ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 18045— 2013

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. МЕТОДОЛОГИЯ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ISO/IEC 18045:2008
Information technology — Security techniques — Methodology for IT security evaluation
(IDT)

Издание официальное

Москва
Стандартинформ
2014

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»), Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»)

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 28 августа 2013 г. №624-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 18045:2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» («ISO/IEC Information technology — Security techniques — Methodology for IT security evaluation»)

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 18045—2008

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). 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 информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

Содержание

Введение

Международный стандарт ISO/IEC 18045:2008 был подготовлен Совместным техническим комитетом ISO/IEC JTC 1 *«Информационные технологии»*, Подкомитетом SC 27 *«Методы и средства обеспечения безопасности ИТ»*. Идентичный ISO/IEC 18045:2008 текст опубликован организациями — спонсорами проекта «Общие критерии» как «Общая методология оценки безопасности информационных технологий».

Потенциальные пользователи этого международного стандарта — прежде всего оценщики, применяющие ИСО/МЭК 15408 (здесь и далее, если не указывается конкретная часть стандарта, то ссылка относится ко всем частям ИСО/МЭК 15408), и органы по сертификации, подтверждающие действия оценщика, а также заявители оценки, разработчики, авторы ПЗ/ЗБ и другие стороны, заинтересованные в безопасности ИТ.

Этот международный стандарт признает, что не на все вопросы оценки безопасности ИТ здесь представлены ответы и что дальнейшие интерпретации будут необходимы. В конкретных системах оценки решат, как обращаться с такими интерпретациями, хотя они могут быть подчинены соглашениям о взаимном признании. Список связанных с методологией вопросов, которые могут определяться в конкретной системе оценки, приведен в приложении А.

Вторая редакция стандарта отменяет и заменяет первую редакцию (ГОСТ Р ИСО/МЭК 18045:2007), которая подверглась технической переработке.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. МЕТОДОЛОГИЯ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Information technology — Security techniques — Methodology for IT security evaluation

Дата введения — 2014—07—01

1 Область применения

Настоящий стандарт — документ, сопровождающий ИСО/МЭК 15408 «Информационная технология — *Методы и средства обеспечения безопасности — Критерии оценки безопасности информационных технологий».* Настоящий стандарт описывает минимум действий, выполняемых оценщиком при проведении оценки по ИСО/МЭК 15408 с использованием критериев и свидетельств оценки, определенных в ИСО/МЭК 15408.

Настоящий стандарт не определяет действия оценщика для некоторых компонентов высокого доверия ИСО/МЭК 15408, по оценке которых пока нет единых согласованных руководств.

2 Нормативные ссылки

Указанные в данном разделе документы являются необходимыми для применения настоящего стандарта. Для датированных ссылок используют только указанное издание. Для недатированных ссылок — последнее издание со всеми изменениями и дополнениями.

ИСО/МЭК 15408 (все части) *Информационная технология — Методы и средства обеспечения безопасности — Критерии оценки безопасности ИТ* [ISO/IEC 15408 (all parts) Information technology — Security techniques — Evaluation criteria for IT security].

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

Примечание — Для терминов, выделенных в тексте определений полужирным шрифтом, в данном разделе даны собственные определения.

3.1 **действие** (action): Элемент действий оценщика из ИСО/МЭК 15408-3.

Примечание — Эти действия или сформулированы в явном виде как действия оценщика, или неявно следуют из действий разработчика (подразумеваемые действия оценщика) в рамках компонентов требований доверия из ИСО/МЭК 15408-3.

3.2 **вид деятельности** (activity): Применение класса требований доверия из ИСО/МЭК 15408-3.

3.3 **проверить** (check): Вынести **вердикт** посредством простого сравнения.

Примечание — Специальные знания и опыт оценщика не требуются. В формулировке, в которой используется этот глагол, описывается то, что сравнивается.

3.4 **поставка для оценки** (evaluation deliverable): Любой ресурс, который оценщик или орган оценки требует от заявителя или разработчика для выполнения одного или нескольких видов деятельности по проведению оценки или по надзору за оценкой.

Издание официальное

3.5 **свидетельство оценки** (evaluation evidence): Фактическая **поставка для оценки**.

3.6 **технический отчет об оценке** (evaluation technical report): Отчет, выпущенный оценщиком и представленный в орган оценки, в котором приводится **общий вердикт** и его логическое обоснование.

3.7 **исследовать** (examine): Вынести **вердикт** на основе анализа с использованием специальных знаний и опыта оценщика.

Примечание — Формулировка, в которой используется этот глагол, указывает на то, что конкретно и какие свойства подвергаются анализу.

3.8 **интерпретация** (interpretation): Разъяснение или расширение требования ИСО/МЭК 15408, ИСО/МЭК 18045 или **системы оценки**.

3.9 **методология** (methodology): Система принципов, процедур и процессов, применяемых для оценки безопасности ИТ.

3.10 **сообщение о проблеме** (observation report): Сообщение, документально оформленное оценщиком, в котором он просит разъяснений или указывает на возникшую при оценке проблему.

3.11 **общий вердикт** (overall verdict): *Положительный* или *отрицательный* вывод оценщика по результатам оценки.

3.12 **вердикт органа оценки** (oversight verdict): Вывод органа оценки, подтверждающий или отклоняющий *общий вердикт*, который основан на результатах деятельности по надзору за оценкой.

3.13 **зафиксировать** (record): Сохранить в документальной форме описания процедур, событий, данных наблюдений, предположений и результатов на уровне детализации, достаточном для обеспечения возможности воспроизведения процесса выполнения оценки в будущем.

3.14 **привести в отчете (сообщении)** (report): Включить результаты оценки и вспомогательные материалы в **технический отчет об оценке** или в **сообщение о проблеме**.

3.15 **система оценки** (scheme): Совокупность правил, установленных органом оценки и определяющих среду оценки, включая критерии и **методологию**, требуемые для проведения оценки безопасности ИТ.

3.16 **подвид деятельности** (sub-activity): Применение компонента требований доверия из ИСО/МЭК 15408-3.

Примечание — Семейства требований доверия прямо не рассматриваются в настоящем стандарте, поскольку при проведении оценки всегда используется только один компонент доверия из применяемого семейства.

3.17 **прослеживание** (tracing): Однонаправленная связь между двумя совокупностями сущностей, которая показывает, какие сущности в первой совокупности каким сущностям из второй соответствуют.

3.18 **вердикт** (verdict): Вывод оценщика *положительный, отрицательный или неокончательный* применительно к некоторому элементу действий оценщика, компоненту или классу требований доверия из ИСО/МЭК 15408.

Примечание — См. также общий вердикт.

3.19 **шаг оценивания** (work unit): Наименьшая структурная единица работ по оценке.

