:

а) специальные публикации (журналы, книги);

б) результаты исследований.

Оценщик не должен ограничиваться рассмотрением доступной информации из вышеупомянутых источников, необходимо рассмотреть любую другую доступную информацию, имеющую отношение к уязвимостям ОО.

В процессе исследования предоставленных разработчиком свидетельств оценщиком должна использоваться доступная информация для дальнейшего поиска потенциальных уязвимостей. Оценщику также необходимо особо рассмотреть всю доступную информацию, имеющую отношение к идентифицированным уязвимостям ОО.

Поиск доступной информации необходимо сосредоточить на тех источниках, которые относятся к конкретному продукту ИТ, принятому в качестве ОО. При определении требуемой области этого поиска необходимо рассмотреть следующие факторы: тип ОО, опыт оценщика для данного типа ОО, ожидаемый потенциал нападения и уровень (степень детализации) доступных свидетельств по классу ADV «Разработка».

Процесс идентификации является итерационным (повторяющимся), т. е. идентификация одной потенциальной уязвимости может привести к идентификации иных потенциальных недостатков, которые требуют дальнейшего исследования.

Оценщик приводит в отчете (сообщении) информацию о действиях, предпринятых им для идентификации потенциальных уязвимостей на основе доступной информации. Однако, осуществляя поиск уязвимостей на основе доступной информации, оценщик может не иметь возможности до начала анализа изложить шаги, которые он предпримет при идентификации потенциальных уязвимостей, поскольку подход к анализу может изменяться в зависимости от информации, выявленной в процессе поиска.

Оценщик приводит в отчете свидетельства, исследованные в процессе поиска потенциальных уязвимостей. Выбор свидетельств может осуществляться на основании идентифицированных оценщиком потенциальных недостатков безопасности, связанных с возможностью получения нарушителем конкретных свидетельств, или согласно другому обоснованию, предложенному оценщиком.

Детализация в соответствии с ИСО/МЭК ТО 20004

Оценщик должен идентифицировать потенциальные уязвимости в ОО, которые на его взгляд не были определены разработчиком ОО, для этого оценщик должен провести анализ информации об уязвимостях, полученной:

а) из банка данных угроз безопасности информации (базы данных уязвимостей);

б) от уполномоченных федеральных органов исполнительной власти;

в) из иных источников (например, CVE, CWE).

Оценщик должен задокументировать идентифицированные при анализе уязвимости. Описание идентифицированных уязвимостей рекомендуется выполнять с учетом ГОСТ Р 56545 и ГОСТ Р 56546.

Шаг оценивания AVA_VAN.X-5

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен привести в ТОО идентифицированные потенциальные уязвимости, которые подлежат тестированию и применимы к данному ОО в среде его функционирования.

Может быть установлено, что не требуется дальнейшее рассмотрение конкретной потенциальной уязвимости, если оценщик идентифицирует, что использующихся в среде функционирования мер защиты, относящихся или не относящихся к ИТ, достаточно для предотвращения возможности использования потенциальной уязвимости в данной среде функционирования. Например, ограничение физического доступа к ОО и предоставление такого доступа только уполномоченным пользователям может

значительно снизить вероятность использования потенциальной уязвимости для несанкционированного вмешательства в процесс функционирования ОО.

Оценщик фиксирует любые причины исключения потенциальных уязвимостей из дальнейшего рассмотрения, если он делает заключение, что потенциальная уязвимость не применима в среде функционирования. Иначе оценщик фиксирует выявленную потенциальную уязвимость как уязвимость, предназначенную для дальнейшего рассмотрения.

Оценщик должен привести в ТОО перечень потенциальных уязвимостей, применимых к ОО в его среде функционирования, который может использоваться в качестве исходных данных для проведения тестирования проникновения.

Детализация в соответствии с ИСО/МЭК ТО 20004

Целью использования большого количества источников информации об уязвимостях является эксплуатация уязвимостей, которые могут быть актуальными для различных условий функционирования ОО. Для того чтобы ограничить множество потенциальных уязвимостей, используемых при оценке по требованиям безопасности информации, исходное множество потенциально актуальных уязвимостей должно быть отсортировано методом исключения уязвимостей, которые не являются актуальными из-за применяемых в среде функционирования ОО мер безопасности, предотвращающих наличие потенциальных уязвимостей в данной среде функционирования. Оценщик должен задокументировать обоснование каждого исключения уязвимости.

Используя указанные выше действия для сортировки уязвимости, уточняются шаги оценивания AVA_VAN.X-3 в части рассмотрения уязвимостей для ОО и формируется актуальный перечень уязвимостей.

Детализация шагов AVA_VAN.X-5 — AVA_VAN.X-11 в соответствии с ГОСТ Р 58143—2018. С учетом выполнения шагов AVA_VAN.X-5 - AVA_VAN.X-11 выполняется шаг AVA_VAN.X-12.

Шаг оценивания AVA_VAN.X-12

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен привести в ТОО информацию обо всех пригодных для использования уязвимостях и остаточных уязвимостях, детализируя для каждой:

а) источник уязвимости (например, стала известна при выполнении действий ГОСТ Р ИСО/МЭК 18045, известна оценщику, прочитана в публикации);

б) связанные с уязвимостью невыполненные ФТБ;

в) описание уязвимости;

г) пригодна ли уязвимость для использования в среде функционирования (т. е. пригодна ли уязвимость для использования или является остаточной уязвимостью);

д) количество времени, уровень компетентности, уровень знания ОО, необходимый уровень доступа к ОО, оборудование, требуемые для использования идентифицированных уязвимостей, а также соответствующие значения, полученные на основе таблиц В.2 и В.3 приложения В.4 ГОСТ Р ИСО/МЭК 18045.

Детализация в соответствии с ИСО/МЭК ТО 20004

В дополнение к информации, изложенной в подпунктах 14.2.2.7.7, 14.2.3.7.7 и 14.2.4.7.7 ГОСТ Р ИСО/МЭК 18045, оценщик должен включить в ТОО следующую подробную информацию обо всех пригодных для использования уязвимостях и остаточных уязвимостях:

а) соответствующие идентификаторы уязвимостей (идентификатор, наименование, краткое описание);

б) идентификаторы шаблонов атак (идентификатор, наименование), используемые для доказательства подтверждения уязвимости.

УДК 004.622:006.354 ОКС 35.020

Ключевые слова: информационная технология, объект оценки, анализ уязвимостей, недостаток, программное обеспечение

БЗ 10—2016/31

Редактор *А.А. Кабанов*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 25.05.2018. Подписано в печать 29.05.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,68.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 123001 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru