ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(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. № 274-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 содержит детализацию рекомендаций по планированию, выполнению и составлению отчетности тестирования проникновения объекта оценки на базе требований «Анализ уязвимостей» из ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Настоящий стандарт содержит руководство и процедуры тестирования проникновения, позволяющие получить согласованные воспроизводимые результаты при идентификации, оценке и описании уязвимостей.

Настоящий стандарт распространяется на деятельность оценщиков (испытательных лабораторий), использующих ГОСТ Р ИСО/МЭК 15408 и 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.

Настоящий стандарт может использоваться следующим образом:

- оценщиками — при разработке тестов проникновения (как часть действий по оценке, требуемых в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045;
- разработчиками — при разработке своих тестов проникновения (как часть процесса разработки объекта оценки);
- заявителями сертификации — для понимания того, какие действия по тестированию будут выполняться в ходе оценки;
- разработчиками профилей защиты/заданий по безопасности — для четкого определения потенциалов нападения и шаблонов атак.

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 2

Тестирование проникновения

Information technology. Security techniques. Refining software vulnerability analysis under GOST R ISO/IEC 15408 and GOST R ISO/IEC 18045. Part 2. Penetration testing

Дата введения — 2018—11—01

1 Область применения

Настоящий стандарт содержит руководство по планированию, выполнению и составлению отчетности тестирования проникновения объекта оценки на базе требований «Анализ уязвимостей» из ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. В частности, данный стандарт уточняет действия по тестированию проникновения, предусмотренные компонентами требований доверия к безопасности из семейства доверия AVA_VAN «Анализ уязвимостей» и описанные в ГОСТ Р ИСО/МЭК 18045, и обеспечивает более полное руководство по их выполнению. Настоящий стандарт включает процесс-ориентированное руководство и процедуры тестирования, необходимые для получения согласованных воспроизводимых результатов при идентификации, оценке и описании уязвимостей.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 15408-3—2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности

ГОСТ Р ИСО/МЭК 18045—2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий

ГОСТ Р 56545—2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей

ГОСТ Р 56546—2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем

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

Издание официальное

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 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 58142, а также следующий термин с соответствующим определением:

3.1 **фаззинг:** Тестирование, использующее как корректные, так и случайные (включая некорректные) входные данные для проверки, устанавливающей, обрабатываются ли должным образом интерфейсом случайные входные данные или возникает ошибочная ситуация (ошибочное условие), указывающая (указывающее) на наличие недостатков при разработке (ошибки исходного кода) или при эксплуатации.

4 Обозначения и сокращения

В настоящем стандарте применены следующие обозначения:

ИФБО — интерфейс ФБО;

ОО — объект оценки;

ТДБ — требование доверия к безопасности;

ТОО — технический отчет по оценке;

ФБО — функциональные возможности безопасности ОО;

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.

Детализация действий, предусмотренных компонентами ТДБ семейства AVA_VAN, связанных с идентификацией потенциальных уязвимостей, приведена в ГОСТ Р 58142.

В настоящем стандарте приводится детализация действий оценщика в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045 при тестировании проникновения.

Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы сделать заключение, что ОО является стойким к нападениям, выполняемым нарушителем, обладающим:

- базовым потенциалом нападения в AVA_VAN.1.3.E (ГОСТ Р ИСО/МЭК 15408-3, подпункт 15.2.3.4.3);
- базовым потенциалом нападения в AVA_VAN.2.4.E (ГОСТ Р ИСО/МЭК 15408-3, подпункт 15.2.4.4.4);
- усиленным базовым потенциалом нападения в AVA_VAN.3.4.E (ГОСТ Р ИСО/МЭК 15408-3, подпункт 15.2.5.4.4);
- умеренным потенциалом нападения в AVA_VAN.4.4.E (ГОСТ Р ИСО/МЭК 15408-3, подпункт 15.2.6.4.4);
- высоким потенциалом нападения в AVA_VAN.5.4.E (ГОСТ Р ИСО/МЭК 15408-3, подпункт 15.2.7.4.4).

ГОСТ Р ИСО/МЭК 18045 устанавливает конкретные шаги оценивания, связанные с действием «Тестирование проникновения» (в подпунктах 14.2.1.6, 14.2.2.7, 14.2.3.7, 14.2.4.7) следующим образом.

AVA_VAN.1-5, AVA_VAN.2-6, AVA_VAN.3-6, AVA_VAN.4-6

Оценщик должен разработать тесты проникновения, основываясь на проведенном независимом поиске потенциальных уязвимостей.

Тесты проникновения предназначены для того, чтобы оценщик мог сделать заключение о восприимчивости ОО, находящегося в своей среде функционирования, к потенциальным уязвимостям, идентифицированным в процессе поиска по источникам доступной информации. При этом текущая информация об известных потенциальных уязвимостях, предоставленная оценщику третьей стороной (например, органом по сертификации), рассматривается оценщиком наряду с обнаруженными в результате выполнения других действий по оценке потенциальными уязвимостями.

Не предполагается тестирование оценщиком на предмет наличия потенциальных уязвимостей помимо тех, для использования которых требуется:

- базовый потенциал нападения (в случае AVA_VAN.1-5);
- базовый потенциал нападения (в случае AVA_VAN.2-6);
- усиленный базовый потенциал нападения (в случае AVA_VAN.3-6); или
- умеренный потенциал нападения (в случае AVA_VAN.4-6).

AVA_VAN.1-6, AVA_VAN.2-7, AVA_VAN.3-7, AVA_VAN.4-7

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на перечне потенциальных уязвимостей; детализация этой документации должна быть достаточна для обеспечения воспроизводимости тестов.

Для каждой потенциальной уязвимости оценщик должен определить наиболее подходящий способ тестирования ОО. При этом должны быть рассмотрены:

а) ИФБО или другой интерфейс ОО, который будет использован для инициирования выполнения ФБО и наблюдения за результатом;

б) начальные условия, которые будут необходимы для выполнения тестирования (т. е. какие-либо конкретные необходимые объекты или субъекты и их атрибуты безопасности);

в) специальное оборудование для тестирования, которое потребуется либо для инициирования ИФБО, либо для наблюдения за ИФБО;

г) возможность использования при анализе уязвимости результатов ранее выполненных тестов (без их повторного проведения), когда результаты нападения являются очевидными.

AVA_VAN.1-7, AVA_VAN.2-8, AVA_VAN.3-8, AVA_VAN.4-8

Оценщик должен провести тестирование проникновения.

Оценщик использует документацию для тестов проникновения, подготовленную на шаге оценивания:

- AVA_VAN.1-5 (в случае AVA_VAN.1-7);
- AVA_VAN.2-6 (в случае AVA_VAN.2-8);
- AVA_VAN.3-6 (в случае AVA_VAN.3-8); или
- AVA_VAN.4-6 (в случае AVA_VAN.4-8)

как основу для выполнения тестов проникновения по отношению к ОО, но это не препятствует оценщику выполнить дополнительные специальные тесты проникновения.

AVA_VAN.1-8, AVA_VAN.2-9, AVA_VAN.3-9, AVA_VAN.4-9

Оценщик должен зафиксировать фактические результаты выполнения тестов проникновения.

AVA_VAN.1-9, AVA_VAN.2-10, AVA_VAN.3-10, AVA_VAN.4-10

Оценщик должен привести в ТОО информацию о результатах деятельности по тестированию проникновения, кратко изложив подход к тестированию, тестируемую конфигурацию, глубину и результаты тестирования.

AVA_VAN.1-10 и AVA_VAN.2-11

Оценщик должен исследовать результаты всего тестирования проникновения и выводы по всему анализу уязвимостей, чтобы сделать заключение, является ли ОО, находящийся в своей среде функционирования, стойким к действиям нарушителя, обладающего базовым потенциалом нападения.

Если результаты показывают, что ОО, находящийся в своей среде функционирования, имеет уязвимости, пригодные для использования нарушителем, обладающим меньшим, чем усиленный базовый, потенциалом нападения, то по этому действию (а именно, AVA_VAN.1.3E или AVA_VAN.2.4E) оценщиком делается отрицательное заключение.

Руководство, представленное в приложении В.4 ГОСТ Р ИСО/МЭК 18045, необходимо использовать для определения потенциала нападения, требуемого для использования конкретной уязвимости, и установления возможности использования уязвимости в предполагаемой среде функционирования.

AVA_VAN.3-11

Оценщик должен исследовать результаты всего тестирования проникновения и выводы по всему анализу уязвимостей, чтобы сделать заключение, является ли ОО, находящийся в своей среде функционирования, стойким к действиям нарушителя, обладающего усиленным базовым потенциалом нападения.

Если результаты показывают, что ОО, находящийся в своей среде функционирования, имеет уязвимости, пригодные для использования нарушителем, обладающим меньшим, чем умеренный, потенциалом нападения, то по этому действию (а именно, AVA_VAN.3.4E) делается отрицательное заключение.

Руководство, представленное в приложении В.4 ГОСТ Р ИСО/МЭК 18045, необходимо использовать для определения потенциала нападения, требуемого для использования конкретной уязвимости, и установления возможности использования уязвимости в предполагаемой среде функционирования.

AVA_VAN.4-11

Оценщик должен исследовать результаты всего тестирования проникновения и выводы по всему анализу уязвимостей, чтобы сделать заключение, является ли ОО, находящийся в своей среде функционирования, стойким к действиям нарушителя, обладающего умеренным потенциалом нападения.

Если результаты показывают, что ОО, находящийся в своей среде функционирования, имеет уязвимости, пригодные для использования нарушителем, обладающим меньшим, чем высокий потенциалом нападения, то по этому действию оценщика (AVA_VAN.4.4E) делается отрицательное заключение.

Руководство, представленное в приложении В.4 ГОСТ Р ИСО/МЭК 18045, необходимо использовать для определения потенциала нападения, требуемого для использования конкретной уязвимости, и установления возможности использования уязвимости в предполагаемой среде функционирования.

AVA_VAN.1-11, AVA_VAN.2-12, AVA_VAN.3-12, AVA_VAN.4-12

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

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

б) связанные с ней невыполненные ФТБ;

в) описание;

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

д) количество времени, уровень компетентности, уровень знаний ОО, уровень возможности доступа, оборудование, требуемые для использования идентифицированных уязвимостей, а также соответствующие значения, полученные на основе таблиц В.2 и В.3 в приложении В.4 ИСО/МЭК 18045.

Примечание — Как указано в подпункте 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 «Тестирование проникновения приведено на рисунке 1.