Примечание — Каждое действие в методологии оценки включает один или несколько шагов оценивания, которые объединены в пределах этого действия методологии оценки согласно элементу содержания и представления свидетельств или элементу действий разработчика. Шаги оценивания представлены в настоящем стандарте в том же порядке, что и элементы ИСО/МЭК 15408, из которых они следуют. Шаги оценивания идентифицированы условным обозначением типа ALC_TAT.1-2. В этом обозначении последовательность символов ALC_TAT.1 указывает на компонент ИСО/МЭК 15408 (т. е. на подвид деятельности из настоящего стандарта), а завершающая цифра (2) указывает, что это второй шаг оценивания в подвиде деятельности ALC_TAT.1.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения:

ЗБ (ST) — задание по безопасности

ИТ (IT) — информационная технология

ИФБО (TSFI) — интерфейс ФБО

ОО (TOE) — объект оценки

ОУД (EAL) — оценочный уровень доверия

ПБОр (OSP) — политика безопасности организации

ПЗ (PP) — профиль защиты

ТДБ (SAR) — требование доверия к безопасности

УК (CM) — управление конфигурацией
ФБО (TSF) — функциональные возможности безопасности ОО
ФТБ (SFR) — функциональное требование безопасности
ТОО (ETR) — технический отчет об оценке
СП (OR) — сообщение о проблеме

5 Краткий обзор

5.1 Структура стандарта

Раздел 6 определяет соглашения, используемые в настоящем стандарте.

В разделе 7 описываются общие задачи оценки без определения вердиктов, связанных с ними, поскольку эти задачи не отображаются на элементы действий оценщика из ИСО/МЭК 15408.

Раздел 8 описывает работы, необходимые для получения результата оценки ПЗ.

В разделах 9—15 определяются действия по оценке, сгруппированные по классам доверия.

Приложение А охватывает базовые методы оценки, используемые для предоставления технических свидетельств результатов оценки.

В приложении В приводится пояснение критериев оценки уязвимостей и примеры их применения.

6 Принятые соглашения

6.1 Терминология

В отличие от ИСО/МЭК 15408, где каждый элемент во всех компонентах одного семейства доверия имеет один и тот же номер, указанный последней цифрой его условного обозначения, настоящий стандарт может вводить новые шаги оценивания при изменении элемента действий оценщика из ИСО/МЭК 15408 в зависимости от подвида деятельности; в результате последняя цифра условного обозначения последующих шагов оценивания изменится, хотя шаг оценивания останется тем же самым.

Любая определенная в методологии работа по оценке, которая не следует непосредственно из требований ИСО/МЭК 15408, называется *задачей* или *подзадачей*.

6.2 Употребление глаголов

Вспомогательный глагол *должен* используется только при обязательности содержащего его текста и, следовательно, только в рамках определённого шага оценивания или подзадачи. Шаги оценивания и подзадачи содержат обязательные действия по оценке, которые оценщик должен выполнить, чтобы вынести вердикт.

Текст, сопровождающий шаги оценивания и подзадачи, содержит дальнейшие разъяснения использования формулировок ИСО/МЭК 15408 при оценке. Употребление глаголов соответствует принятым в ИСО определениям этих глаголов. Вспомогательный глагол *следует* используется в том случае, если описываемый метод строго предпочтителен. Все прочие вспомогательные глаголы, в том числе *может*, используются в том случае, когда описываемый метод не является обязательным или строго предпочтительным, а текст служит для пояснения.

Глаголы *проверить (check), исследовать (examine), привести в отчете (report) и зафиксировать (record)* в тексте настоящего стандарта имеют точный смысл, указанный в определениях раздела 3.

6.3 Общие указания по оценке

Материал, который применим более чем к одному подвиду деятельности, приводится в одном месте. Указания, которые являются широко применимыми (к нескольким видам деятельности или ОУД), приведены в приложении А. Указания, относящиеся к нескольким подвидам одного вида деятельности, содержатся во вводной части описания этого вида деятельности. Если указания относятся только к одному подвиду деятельности, они содержатся только в его описании.

6.4 Взаимосвязь между структурами ИСО/МЭК 15408 и ИСО/МЭК 18045

Имеется прямая взаимосвязь между структурой ИСО/МЭК 15408 (класс—семейство—компонент—элемент) и структурой настоящего стандарта. Рисунок 1 иллюстрирует соответствие между такими конструкциями ИСО/МЭК 15408, как классы, компоненты и элементы действий оценщика, и рассматриваемыми в методологии оценки видами деятельности, подвидами деятельности и действиями по оценке.

Впрочем, некоторые шаги оценивания из методологии оценки могут следовать из требований ИСО/МЭК 15408, содержащихся в элементах действий разработчика или содержания и представления свидетельств.

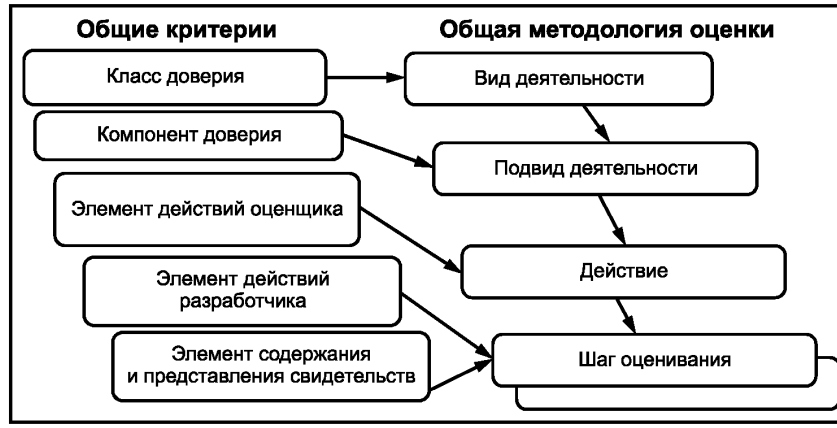

Рисунок 1 — Соотношение структур ИСО/МЭК 15408 и ИСО/МЭК 18045

7 Процесс оценки и соответствующие задачи оценки

7.1 Введение

В данном разделе представлен краткий обзор процесса оценки и определены задачи, которые следует выполнить оценщику при проведении оценки.

Каждый тип оценки: оценка ПЗ или оценка ОО (в том числе оценка ЗБ) проводится в рамках единого процесса и включает четыре общие задачи для оценщика: задачу получения исходных данных для оценки, задачу оформления результатов оценки, задачу выполнения подвидов деятельности по оценке и задачу демонстрации технической компетентности органу по оценке.

Задача получения исходных данных для оценки и задача оформления результатов оценки, которые относятся к управлению свидетельствами оценки и созданию отчетов (сообщений), полностью описаны в данном разделе. Каждая из задач включает связанные с ней подзадачи, которые применяются и являются нормативными для всех типов оценок по ИСО/МЭК 15408 (оценка ПЗ или оценка ОО).

Подвиды деятельности по оценке в данном разделе вводятся, а полностью описываются в последующих разделах.

В противоположность подвидам деятельности по оценке, задача получения исходных данных для оценки и задача оформления результатов оценки не имеют связанных с ними вердиктов, поскольку эти задачи не отображаются на элементы действий оценщика из ИСО/МЭК 15408; они выполняются, чтобы обеспечить соответствие универсальным принципам и настоящему стандарту.

Задача демонстрации технической компетентности органу по оценке может быть выполнена органом по оценке с помощью анализа итогов задачи по оформлению результатов оценки или может включать демонстрацию оценщиками их понимания исходных данных для подвидов деятельности по оценке. Для этой задачи не имеется связанного с ней вердикта оценщика, но имеется вердикт органа по оценке. Подробные критерии для выполнения этой задачи остаются на усмотрение органа по оценке, как отмечено в приложении А.5.

7.2 Краткое описание процесса оценки

7.2.1 Цели

В данном подразделе представлена общая модель методологии оценки и определяются:

a) роли и обязанности сторон, вовлеченных в процесс оценки;

b) общая модель оценки.

7.2.2 Обязанности ролей

Общая модель определяет следующие роли: заявителя, разработчика, оценщика и органа оценки.

Заявитель предъявляет запрос об оценке и отвечает за поддержание процесса оценки. Это означает, что заявитель заключает различные соглашения по поводу проведения оценки (например относительно начала процесса оценки). Кроме того, заявитель отвечает и за то, чтобы оценщику были доступны свидетельства оценки.

Разработчик создает ОО и отвечает за предоставление необходимых для оценки свидетельств (например сведений об обучении персонала, информацию о проекте) от лица заявителя.

Оценщик выполняет задачи оценки, требуемые в контексте оценки: получает свидетельства оценки от разработчика, действующего от лица заявителя или непосредственно от самого заявителя, выполняет подвиды деятельности по оценке и предоставляет результаты оценивания органу оценки.

Орган оценки устанавливает и поддерживает систему оценки, контролирует процесс оценки, проводимый оценщиком, выпускает отчеты о сертификации/ратификации, а также сертификаты, основанные на результатах оценки, предоставленных оценщиком.

7.2.3 Взаимоотношения между ролями

Для предотвращения негативных воздействий на процесс оценки требуется обеспечить некоторое разделение ролей. Это подразумевает, что все роли, описанные выше, выполняются различными юридическими и физическими лицами, за исключением того, что роли разработчика и заявителя может выполнять одно лицо.

Кроме того, при проведении некоторых видов оценки (например оценки по ОУД1) может не требоваться вовлечение разработчика в процесс оценки. В таком случае ОО оценщику предоставляет заявитель, и он же генерирует свидетельства оценки.

7.2.4 Общая модель оценки

Процесс оценки состоит из выполнения оценщиком задачи получения исходных данных для оценки, задачи оформления результатов оценки и задачи выполнения подвидов деятельности по оценке. На рисунке 2 отражены отношения между этими задачами и подвидами деятельности.

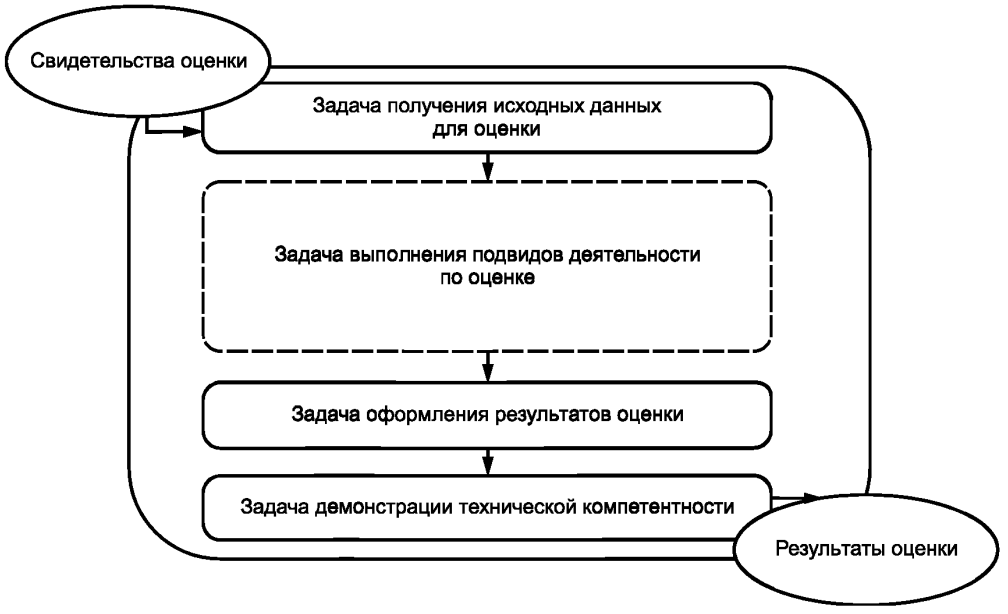

Рисунок 2 — Общая модель оценки

Процессу оценки может предшествовать фаза подготовки, где заявитель и оценщик налаживают друг с другом связь и устанавливают деловые отношения. Во время этой фазы может значительно варьироваться состав выполняемых работ и число вовлеченных сторон. Как правило, именно во время этого шага оценщик выполняет анализ выполнимости успешной оценки.

7.2.5 Вердикты оценщика

Оценщик выносит вердикт относительно выполнения требований ИСО/МЭК 15408, а не требований настоящего стандарта. Наименьшая структурная единица ИСО/МЭК 15408, по которой выносится вердикт, — элемент действий оценщика (явный или подразумеваемый). Вердикт по выполняемому эле-

менту действий оценщика из ИСО/МЭК 15408 выносится как результат выполнения соответствующего действия по оценке из методологии оценки и составляющих его шагов оценивания. В итоге результат оценки формируется в соответствии с разделом 9 «Результаты оценки» стандарта ИСО/МЭК 15408-1.