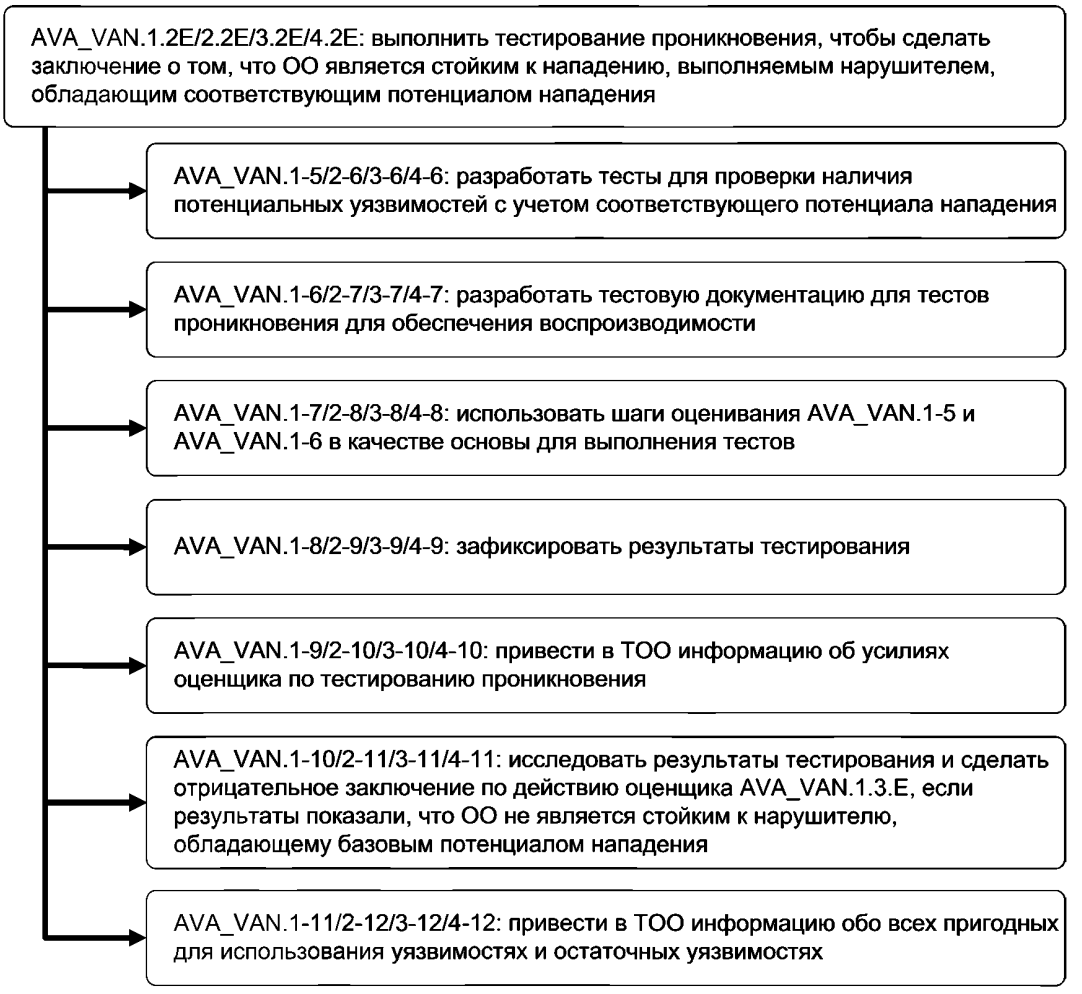

Рисунок 1 — Описание действия оценщика «Тестирование проникновения»

6 Стадии тестирования проникновения

Выделяются следующие стадии проведения тестирования проникновения:
- планирование тестирования проникновения;
- разработка тестов проникновения;
- проведение тестирования проникновения;
- разработка отчетности по результатам тестирования проникновения.

6.1 Планирование тестирования проникновения

Планирование тестирования проникновения включает:
- определение профиля нападения;
- идентификацию потенциальных уязвимостей;
- описание возможностей и мотивации нарушителя;
- идентификацию шаблонов атак.

6.1.1 Определение профиля нападения

Определение профиля нападения является первым этапом при тестировании проникновения. На этом этапе необходимо:

- определить исследуемую архитектуру;
- определить архитектуру безопасности (состав и структуру средств защиты информации), включая доверенные области;
- идентифицировать предназначенные для тестирования информационные ресурсы (активы, являющиеся целью атаки) с обоснованием включения или исключения их из области проведения тестирования;
- идентифицировать интерфейс ФБО, доступный потенциальному нарушителю;
- классифицировать интерфейсы, способы их использования и степень доступности потенциальному нарушителю;
- идентифицировать параметры, которые нарушитель может определить с использованием интерфейса.

На данном этапе обеспечивается сбор информации для определения профиля атаки.

6.1.2 Идентификация потенциальных уязвимостей:

- изучение доступных источников для идентификации потенциальных уязвимостей и поиск уязвимостей, характерных для ОО;
- фаззинг;
- документирование потенциальных уязвимостей.

Примечание — Предполагается использование (разработка и поддержание) национального источника информации о направлениях (векторах) атак. При этом зарубежные источники информации могут использоваться, как вспомогательные.

В соответствии с ГОСТ Р ИСО/МЭК 18045 определяются лица, ответственные за реализацию действия «Идентификация потенциальной уязвимости».

Фаззинг эффективно используется для нахождения ошибок программной реализации, а также для идентификации потенциальных уязвимостей программного обеспечения. Несмотря на то, что фаззинг непосредственно не является проверкой тестирования проникновения, его результаты предназначены для определения потенциальных уязвимостей.

Фаззинг направлен на выявление ошибок в программном обеспечении посредством ввода случайных (в том числе и некорректных) данных и обнаружения возможных отказов. Фаззинг является, как правило, автоматизированным или полуавтоматическим процессом, который включает неоднократное формирование и ввод данных в ОО для последующей обработки. Оценщик должен определить, действительно ли фаззинг вызывает отказ программного обеспечения. Преимущество фаззинга с точки зрения безопасности состоит в возможности обнаружения ранее неизвестных уязвимостей, которые сложно или невозможно обнаружить при прочих условиях.

Варианты тестирования, основанные на неправильном умышленном или неумышленном использовании внешних объектов или зависимых от ОО компонентов, должны моделировать сбои программного обеспечения для выявления ошибок безопасности и потенциальных уязвимостей. Оценщик должен также моделировать нетипичные действия, которые направлены на разрушение предположений, созданных при разработке программного обеспечения относительно собственного состояния и состояния среды функционирования.

Примечание — Результат ошибки может быть неочевидным, последствия ошибки может быть сложно обнаружить вне ОО. Результат может быть представлен в виде сообщения об ошибке или полного нарушения функционирования ОО.

Примечание — Для воспроизведения результатов тестирования необходимо зарегистрировать условия тестирования, при которых происходит сбой или другое нетипичное поведение, а также необходимо зарегистрировать состояние ОО во время сбоя или другого результирующего действия в ходе тестирования.

Потенциальные уязвимости, идентифицированные посредством фаззинга, могут использоваться в качестве целей атаки с использованием метода тестирования проникновения. Результаты фаззинга должны быть классифицированы и ранжированы с целью упорядочивания дальнейшего порядка тестирования.

Данный пункт описывает процедуру проведения фаззинга, ориентированного на проникновение, и процедуру использования результатов для идентификации потенциальных уязвимостей. Также описывается процедура использования результатов фаззинга для уточнения шаблонов атак.

Потенциальные уязвимости (недостатки) должны быть задокументированы. Документация должна включать характеристику следующих элементов:

- исследуемая система(ы) или компонент(ы) ОО;
- уязвимый интерфейс ФБО в рамках оцененной конфигурации ОО;
- типы уязвимостей (недостатков);
- описание уязвимостей (недостатков);
- потенциальное воздействие эксплуатации уязвимостей (недостатков).

6.1.3 Описание возможностей и мотивации нарушителя

При описании фактических (требуемых) знаний нарушителя предполагается, что оценщик должен определить, какой объем информации должен иметь соответствующий потенциальный нарушитель об ОО, его взаимодействии с внешними объектами и способах взаимодействия компонентов ОО друг с другом. Объем знаний, который нарушитель имеет об ОО, может изменяться от начального уровня осведомленности до полного, включая владение информацией об исходном коде, или некоторый промежуточный уровень осведомленности.

Например, для ОО, являющегося собственной разработкой, менее вероятно знание нарушителем его исходного кода. Тем не менее, в случае с доступным программным обеспечением нарушитель может обладать полным объемом информации об исходном коде, но не обязательно знанием о среде его функционирования.

Для описания требуемого уровня доступа нарушителя оценщик должен определить, какая модель доступа к ОО и его среде функционирования является типичной для легитимных пользователей и возможна для использования нарушителем.

При описании фактической мотивации нарушителя оценщик должен определить, намерен ли нарушитель нарушить свойства конфиденциальности, чтобы поставить под угрозу целостность и/или затронуть доступность целевого программного обеспечения при оценке.

Раскрытие действий нарушителя возможно путем моделирования действий нарушителя и определения способов реализации шаблонов атак.

6.1.4 Идентификация шаблонов атак

Идентификация шаблонов атак основана на наблюдениях за успешными реализациями атак на различные автоматизированные системы.

Оценщик должен рассмотреть информацию относительно признаков соответствующего вида атаки, идентифицированных потенциальных уязвимостей (недостатков), возможностей нарушителя и его мотивации, соответствующего уровня доступа нарушителя и его намерений с целью идентифицировать актуальные шаблоны атак для конкретного теста проникновения.

ИСО/МЭК ТО 20004 определяет механизм идентификации применимых шаблонов атак.

6.2 Разработка тестов проникновения

Разработка тестов проникновения включает:

- разработку тестов проникновения, используя идентифицированные шаблоны атак;
- разработку тестов проникновения с использованием метода гипотез (предположений) о недостатках;
- документирование тестов проникновения.

Используя результаты определения шаблонов атак и идентификации соответствующих уязвимостей и недостатков, оценщик разрабатывает план тестирования проникновения, определяя соответствующий шаблон атаки по отношению к виду атаки, порядок выполнения атаки, определение условий проведения атаки, порядок тестирования и определение ожидаемых результатов, которые позволяют оценщику решить, было ли проникновение успешным, не успешным или требует дальнейшего исследования.

Разработка тестов проникновения с использованием идентифицированных шаблонов атак заключается в описании порядка получения специфичных примеров реализации атак из шаблонов атак.

Разработка тестов проникновения с использованием метода гипотез (предположений) о недостатках заключается в моделировании действий нарушителя и определения способов реализации и использования шаблонов атак.

Документирование тестов проникновения заключается в регистрации данных о тесте проникновения, порядке тестирования и ожидаемых результатах тестирования.

Документирование может выполняться как для отдельного тестирования компонента ОО, так и для комплексного тестирования ОО в целом.

6.3 Проведение тестирования проникновения

Проведение тестирования проникновения включает:

- выполнение тестов проникновения;
- анализ результатов тестов;
- уточнение тестов с учетом полученных результатов;
- документирование результатов тестирования проникновения.

При выполнении тестов проникновения оценщик должен осуществлять их в тестовой среде, соответствующей условиям эксплуатации ОО (моделированная, виртуальная, эксплуатационная);

При выполнении тестов проникновения оценщик должен использовать инструментальные средства.

Тестовая последовательность действий, выполняемых при тестировании проникновения, должна обеспечивать возможность повторного воспроизведения теста и получения результата, который был получен оценщиком.

Анализ результатов тестов заключается в сравнении полученных результатов с ожидаемыми результатами, а также в проверках:

- было ли проникновение успешным, не успешным или невыполнимым;
- имеется ли наличие других непредсказуемых результатов.

Результаты должны быть задокументированы и должны отражать соответствие спецификации ОО.

При необходимости, используя результаты тестирования, тест проникновения может быть уточнен и воспроизведен. Уточнение может включать:

- тестирование одного и того же интерфейса с различными параметрами для получения доступа к ОО выбранным при тестировании способом;
- тестирование других или дополнительных интерфейсов для получения доступа к ОО выбранным при тестировании способом;
- тестирование одних и тех же интерфейсов для проверки с использованием метода гипотез (предположений) о недостатках.

Все результаты тестирования, а также действия оценщика должны быть задокументированы.

6.4 Разработка отчетности по результатам тестирования проникновения

Отчетность по результатам тестирования проникновения должна содержать:

- условия проведения тестирования проникновения;
- обобщенные результаты тестирования проникновения;
- детализацию результатов тестирования проникновения по отношению к каждой потенциальной уязвимости.

Обобщенные результаты тестирования проникновения должны содержать:

- описание модели профиля нападения;
- покрытие ОО тестами проникновения;
- изложение идентифицированных уязвимостей с указанием их опасности.

Покрытие ОО тестами проникновения включает описание:

- сопоставления гипотез (предположений) о недостатках и выполненных шаблонов атак;
- сопоставления гипотез (предположений) о недостатках и шаблонов атак, которые подтверждают идентифицированные недостатки;
- сопоставления гипотез (предположений) о недостатках и шаблонов атак, которые были признаны нереализуемыми по отношению к рассматриваемому ОО;
- сопоставления гипотез (предположений) о недостатках и шаблонов атак, по которым не получилось вынести решение по результатам выполненного тестирования проникновения.

Детализация результатов по отношению к каждой потенциальной уязвимости включает:

- изложение результатов тестирования;
- описание подтвержденных уязвимостей;

Примечание — Описание подтвержденных уязвимостей рекомендуется выполнять с учетом ГОСТ Р 56545 и ГОСТ Р 56546.

- описание использования шаблонов атак, включая алгоритм выполнения шаблона (и использованные вариации);

- оценку опасности уязвимости;
- рекомендации для каждого недостатка (уязвимости).

Рекомендации для каждого недостатка (уязвимости) могут включать:

- описание недостатков (уязвимостей) и назначенного времени их устранения, предшествующего сертификации ОО;
- описание недостатков (уязвимостей), которые необходимо обсудить с разработчиком и органом по сертификации;
- описание недостатков (уязвимостей), которые не могут быть использованы в предполагаемой среде эксплуатации ОО.