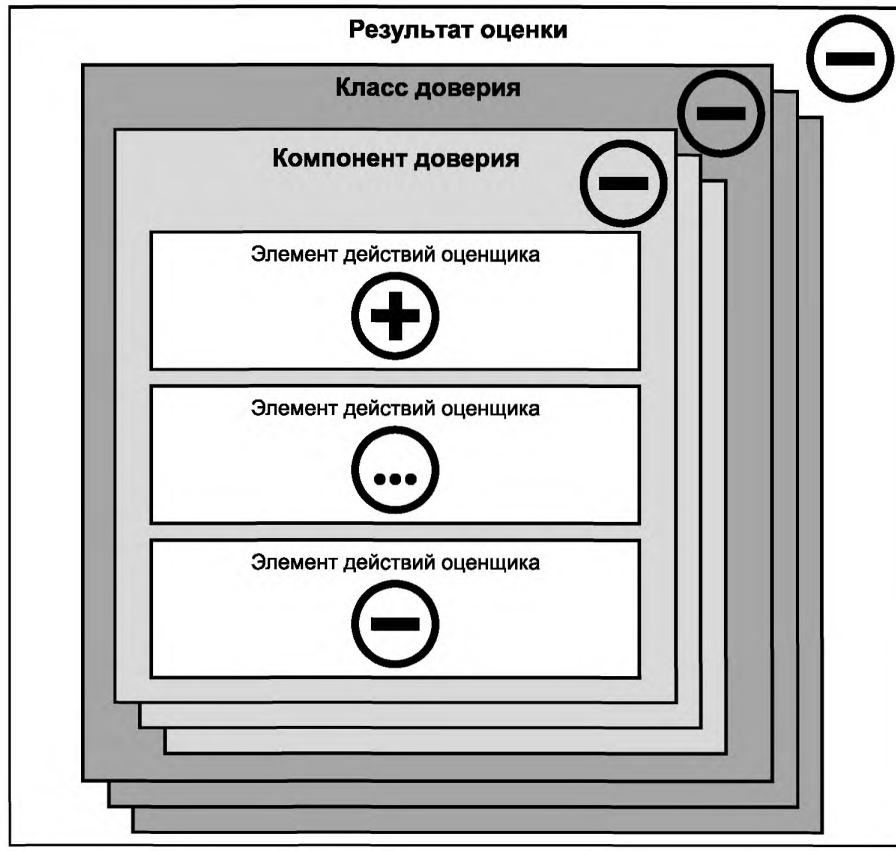

Рисунок 3 — Пример правила вынесения вердикта

В настоящем стандарте различаются три взаимоисключающих вида вердикта:

a) условиями *положительного* вердикта являются завершение оценщиком элемента действий оценщика из ИСО/МЭК 15408 и определение, что требования к оцениваемому ПЗ, ЗБ или ОО выполнены. Для элемента условиями положительного вердикта являются:

1) успешное завершение всех шагов оценивания, составляющих соответствующее действие из методологии оценки;

2) предоставление всех свидетельств оценки, требуемых для выполнения шагов оценивания, в логичной последовательности и в такой форме, чтобы они могли быть в полной мере поняты оценщиком;

3) отсутствие в свидетельствах оценки, требуемых для выполнения шагов оценивания, явных внутренних противоречий или несогласованности с другими свидетельствами. Следует отметить, что под явными подразумеваются такие противоречия, которые оценщик обнаруживает в процессе выполнения шагов оценивания: оценщику не следует каждый раз при выполнении шага оценивания проводить полный анализ непротиворечивости всех свидетельств.

b) условиями *отрицательного* вердикта являются завершение оценщиком элемента действий оценщика из ИСО/МЭК 15408 и определение того, что требования к оцениваемому ПЗ, ЗБ или ОО не выполнены или что свидетельства оценки не являются логически связанными и однозначно понятными, а также при выявлении явной несогласованности в свидетельствах оценки.

c) Все вердикты поначалу *неокончательные* и остаются такими до вынесения *положительного* или *отрицательного* вердикта.

Общий вердикт *положительный* тогда и только тогда, когда все составляющие вердикта *положительные*. В примере, показанном на рисунке 3, вердикт для одного из элементов действий оценщика

отрицательный, поэтому вердикты для соответствующего компонента доверия, класса доверия и общий вердикт также *отрицательные*.

7.3 Задача получения исходных данных для оценки

7.3.1 Цели

Цель этой задачи состоит в том, чтобы обеспечить оценщика корректной версией свидетельств, необходимых для оценки, а также соответствующую их защиту. Иначе не может быть обеспечена ни техническая точность оценки, ни проведение оценки способом, обеспечивающим повторяемость и воспроизводимость результатов.

7.3.2 Замечания по применению

Ответственность за представление всех требуемых свидетельств оценки возлагается на заявителя. Однако большинство свидетельств оценки, вероятно, будет создано и поставлено разработчиком от имени заявителя.

Поскольку требования доверия относятся к ОО в целом, то необходимо, чтобы оценщику были доступны свидетельства оценки, относящиеся ко всем частям ОО. Область применения и требуемое содержание такого свидетельства оценки не зависят от уровня контроля разработчиком над каждой частью ОО. Например, если требуется проект, то требования семейства ADV_TDS «Проект ОО» относятся ко всем подсистемам, являющимся частью ФБО. Кроме того, требования доверия, согласно которым требуется выполнение определенных процедур (например из семейств ALC_CMC «Возможности УК» и ALC_DEL «Поставка»), также относятся к ОО в целом (включая любую часть, разработанную другим разработчиком).

Оценщику рекомендуется совместно с заявителем представить указатель требуемых свидетельств оценки. Этот указатель может являться совокупностью ссылок на документацию. В нем следует привести достаточную информацию (например аннотацию каждого документа, или, по меньшей мере, его полное название и перечень разделов, представляющих интерес), позволяющую оценщику легко найти требуемое свидетельство.

Информации, содержащейся в требуемом свидетельстве оценки, не предписана какая-либо специфическая структура документирования. Свидетельство оценки для подвида деятельности может быть обеспечено несколькими отдельными документами, или один документ может удовлетворять нескольким требованиям к исходным данным для некоторого подвида деятельности.

Оценщику требуются завершенные и официально выпущенные версии свидетельств оценки. Однако в процессе оценки в помощь оценщику могут представляться и предварительные материалы свидетельств, например при предварительной неформальной оценке, но не для использования в качестве основы для вердиктов. Оценщику может быть полезно ознакомиться с предварительными версиями следующих типов свидетельств оценки:

a) тестовая документация, позволяющая оценщику предварительно оценить тесты и процедуры тестирования;

b) проектная документация, предоставляющая оценщику исходную информацию для понимания конструкции ОО;

c) исходный код или схемы аппаратуры, позволяющие оценить применение стандартов, используемых разработчиком.

Использование предварительных версий свидетельств оценки наиболее применимо там, где оценка ОО выполняется параллельно с его разработкой. Однако это возможно и при оценке разработанного ОО, когда разработчику приходится выполнять дополнительную работу по устранению недостатков, указанных оценщиком (например по исправлению ошибки в проекте или в реализации), или когда требуются свидетельства для оценки безопасности, отсутствующие в имеющейся документации (например когда ОО изначально разрабатывался без учета требований ИСО/МЭК 15408).

7.3.3 Подзадача управления свидетельством оценки

7.3.3.1 Контроль конфигурации

Оценщик должен осуществлять контроль конфигурации свидетельства оценки.

ИСО/МЭК 15408 подразумевает, что после получения свидетельства оценщик способен идентифицировать и локализовать каждый элемент свидетельства оценки, а также определить, находится ли в его распоряжении конкретная версия документа.

Оценщик должен защищать свидетельство оценки от изменения или утраты, когда оно находится в его распоряжении.

7.3.3.2 Дальнейшее использование

Системы оценки могут предусматривать контроль за изъятием из использования свидетельств оценки после завершения оценки. Изъятие из использования свидетельств оценки может достигаться посредством следующих действий:

a) возврата свидетельств оценки;

b) архивирования свидетельств оценки;

c) уничтожения свидетельств оценки.