7 Действия по тестированию проникновения

ГОСТ Р ИСО/МЭК 18045 определяет шаги оценивания при тестировании проникновения:

7.1 Подвид деятельности по оценке (AVA_VAN.1)

Действие AVA_VAN.1.3E

Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы сделать заключение, что ОО является стойким к нападениям, выполняемым нарушителем.

Шаг оценивания AVA_VAN.1-5

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен разработать тесты проникновения, основываясь на проведенном независимом поиске потенциальных уязвимостей.

Назначением тестирования проникновения является предоставление оценщику возможности сделать заключение о восприимчивости ОО, находящегося в своей среде функционирования, к потенциальным уязвимостям, идентифицированным в процессе поиска уязвимостей на основе доступной информации. При этом текущая информация об известных потенциальных уязвимостях, предоставленная оценщику третьей стороной (например, органом по сертификации), рассматривается оценщиком наряду с обнаруженными в результате выполнения других действий по оценке потенциальными уязвимостями.

В ряде случаев целесообразным является выполнение тестирования каждой конкретной потенциальной уязвимости отдельным набором тестов.

Не предполагается тестирование оценщиком потенциальных уязвимостей (в том числе известных из доступных источников), для использования которых требуется потенциал нападения отличный от Базового. Однако в некоторых случаях необходимо выполнить тестирование возможности использования уязвимости прежде, чем может быть определена пригодность ОО к использованию. Если в результате исследований оценщик обнаруживает некоторую потенциальную уязвимость, для использования которой требуется потенциал нападения выше Базового, такая уязвимость приводится в ТОО как остаточная уязвимость.

Детализация в соответствии с ИСО/МЭК ТО 20004

Тесты проникновения разрабатываются с учетом идентифицированных уязвимостей.

Тесты проникновения разрабатываются на основе шаблонов атак. В качестве перечня шаблонов атак могут использоваться доступные национальные источники или, как вспомогательные, зарубежные источники (например, CAPEC).

Примечание — Общий перечень шаблонов атак и их классификация (Common Attack Pattern Enumeration and Classification, CAPEC) является доступным источником и предназначен для более объективного описания потенциала атаки в отношении актуальных потенциальных уязвимостей и описания актуальных тестов проникновения.

Общий перечень шаблонов атак и их классификация разрабатывается международным сообществом и содержит перечень шаблонов атак на программное обеспечение. Шаблоны атак являются описанием общих способов эксплуатации программного обеспечения, которое отражает действие с точки зрения нарушителя. Шаблоны атак разработаны на основе детального анализа реальных примеров эксплуатации уязвимостей программного обеспечения.

Содержание шаблонов атак пополняется для формирования стандартизированного механизма идентификации, сбора, совершенствования и распространения перечня шаблонов атак на программное обеспечение среди сообщества разработчиков.

Оценщик должен разработать собственные атаки (разработанные не по шаблонам атак), которые могут учитывать условия применения и среду функционирования ОО.

Шаг оценивания AVA_VAN.1-6

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на перечне потенциальных уязвимостей, с детализацией, достаточной для обеспечения воспроизводимости тестов. Тестовая документация должна включать:

а) идентификацию тестируемой потенциальной уязвимости ОО;

б) инструкции по подключению и настройке всего требуемого тестового оборудования в соответствии с требованиями к проведению конкретного теста проникновения;

в) инструкции по установке всех предварительных (начальных) условий выполнения теста проникновения;

г) инструкции по инициированию тестируемых ФБО;

д) инструкции по наблюдению режима выполнения ФБО;

е) описание всех ожидаемых результатов и содержания анализа, который необходимо выполнить в отношении наблюдаемого режима выполнения ФБО для сравнения с ожидаемыми результатами;

ж) инструкции по завершению теста и установке требуемого послетестового состояния ОО.

Оценщик осуществляет подготовку к тестированию проникновения, руководствуясь перечнем потенциальных уязвимостей, идентифицированных при поиске уязвимостей на основе доступной информации.

Не предполагается, что оценщик сделает заключение о возможности использования потенциальных уязвимостей для реализации атак, использование которых требует наличие потенциала нападения, отличного от Базового потенциала нападения. Однако в ходе исследования оценщиком может быть обнаружена потенциальная уязвимость, использование которой возможно только нарушителем с потенциалом нападения, превышающим Базовый потенциал нападения. Такие уязвимости приводятся в ТОО как остаточные уязвимости.

Для каждой потенциальной уязвимости оценщик должен определить наиболее подходящий способ тестирования ОО. При этом должны быть рассмотрены:

а) ИФБО или другой интерфейс ОО, который будет использован для инициирования выполнения ФБО и наблюдения за результатом выполнения;

б) начальные условия, необходимые для выполнения тестирования (т. е. какие-либо конкретные необходимые объекты или субъекты и их атрибуты безопасности);

в) специальное оборудование для тестирования, которое потребуется либо для инициирования ИФБО, либо для наблюдения за ИФБО (при необходимости);

г) возможность использования при анализе уязвимости результатов ранее выполненных тестов (без их повторного проведения), если результаты нападения являются очевидными.

Оценщиком при необходимости может быть выполнено тестирование проникновения с использованием ряда наборов тестов (тестовых ситуаций), где каждый набор тестов будет использоваться для тестирования конкретной потенциальной уязвимости.

Целью определения установленного уровня детализации потенциальных уязвимостей в тестовой документации является предоставление возможности другому оценщику воспроизвести тесты и получить эквивалентный результат.

Детализация в соответствии с ИСО/МЭК ТО 20004

Оценщику необходимо разработать, уточнить и задокументировать набор тестовых случаев для осуществления в полном объеме анализа уязвимостей для актуальных недостатков и тестов проникновения ОО на основе выполнения актуальных шаблонов атак, направленных на эксплуатацию соответствующих актуальных недостатков. Каждый тестовый случай будет использоваться для проверки конкретного варианта, состоящего из конкретного шаблона атаки, направленного на эксплуатацию конкретного потенциального недостатка.

В дополнение к информации, определенной в подпункте 14.2.1.6.2 ГОСТ Р ИСО/МЭК 18045, тестовая документация должна включать следующую информацию для каждого тестового случая:

а) идентификацию недостатка, наличие которого тестируется в ОО;

б) идентификацию шаблона атаки, которая будет выполняться во время испытаний;

в) подробное описание выполнения атаки в данном тестовом случае.