7.3.3.3 Конфиденциальность

Во время проведения оценки оценщик может получить доступ к чувствительной коммерческой информации заявителя и разработчика (например информации о конструкции ОО или специальных инструментальных средствах), а также к чувствительной государственной информации. Системы оценки могут предъявить к оценщику требования по обеспечению конфиденциальности свидетельств оценки. Заявитель и оценщик могут совместно согласовать и дополнительные требования, не противоречащие системе.

Требования конфиденциальности затрагивают многие аспекты проведения оценки, включая получение, обработку, хранение и дальнейшее использование свидетельств оценки.

7.4 Подвиды деятельности по оценке

Подвиды деятельности по оценке изменяются в зависимости от того, оценивается ли ПЗ или ОО. Кроме того, в случае оценки ОО подвиды деятельности зависят от выбранных требований доверия.

7.5 Задача оформления результатов оценки

7.5.1 Цели

Цель этого подраздела состоит в описании сообщения о проблеме (СП) и технического отчета об оценке (ТОО). Системы оценки могут потребовать дополнительные отчеты от оценщика, такие как отчеты об отдельных шагах оценивания или же представление дополнительной информации в СП и ТОО. Настоящий стандарт не препятствует включению дополнительной информации в эти отчеты (сообщения), поскольку он определяет лишь содержание минимально необходимой информации.

Непротиворечивое представление результатов оценки облегчает достижение универсального принципа повторяемости и воспроизводимости результатов. Непротиворечивость охватывает тип и объем информации, приводимой в ТОО и СП. Ответственность за согласованность ТОО и СП, относящихся к различным оценкам, возложена на орган оценки.

Для удовлетворения требований настоящего стандарта к содержанию информации в отчетах (сообщениях) оценщик выполняет две следующие подзадачи:

a) подготовку СП (если это необходимо при выполнении оценки);

b) подготовку ТОО.

7.5.2 Управление результатами оценки

Оценщик поставляет органу оценки ТОО, а также каждый СП, по мере того, как они становятся доступны. Требования контроля обработки ТОО и СП установлены системой оценки, которая может включать поставку заявителю или разработчику. ТОО и СП могут содержать чувствительную коммерческую информацию или персональные данные и, возможно, из них будет необходимо удалить такую информацию перед передачей заявителю.

7.5.3 Замечания по применению

В данной редакции стандарта требования обеспечения оценщика свидетельствами для поддержки переоценки и повторного использования результатов оценивания в явном виде не сформулированы. Когда заявителю требуется информация для переоценки или повторного использования результатов оценивания, следует проконсультироваться в системе оценки, в которой проводилась оценка.

7.5.4 Подзадача подготовки СП

СП предоставляют оценщику механизм для запроса разъяснений (например от органа оценки о применении требований) или для определения проблемы по одному из аспектов оценки.

При отрицательном вердикте оценщик должен представить СП для отражения результата оценки. В противном случае оценщик может использовать СП как один из способов выражения потребности в разъяснении.

В любом СП оценщик должен привести следующее:

a) идентификатор оцениваемого ПЗ или ОО;

b) задачу/подвид деятельности по оценке, при выполнении которой/которого проблема была выявлена;

c) суть проблемы;

d) оценку ее серьезности (например приводит к отрицательному вердикту, задерживает выполнение оценки или требует решения до завершения оценки);

e) наименование организации, ответственной за решение вопроса;

f) рекомендуемые сроки решения;

g) определение влияния на оценку отсутствия решения проблемы.

Адресаты рассылки СП и процедуры обработки сообщения зависят от характера содержания сообщения и от конкретной системы оценки. Системы оценки могут различать типы СП или определять дополнительные, различающиеся по требуемой информации и рассылке (например СП органам оценки и заявителям).

7.5.5 Подзадача подготовки ТОО

7.5.5.1 Цели

Оценщик должен подготовить ТОО, чтобы представить техническое логическое обоснование вердиктов.

Настоящий стандарт определяет требования к минимальному содержанию ТОО; однако системы оценки могут задать дополнительные требования к содержанию, конкретному представлению и структуре информации. Например, в системах оценки может требоваться, чтобы конкретный вводный материал (например налагаемые ограничения и заявление авторских прав) всегда включался в ТОО.

Предполагается, что читатель ТОО знаком с общими концепциями информационной безопасности, ИСО/МЭК 15408, настоящим стандартом, подходами к оценке и ИТ.

ТОО помогает органу оценки подтвердить, что оценка была произведена в соответствии с требованиями стандартов, но допускается, что задокументированные результаты оценки могут не содержать всей необходимой информации, поэтому может потребоваться дополнительная информация конкретно для данной системы оценки. Этот аспект находится за рамками области действия настоящего стандарта.

7.5.5.2 ТОО при оценке ПЗ

В данном подпункте приведено минимально необходимое содержание информации, включаемой в ТОО при оценке ПЗ. Содержание ТОО показано на рисунке 4; этот рисунок может использоваться как образец при построении структурной схемы ТОО.

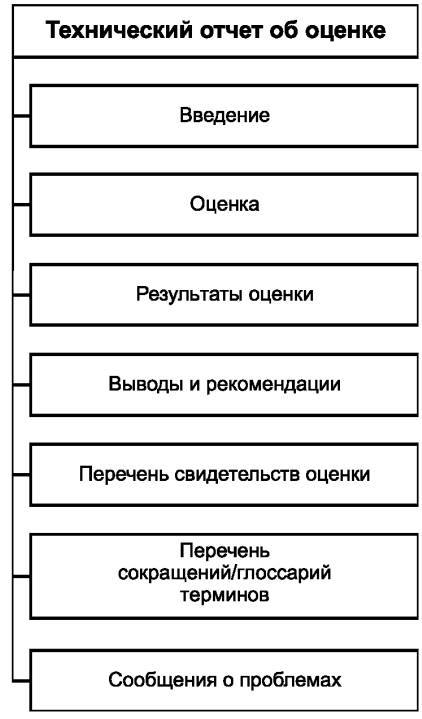

Рисунок 4 — Содержание ТОО при оценке ПЗ

7.5.5.2.1 Введение

Оценщик должен привести в отчете идентификаторы системы оценки.

Идентификаторы системы оценки (например логотип) являются информацией, требуемой для однозначной идентификации системы, ответственной за мониторинг оценки.

Оценщик должен привести в отчете идентификаторы контроля конфигурации ТОО.

Идентификаторы контроля конфигурации ТОО содержат информацию, которая идентифицирует ТОО (например наименование, дату составления и номер версии).

Оценщик должен привести в отчете идентификаторы контроля конфигурации ПЗ.

Идентификаторы контроля конфигурации ПЗ (например название, дата составления и номер версии) требуются, чтобы орган оценки мог определить, что именно оценивается, и подтвердить правильность вынесенных оценщиком вердиктов.

Оценщик должен привести в отчете идентификатор разработчика.

Идентификатор разработчика ПЗ требуется для идентификации стороны, ответственной за создание ПЗ.

Оценщик должен привести в отчете идентификатор заявителя.

Идентификатор заявителя требуется для идентификации стороны, ответственной за представление оценщику свидетельств оценки.