Перечень факторов, определенных в подпункте 14.2.1.6.2 ГОСТ Р ИСО/МЭК 18045, который используется оценщиком при определении наиболее подходящего способа тестирования ОО, должен применяться в контексте множества актуальных шаблонов атак.

Шаг оценивания AVA_VAN.1-7

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен провести тестирование проникновения.

Оценщик использует документацию тестов проникновения, подготовленную на шаге оценивания AVA_VAN.1-5, как основу для выполнения тестов проникновения по отношению к ОО, при этом оценщик может выполнить и дополнительные специальные тесты проникновения. При необходимости оценщик может осуществить дополнительные специальные тесты, основываясь на текущих результатах проводимого им тестирования проникновения, информация о которых должна быть внесена оценщиком в документацию тестов проникновения по факту их выполнения. Указанные тесты могут использоваться с целью исследования непредвиденных результатов, а также потенциальных уязвимостей, предположения о которых сделаны при планировании тестирования проникновения и существование которых оценщик должен подтвердить или опровергнуть.

Не предполагается тестирование оценщиком потенциальных уязвимостей (в том числе известных из доступных источников), для использования которых требуется потенциал нападения отличный от Базового. Однако в некоторых случаях необходимо выполнить тестирование возможности использования уязвимости прежде, чем может быть определена пригодность ОО к использованию. Если в результате исследований оценщик обнаруживает некоторую потенциальную уязвимость, для использования которой требуется потенциал нападения выше Базового, такая уязвимость приводится в ТОО как остаточная уязвимость.

Детализация в соответствии с ИСО/МЭК ТО 20004

Оценщик должен использовать автоматизированные средства, позволяющие моделировать атаки с учетом идентифицированных уязвимостей, на основе выбранных шаблонов атак, а также используя собственные тесты на проникновения.

При тестировании проникновения ОО должен находиться в той среде функционирования, для которой он разрабатывался изначально.

Шаг оценивания AVA_VAN.1-8

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен зафиксировать фактические результаты выполнения тестов проникновения. Некоторые особенности фактических результатов выполнения тестов могут отличаться от ожидаемых (например, поля времени и даты в записи аудита), однако общий результат тестирования проникновения должен соответствовать ожидаемому результату. Необходимо исследовать любые непредвиденные результаты выполнения тестов. Влияние полученных результатов на оценку проведенного тестирования проникновения необходимо установить и логически обосновать.

Детализация в соответствии с ИСО/МЭК ТО 20004

Шаг не детализируется.

Шаг оценивания AVA_VAN.1-9

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен привести в ТОО информацию о действиях по тестированию проникновения, кратко изложив подход к тестированию, тестируемую конфигурацию, глубину и результаты тестирования.

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику изложить общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Целью предоставления указанной информации является формирование краткого обзора действий оценщика по тестированию проникновения. Информация, приводимая оценщиком в ТОО относительно выполненного тестирования проникновения, не должна быть точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов проникновения, но должна обеспечивать достаточность данных, необходимых другим оценщикам и сотрудникам органов по сертификации для понимания выбранного подхода к тестированию проникновения, объема выполненного тестирования проникновения, тестируемых конфигураций ОО и общих результатов действий по тестированию проникновения.

Информация о действиях оценщика по тестированию проникновения, представленная в соответствующем разделе ТОО, включает:

а) описание тестируемых конфигураций ОО (конкретные конфигурации ОО, которые подвергались тестированию проникновения);

б) перечень ИФБО, применительно к которым осуществлялось тестирование проникновения (краткий перечень ИФБО и других интерфейсов ОО, на которых было сосредоточено тестирование проникновения);

в) заключение по данному подвиду деятельности (общий вывод по результатам тестирования проникновения).

Приведенный перечень не является исчерпывающим и определяет базовые сведения о выполненном оценщиком тестировании проникновения, которые необходимо привести в ТОО.

Детализация в соответствии с ИСО/МЭК ТО 20004

Оценщику необходимо определить условия использования специальных тестов проникновения, не разработанных на основе множества актуальных шаблонов атак, в случаях, требующих исследования непредвиденных результатов или потенциальных уязвимостей, о существовании которых оценщик сделал предположение на стадии планирования тестирования.

Шаг оценивания AVA_VAN.1-10

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен исследовать результаты всех действий по тестированию проникновения и выводы по анализу всех уязвимостей, чтобы сделать заключение, является ли ОО, находящийся в своей среде функционирования, стойким к нарушителю, обладающему Базовым потенциалом нападения.

Если результаты показывают, что ОО, находящийся в своей среде функционирования, имеет уязвимости, пригодные для использования нарушителем, обладающим потенциалом нападения ниже Усиленного базового, то по этому действию оценщиком выносится отрицательное заключение.

Руководство из приложения В.4 ГОСТ Р ИСО/МЭК 18045 необходимо использовать для вынесения заключения о потенциале нападения, требуемом для использования конкретной уязвимости, и возможности использования этой уязвимости в предполагаемой среде функционирования. Вычисление потенциала нападения для каждого случая может не требоваться, за исключением случаев, когда у оценщика остается сомнение относительно того, может ли уязвимость использоваться нарушителем, обладающим потенциалом нападения меньшим, чем Усиленный базовый.

Детализация в соответствии с ИСО/МЭК ТО 20004

Шаг не детализируется.

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.

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

Действие AVA_VAN.X.4E

Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы сделать заключение, что ОО является стойким к нападениям, выполняемым нарушителем.

Шаг оценивания AVA_VAN.X-6

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен разработать тесты проникновения, основываясь на проведенном независимом поиске потенциальных уязвимостей.

Назначением тестирования проникновения является предоставление оценщику возможности сделать заключение о восприимчивости ОО, находящегося в своей среде функционирования, к потенциальным уязвимостям, идентифицированным в процессе поиска уязвимостей на основе доступной информации. При этом текущая информация об известных потенциальных уязвимостях, предоставленная оценщику третьей стороной (например, органом по сертификации), рассматривается оценщиком наряду с обнаруженными в результате выполнения других действий по оценке потенциальными уязвимостями.

Оценщику необходимо помнить, что при рассмотрении «Описания архитектуры безопасности» для поиска уязвимостей (как детализировано в AVA_VAN.X-4), необходимо выполнить тестирование с целью подтверждения архитектурных свойств безопасности, в связи с чем может потребоваться проведение тестов проникновения, направленных на нарушение свойств безопасности архитектуры. При разработке стратегии тестирования проникновения оценщик обеспечивает покрытие тестами каждой из основных характеристик в «Описании архитектуры безопасности» либо при функциональном тестировании (как рассмотрено в разделе 13 ГОСТ Р ИСО/МЭК 18045), либо при тестировании проникновения, проведенном оценщиком.

В ряде случаев целесообразным является выполнение тестирования каждой конкретной потенциальной уязвимости отдельным набором тестов.

Не предполагается тестирование оценщиком потенциальных уязвимостей (в том числе известных из доступных источников), для использования которых требуется потенциал нападения отличный от Базового. Однако в некоторых случаях необходимо выполнить тестирование возможности использования уязвимости прежде, чем может быть определена пригодность ОО к использованию. Если в результате исследований оценщик обнаруживает некоторую потенциальную уязвимость, для использования которой требуется потенциал нападения выше Базового, такая уязвимость приводится в ТОО как остаточная уязвимость.

Руководство по определению необходимого для использования потенциальной уязвимости потенциала нападения представлено в приложении В.4 ГОСТ Р ИСО/МЭК 18045.

В случаях, когда предполагается, что потенциальные уязвимости могут использовать только нарушители, обладающие усиленным Базовым, Умеренным или Высоким потенциалом нападения, наличие таких уязвимостей не требует вынесения отрицательного заключению по данному действию. Если по результатам анализа уязвимостей указанное предположение подтверждается, эти потенциальные уязвимости не требуется рассматривать далее в качестве исходных данных для тестирования проникновения. Указанные уязвимости приводятся в ТОО как остаточные.

Потенциальным уязвимостям, которые, предположительно, могут использовать нарушители, обладающие Базовым потенциалом нападения, и использование которых приводит к нарушению целей безопасности, присваивается высшая степень опасности. Указанные уязвимости включаются в перечень исходных данных тестирования проникновения как уязвимости ОО, подлежащие непосредственному тестированию.

Детализация в соответствии с ИСО/МЭК ТО 20004

Тесты проникновения разрабатываются с учетом идентифицированных уязвимостях.

Тесты проникновения разрабатываются на основе шаблонов атак. В качестве перечня шаблонов атак могут использоваться доступные источники (например, CAPEC).

Оценщик должен разработать собственные атаки (разработанные не по шаблонам атак), которые могут учитывать условия применения и среду функционирования ОО.

Шаг оценивания AVA_VAN.X-7

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на перечне потенциальных уязвимостей, с детализацией, достаточной для обеспечения воспроизводимости тестов. Тестовая документация должна включать:

а) идентификацию тестируемой потенциальной уязвимости оцениваемого ОО;

б) инструкции по подключению и настройке всего требуемого тестового оборудования в соответствии с требованиями к проведению конкретного теста проникновения;

в) инструкции по установке всех предварительных начальных условий выполнения теста проникновения;

г) инструкции по инициированию тестируемых ФБО;

д) инструкции по наблюдению режима выполнения ФБО;

е) описание всех ожидаемых результатов и содержания анализа, который необходимо выполнить в отношении наблюдаемого режима выполнения ФБО для сравнения с ожидаемыми результатами;

ж) инструкции по завершению теста и установке требуемого послетестового состояния ОО.

Оценщик осуществляет подготовку к тестированию проникновения, руководствуясь перечнем потенциальных уязвимостей, идентифицированных при поиске уязвимостей на основе доступной информации, и результатами анализа свидетельств.

Не предполагается, что оценщик сделает заключение о возможности использования потенциальных уязвимостей для реализации атак, использование которых требует наличие потенциала нападения, отличного от Базового потенциала нападения. Однако в ходе исследования оценщиком может быть обнаружена потенциальная уязвимость, использование которой возможно только нарушителем с потенциалом нападения, превышающим Базовый потенциал нападения. Такие уязвимости приводятся в ТОО как остаточные уязвимости.

Для каждой потенциальной уязвимости оценщик должен определить наиболее подходящий способ тестирования ОО. При этом должны быть рассмотрены:

а) ИФБО или другой интерфейс ОО, который будет использован для инициирования выполнения ФБО и наблюдения за результатом их выполнения (возможно, что оценщику потребуется использование иного интерфейса ОО, помимо ИФБО, для демонстрации свойств ФБО, в частности, приведенных в «Описании архитектуры безопасности» (в соответствии с требованиями семейства ADV_ARC). Необходимо отметить, что, хотя интерфейсы ОО предоставляют средства тестирования свойств ФБО, сами эти интерфейсы не являются предметом тестирования);

б) начальные условия, необходимые для выполнения тестирования (т. е. какие-либо конкретные необходимые объекты или субъекты и их атрибуты безопасности);

в) специальное оборудование для тестирования, которое потребуется либо для инициирования ИФБО, либо для наблюдения за ИФБО (при необходимости);

г) возможность использования при анализе уязвимости результатов ранее выполненных тестов (без их повторного проведения), если результаты нападения являются очевидными.

Оценщиком при необходимости может быть выполнено тестирование проникновения с использованием ряда наборов тестов (тестовых ситуаций), где каждый набор тестов будет использоваться для тестирования конкретной потенциальной уязвимости.

Целью определения установленного уровня детализации потенциальных уязвимостей в тестовой документации является предоставление возможности другому оценщику (например, органу по сертификации) воспроизвести тесты и получить эквивалентный результат.

Детализация в соответствии с ИСО/МЭК ТО 20004

Оценщику необходимо разработать, уточнить и задокументировать набор тестовых случаев для осуществления в полном объеме анализа уязвимостей для актуальных недостатков и тестов проникновения ОО на основе выполнения актуальных шаблонов атак, направленных на эксплуатацию соответствующих актуальных недостатков. Каждый тестовый случай будет использоваться для проверки конкретного варианта, состоящего из конкретного шаблона атаки, направленного на эксплуатацию конкретного потенциального недостатка.