Оценщик должен привести в отчете идентификатор оценщика.

Идентификатор оценщика необходим для идентификации стороны, выполняющей оценку и ответственной за вердикты по результатам оценки.

7.5.5.2.2 Оценка

Оценщик должен привести в отчете сведения о применяемых методах оценки, технологии, инструментальных средствах и стандартах.

Оценщик приводит ссылки на использованные при оценке ПЗ критерии оценки, методологию и интерпретации.

Оценщик должен привести в отчете сведения о любых ограничениях, принятых при оценке, об ограничениях на распространение результатов оценки и о предположениях, сделанных во время оценки, которые влияют на ее результаты.

Оценщик может включить в отчет информацию о правовых или законодательных аспектах, организации работ, конфиденциальности и т.д.

7.5.5.2.3 Результаты оценки

Оценщик должен привести в отчете вердикт, сопровождаемый обоснованием, для каждого из компонентов доверия, составляющих вид деятельности APE как результат выполнения соответствующего действия методологии оценки и составляющих его шагов оценивания.

Обоснование представляет объяснение для вынесения вердикта, сделанного на основе ИСО/МЭК 15408, ИСО/МЭК 18045, любых их интерпретаций и изученных свидетельств оценки, и показывает, насколько свидетельства оценки удовлетворяют или не удовлетворяют каждому аспекту критериев. Оно содержит описание выполненной работы, используемых методов и процедур получения результатов. Обоснование может обеспечивать детализацию до уровня шагов оценивания из методологии оценки.

7.5.5.2.4 Выводы и рекомендации

Оценщик должен привести в отчете выводы по результатам оценки, в частности, общий вердикт в соответствии с разделом 9 «Результаты оценки» ИСО/МЭК 15408-1 и процедурой вынесения вердикта, описанной в пункте 7.2.5 настоящего стандарта.

Оценщик дает рекомендации, которые могут быть полезны для органа оценки. Эти рекомендации могут указывать на недостатки ПЗ, обнаруженные во время оценки, или упоминать о его свойствах, которые особенно полезны.

7.5.5.2.5 Перечень свидетельств оценки

Оценщик должен привести в отчете следующую информацию о каждом свидетельстве оценки:

- о составителе свидетельства (например разработчик, заявитель);
- о названии свидетельства;
- об уникальной ссылке на свидетельство (например дата составления и номер версии).

7.5.5.2.6 Перечень сокращений/глоссарий терминов

Оценщик должен привести в отчете перечень всех сокращений, используемых в ТОО.

В ТОО нет необходимости повторять определения глоссария, уже приведенные в ИСО/МЭК 15408 или настоящем стандарте.

7.5.5.2.7 Сообщения о проблемах

Оценщик должен привести в отчете полный перечень, уникально идентифицирующий все СП, подготовленные во время оценки, а также их статус.

Для каждого СП в перечне следует привести идентификатор СП, а также название или аннотацию.

7.5.5.3 ТОО при оценке ОО

В данном подпункте приведено минимально необходимое содержание информации, включаемой в ТОО при оценке ОО. Содержание ТОО показано на рисунке 5; этот рисунок может использоваться как образец при построении структурной схемы ТОО.

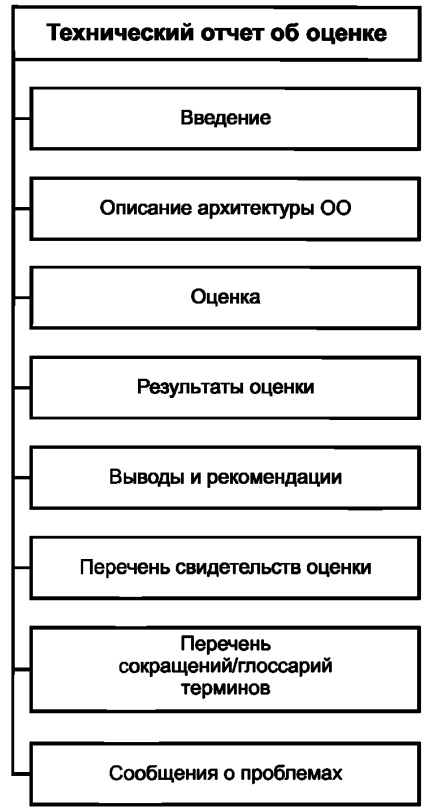

Рисунок 5 — Содержание ТОО при оценке ОО

7.5.5.3.1 Введение

Оценщик должен привести в отчете идентификаторы системы оценки.

Идентификаторы системы оценки (например логотип) являются информацией, требуемой для однозначной идентификации системы, ответственной за мониторинг оценки.

Оценщик должен привести в отчете идентификаторы контроля конфигурации ТОО.

Идентификаторы контроля конфигурации ТОО содержат информацию, которая идентифицирует ТОО (например название, дату составления и номер версии).

Оценщик должен привести в отчете идентификаторы контроля конфигурации ЗБ и ОО.

Идентификаторы контроля конфигурации ЗБ и ОО требуются, чтобы орган оценки мог определить, что именно оценивается, и подтвердить правильность вынесенных оценщиком вердиктов.

Если ЗБ содержит «Утверждения о соответствии» ОО требованиям одного или нескольких ПЗ, ТОО должен содержать ссылку на соответствующие ПЗ.

Ссылка на ПЗ содержит информацию, которая уникально идентифицирует ПЗ (например название, дату составления и номер версии).

Оценщик должен привести в отчете идентификатор разработчика.

Идентификатор разработчика ОО требуется для идентификации стороны, ответственной за создание ОО.

Оценщик должен привести в отчете идентификатор заявителя.

Идентификатор заявителя требуется для идентификации стороны, ответственной за представление оценщику свидетельств оценки.

Оценщик должен привести в отчете идентификатор оценщика.

Идентификатор оценщика необходим для идентификации стороны, выполняющей оценку и ответственной за вердикты по результатам оценки.

7.5.5.3.2 Описание архитектуры ОО

Оценщик должен привести в отчете высокоуровневое «Описание ОО» и его главных компонентов, основанное на свидетельстве оценки, указанном в семействе доверия ИСО/МЭК 15408 «Проект ОО» (ADV_TDS), где оно применимо.

Назначение этого пункта состоит в указании степени архитектурного разделения главных компонентов. Если в ЗБ нет требований из семейства ADV_TDS «Проект ОО», этот пункт не применим и считается удовлетворенным.

7.5.5.3.3 Оценка

Оценщик должен привести в отчете сведения о методах оценки, технологии, инструментальных средствах и применяемых стандартах.

Оценщик может сослаться на критерии оценки, методологию и интерпретации, использованные при оценке ОО, или на устройства, применяемые при тестировании.

Оценщик должен привести в отчете сведения о любых ограничениях, принятых при оценке, об ограничениях на распространение результатов оценки и о предположениях, сделанных во время оценки, которые влияют на ее результаты.

Оценщик может включить в отчет информацию о правовых или законодательных аспектах, организации работ, конфиденциальности и т. д.

7.5.5.3.4 Результаты оценки

Для каждого вида деятельности по оценке ОО оценщик должен привести в отчете:

- название рассматриваемого вида деятельности;
- вердикт, сопровождаемый обоснованием для каждого компонента доверия, составляющего этот вид деятельности как результат выполнения соответствующего действия методологии оценки и составляющих его шагов оценивания.

В обосновании поясняется вердикт с использованием ИСО/МЭК 15408, настоящего стандарта, любых их интерпретаций и изученных свидетельств оценки, а также демонстрируется, насколько свидетельства оценки удовлетворяют или не удовлетворяют каждому аспекту критериев. Обоснование содержит описание выполненной работы, используемых методов и процедур получения результатов. Обоснование может обеспечивать детализацию до уровня шагов оценивания из методологии оценки.

Оценщик должен привести в отчете всю информацию, специально запрошенную на шагах оценивания.

Для видов деятельности AVA и ATE указываются шаги оценивания, которые определяют информацию, включаемую в ТОО.

7.5.5.3.5 Выводы и рекомендации

Оценщик должен привести в отчете выводы по результатам оценки об удовлетворении ОО требованиям своего ЗБ, в частности, общий вердикт в соответствии с разделом 9 «Результаты оценки» ИСО/МЭК 15408-1 и процедурой вынесения вердикта, описанной в пункте 7.2.5 настоящего стандарта.

Оценщик дает рекомендации, которые могут быть полезны для органа оценки. Эти рекомендации могут указывать на недостатки продукта ИТ, обнаруженные во время оценки, или упоминать о его свойствах, которые особенно полезны.

7.5.5.3.6 Перечень свидетельств оценки

Оценщик должен привести в отчете следующую информацию о каждом свидетельстве оценки:

- о составителе свидетельства (например разработчик, заявитель);
- о названии свидетельства;
- об уникальной ссылке на свидетельство (например дата составления и номер версии).

7.5.5.3.7 Перечень сокращений/глоссарий терминов

Оценщик должен привести в отчете перечень всех сокращений, используемых в ТОО.

В ТОО нет необходимости повторять определения глоссария, уже приведенные в ИСО/МЭК 15408 или настоящем стандарте.

7.5.5.3.8 Сообщения о проблемах

Оценщик должен привести в отчете полный перечень, уникально идентифицирующий все СП, подготовленные во время оценки, а также их статус.

Для каждого СП в перечне следует привести идентификатор СП, а также название или аннотацию.

8 Класс APE: Оценка профиля защиты

8.1 Введение

Этот раздел описывает оценку ПЗ. Требования и методология оценки ПЗ идентичны для каждой оценки ПЗ, независимо от ОУД (или другой совокупности требований доверия), заявленного в ПЗ. Методология оценки в этом разделе основана на требованиях к ПЗ, определенных в классе APE из ИСО/МЭК 15408-3.

Данный раздел следует использовать вместе с приложениями A, B и C в ИСО/МЭК 15408-1, поскольку в этих приложениях разъясняются приведенные здесь понятия и приводятся многочисленные примеры.

8.2 Замечания по применению

8.2.1 Повторное использование результатов оценки сертифицированных ПЗ

При осуществлении оценки ПЗ, который основан на одном или нескольких сертифицированных ПЗ, есть возможность использовать тот факт, что данные ПЗ уже прошли сертификацию. Возможность повторного использования результата оценки сертифицированных ПЗ больше, если оцениваемый ПЗ не добавляет угроз, ПБОр, целей безопасности и/или требований безопасности к тем ПЗ, с которыми утверждается соответствие. Если в оцениваемом ПЗ содержится намного больше угроз, ПБОр, целей безопасности и/или требований безопасности, чем в сертифицированном ПЗ, повторное использование результатов сертификации может быть бесполезным.

Оценщику разрешается повторно использовать результаты оценки ПЗ, проводя определенные исследования только частично или вовсе не выполняя их, если эти исследования или их части были проведены в рамках оценки ПЗ. Делая это, оценщику следует предположить, что анализ ПЗ был проведен правильно.

Примером может служить следующая ситуация: анализируется соответствие некоторому ПЗ, содержащему ряд требований безопасности. Эти требования в процессе оценки ПЗ были признаны внутренне непротиворечивыми. Если в оцениваемом ПЗ используются эти же требования, анализ непротиворечивости не обязательно повторно проводить во время оценки ПЗ. Если же оцениваемый ПЗ добавляет одно или более требований или выполняет над ними операции, анализ необходимо повторить. Однако есть возможность сократить объем работ при анализе непротиворечивости, используя тот факт, что исходные требования внутренне непротиворечивы. Если исходные требования внутренне непротиворечивы, оценщик только должен определить, что:

a) ряд новых и/или измененных требований внутренне непротиворечив, и

b) все новые и/или измененные требования совместимы с исходными требованиями.

Оценщик отмечает в ТОО каждый случай, где исследования не сделаны или только частично сделаны по этой причине.

8.3 «Введение ПЗ» (APE_INT)

8.3.1 Подвид деятельности по оценке (APE_INT.1)

8.3.1.1 Цели

Цель этого подвида деятельности — сделать заключение о том, что ПЗ правильно идентифицирован и что «Ссылка на ПЗ» и «Аннотация ОО» не противоречат друг другу.

8.3.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.3.1.3 Действие APE_INT.1.1E

ИСО/МЭК 15408-3 APE_INT.1.1C: *«Введение ПЗ» должно содержать «Ссылку на ПЗ» и «Аннотацию ОО»*.

8.3.1.3.1 Шаг оценивания APE_INT.1-1

Оценщик должен проверить, представлены ли в разделе «Введение ПЗ» «Ссылка на ПЗ» и «Аннотация ОО».

ИСО/МЭК 15408-3 APE_INT.1.2C: *«Ссылка на ПЗ» должна уникально идентифицировать ПЗ.*

8.3.1.3.2 Шаг оценивания APE_INT.1-2

Оценщик должен исследовать «Ссылку на ПЗ» в целях определения того, что она уникально идентифицирует ПЗ.

Оценщик выносит заключение о том, что «Ссылка на ПЗ» идентифицирует ПЗ так, чтобы его можно было легко отличить от другого ПЗ, и что она уникально идентифицирует каждую версию ПЗ, например благодаря включению номера версии и/или даты публикации.

Рекомендуется наличие в ПЗ некоторой системы ссылок с поддержкой уникальных ссылок (например с использованием номеров, букв или даты публикации для обозначения ссылки на конкретную версию).

ИСО/МЭК 15408-3 APE_INT.1.3C: *В «Аннотации ОО» должна быть предоставлена краткая информация об использовании и основных функциональных возможностях безопасности ОО.*

8.3.1.3.3 Шаг оценивания APE_INT.1-3

Оценщик должен исследовать «Аннотацию ОО», чтобы сделать заключение о том, что она описывает использование и основные характеристики безопасности ОО.