В дополнение к информации, определенной в подпунктах 14.2.2.7.2, 14.2.3.7.2 и 14.2.4.7.2 ГОСТ Р ИСО/МЭК 18045, тестовая документация должна включать следующую информацию для каждого тестового случая:

а) идентификацию недостатка, наличие которого тестируется в ОО;

б) идентификацию шаблона атаки, которая будет выполняться во время испытаний;

в) подробное описание выполнения атаки в данном тестовом случае.

Перечень факторов, определенных в подпунктах 14.2.2.7.2, 14.2.3.7.2 и 14.2.4.7.2 ГОСТ Р ИСО/МЭК 18045, который используется оценщиком при определении наиболее подходящего способа протестировать восприимчивость ОО, должен применяться в контексте множества актуальных шаблонов атак.

Шаг оценивания AVA_VAN.X-8

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен провести тестирование проникновения.

Оценщик использует документацию тестов проникновения, подготовленную на шаге оценивания AVA_VAN.X-6, как основу для выполнения тестов проникновения по отношению к ОО, при этом оценщик может выполнить и дополнительные специальные тесты проникновения. При необходимости оценщик может осуществить дополнительные специальные тесты, основываясь на текущих результатах проводимого им тестирования проникновения, информация о которых должна быть внесена оценщиком в документацию тестов проникновения по факту их выполнения. Указанные тесты могут использоваться с целью исследования непредвиденных результатов, а также потенциальных уязвимостей, предположения о которых сделаны при планировании тестирования проникновения и существование которых оценщик должен подтвердить или опровергнуть.

Если тестирование проникновения показывает, что уязвимость, о которой было сделано предположение, не существует, оценщику необходимо сделать заключение, был ли корректным анализ оценщика, и не являются ли предоставленные для оценки материалы некорректными или неполными.

Не предполагается тестирование оценщиком потенциальных уязвимостей (в том числе известных из доступных источников), для использования которых требуется потенциал нападения отличный от Базового. Однако в некоторых случаях необходимо выполнить тестирование возможности использования уязвимости прежде, чем может быть определена пригодность ОО к использованию. Если в результате исследований оценщик обнаруживает некоторую потенциальную уязвимость, для использования которой требуется потенциал нападения выше Базового, такая уязвимость приводится в ТОО как остаточная уязвимость.

Детализация в соответствии с ИСО/МЭК ТО 20004

Оценщик должен использовать автоматизированные средства, позволяющие моделировать атаки с учетом идентифицированных уязвимостей, на основе выбранных шаблонов атак, а также используя собственные тесты на проникновения.

При тестировании проникновения ОО должен находиться в той среде функционирования, для которой он разрабатывался изначально.

Шаг оценивания AVA_VAN.X-9

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен зафиксировать фактические результаты выполнения тестов проникновения. Некоторые особенности фактических результатов выполнения тестов могут отличаться от ожидаемых (например, поля времени и даты в записи аудита), однако общий результат тестирования проникновения должен соответствовать ожидаемому результату. Необходимо исследовать любые непредвиденные результаты выполнения тестов. Влияние полученных результатов на оценку проведенного тестирования проникновения необходимо установить и логически обосновать.

Детализация в соответствии с ИСО/МЭК ТО 20004

Шаг не детализируется.

Шаг оценивания AVA_VAN.X-10

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен привести в ТОО информацию о действиях по тестированию проникновения, кратко изложив подход к тестированию, тестируемую конфигурацию, глубину и результаты тестирования.

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику изложить общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Целью предоставления указанной информации является формирование краткого обзора действий оценщика по тестированию проникновения. Информация, приводимая оценщиком в ТОО относительно выполненного тестирования проникновения, не должна быть точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов проникновения, но должна обеспечивать достаточность данных, необходимых другим оценщикам и сотрудникам органов по сертификации для понимания выбранного подхода к тестированию проникновения, объема выполненного тестирования проникновения, тестируемых конфигураций ОО и общих результатов действий по тестированию проникновения.

Информация о действиях оценщика по тестированию проникновения, представленная в соответствующем разделе ТОО, включает:

а) описание тестируемых конфигураций ОО (конкретные конфигурации ОО, которые подвергались тестированию проникновения);

б) перечень ИФБО, применительно к которым осуществлялось тестирование проникновения (краткий перечень ИФБО и других интерфейсов ОО, на которых было сосредоточено тестирование проникновения);

в) заключение по данному подвиду деятельности (общий вывод по результатам тестирования проникновения).

Приведенный перечень не является исчерпывающим и определяет базовые сведения о выполненном оценщиком тестировании проникновения, которые необходимо привести в ТОО.

Детализация в соответствии с ИСО/МЭК ТО 20004

Оценщику необходимо определить условия использования специальных тестов проникновения, не разработанных на основе множества актуальных шаблонов атак, в случаях, требующих исследования непредвиденных результатов или потенциальных уязвимостей, о существовании которых оценщик сделал предположение на стадии планирования тестирования.

Шаг оценивания AVA_VAN.X-11

В соответствии с ГОСТ Р ИСО/МЭК 18045

Оценщик должен исследовать результаты всех действий по тестированию проникновения и выводы по анализу всех уязвимостей, чтобы сделать заключение, является ли ОО, находящийся в своей среде функционирования, стойким к нарушителю, обладающему Базовым потенциалом нападения.

Если результаты показывают, что ОО, находящийся в своей среде функционирования, имеет уязвимости, пригодные для использования нарушителем, обладающим потенциалом нападения ниже Усиленного базового, то по этому действию оценщиком выносится отрицательное заключение.

Руководство из приложения В.4 ГОСТ Р ИСО/МЭК 18045 необходимо использовать для вынесения заключения о потенциале нападения, требуемом для использования конкретной уязвимости, и возможности использования этой уязвимости в предполагаемой среде функционирования. Вычисление потенциала нападения для каждого случая может не требоваться, за исключением случаев, когда у оценщика остается сомнение относительно того, может ли уязвимость использоваться нарушителем, обладающим потенциалом нападения меньшим, чем Усиленный базовый.

Детализация в соответствии с ИСО/МЭК ТО 20004

Шаг не детализируется.

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, тестирование проникновения

БЗ 10—2016/32

Редактор *А.А. Кабанов*
Технический редактор *И.Е. Черепкова*
Корректор *М.С. Кабашова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 25.05.2018. Подписано в печать 01.06.2018. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,51.

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