В «Аннотации ОО» следует приводить краткое (несколько параграфов) описание использования ОО и основные характеристики безопасности, ожидаемые от ОО. Рекомендуется, чтобы «Аннотация ОО» предоставляла потенциальным пользователям и разработчикам ОО возможность быстро сделать заключение, представляет ли для них интерес данный ПЗ.

Оценщик делает заключение о том, является ли «Аннотация ОО» достаточно ясной для разработчиков и пользователей ОО и достаточной для получения ими общего понимания назначения ОО и его основных характеристик безопасности.

ИСО/МЭК 15408-3 APE_INT.1.4C: *В «Аннотации ОО» должен быть идентифицирован тип ОО.*

8.3.1.3.4 Шаг оценивания APE_INT.1-4

Оценщик должен проверить, идентифицирован ли в «Аннотации ОО» тип ОО.

ИСО/МЭК 15408-3 APE_INT.1.5C: *В «Аннотации ОО» должны быть идентифицированы любые не входящие в ОО аппаратные, программные, а также программно-аппаратные средства, доступные для ОО.*

8.3.1.3.5 Шаг оценивания APE_INT.1-5

Оценщик должен исследовать «Аннотацию ОО», чтобы сделать заключение о том, что в ней идентифицированы любые не входящие в ОО аппаратные, программные, а также программно-аппаратные средства, доступные для ОО.

В то время как некоторые ОО являются автономными, другим ОО (особенно если ОО является программным средством) для работы необходимы дополнительные аппаратные, программные или программно-аппаратные средства. В этом подразделе ПЗ автор ПЗ перечисляет все доступные аппаратные, программные или программно-аппаратные средства, которые могут быть запущены на ОО.

Рекомендуется, чтобы это перечисление было достаточно подробным для того, чтобы потенциальные пользователи и разработчики ОО могли определить, может ли их ОО функционировать с перечисленными аппаратными, программными или программно-аппаратными средствами.

8.4 Утверждения о соответствии (APE_CCL)

8.4.1 Подвид деятельности по оценке (APE_CCL.1)

8.4.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы определить обоснованность различных утверждений о соответствии. Он описывает, каким образом ПЗ соответствует ИСО/МЭК 15408, другим ПЗ и пакетам требований.

8.4.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности являются:

a) ПЗ;

b) другие ПЗ, соответствие которым утверждается в ПЗ;

c) пакеты требований, соответствие которым утверждается в ПЗ.

8.4.1.3 Действие APE_CCL.1.1E

ИСО/МЭК 15408-3 APE_CCL.1.1C: *В «Утверждения о соответствии» должно быть включено «Утверждение о соответствии ИСО/МЭК 15408», которое определяет, для какой редакции ИСО/МЭК 15408 утверждается соответствие ПЗ.*

8.4.1.3.1 Шаг оценивания APE_CCL.1-1

Оценщик должен проверить, что в «Утверждения о соответствии» включено «Утверждение о соответствии ИСО/МЭК 15408», которое определяет, для какой редакции ИСО/МЭК 15408 должен соответствовать ПЗ.

Оценщик делает заключение о том, что «Утверждение о соответствии ИСО/МЭК 15408» идентифицирует редакцию ИСО/МЭК 15408, которая использовалась для разработки данного ПЗ. В «Утверждение» следует включать номер редакции ИСО/МЭК 15408 и, если не использовалась международная редакция ИСО/МЭК 15408 на английском языке, то в нем следует указать язык используемой редакции ИСО/МЭК 15408.

ИСО/МЭК 15408-3 APE_CCL.1.2C: *В «Утверждении о соответствии ИСО/МЭК 15408» должно приводиться описание соответствия ПЗ ИСО/МЭК 15408-2; ПЗ либо описывается как соответствующий требованиям ИСО/МЭК 15408-2, либо как содержащий расширенные по отношению к ИСО/МЭК 15408-2 требования.*

8.4.1.3.2 Шаг оценивания APE_CCL.1-2

Оценщик должен проверить, что «Утверждение о соответствии ИСО/МЭК 15408» описывает соответствие ПЗ ИСО/МЭК 15408-2; ПЗ либо описывается как соответствующий требованиям ИСО/МЭК 15408-2, либо как содержащий расширенные по отношению к ИСО/МЭК 15408-2 требования.

ИСО/МЭК 15408-3 APE_CCL.1.3C: *В «Утверждении о соответствии ИСО/МЭК 15408» должно приводиться описание соответствия ПЗ ИСО/МЭК 15408-3; ПЗ либо описывается как соответствующий требованиям ИСО/МЭК 15408-3, либо как содержащий расширенные по отношению к ИСО/МЭК 15408-3 требования.*

8.4.1.3.3 Шаг оценивания APE_CCL.1-3

Оценщик должен проверить, что «Утверждение о соответствии ИСО/МЭК 15408» описывает соответствие ПЗ ИСО/МЭК 15408-3; ПЗ либо описывается как соответствующий требованиям ИСО/МЭК 15408-3, либо как содержащий расширенные по отношению к ИСО/МЭК 15408-3 требования.

ИСО/МЭК 15408-3 APE_CCL.1.4C: *«Утверждение о соответствии ИСО/МЭК 15408» должно согласовываться с «Определением расширенных компонентов».*

8.4.1.3.4 Шаг оценивания APE_CCL.1-4

Оценщик должен исследовать «Утверждение о соответствии ИСО/МЭК 15408-2» в целях вынесения заключения о его согласованности с «Определением расширенных компонентов».

Если «Утверждение о соответствии ИСО/МЭК 15408» в ПЗ содержит «Утверждение о соответствии ИСО/МЭК 15408-2», оценщик делает заключение о том, что «Определение расширенных компонентов» не определяет функциональные компоненты.

Если «Утверждение о соответствии ИСО/МЭК 15408» в ПЗ содержит утверждение о соответствии расширению ИСО/МЭК 15408-2, оценщик делает заключение о том, что «Определение расширенных компонентов» определяет хотя бы один расширенный функциональный компонент.

8.4.1.3.5 Шаг оценивания APE_CCL.1-5

Оценщик должен исследовать «Утверждение о соответствии ИСО/МЭК 15408» в отношении ИСО/МЭК 15408-3 в целях вынесения заключения о его согласованности с «Определением расширенных компонентов».

Если «Утверждение о соответствии ИСО/МЭК 15408» содержит «Утверждение о соответствии ИСО/МЭК 15408-3», оценщик делает заключение о том, что «Определение расширенных компонентов» не определяет компоненты требований доверия.

Если «Утверждение о соответствии ИСО/МЭК 15408» содержит «Утверждение о соответствии расширению ИСО/МЭК 15408-3», оценщик делает заключение о том, что «Определение расширенных компонентов» определяет хотя бы один расширенный компонент доверия.

ИСО/МЭК 15408-3 APE_CCL.1.5C: *В «Утверждении о соответствии» должны быть идентифицированы все ПЗ и пакеты требований безопасности, о соответствии которым утверждается в ПЗ.*

8.4.1.3.6 Шаг оценивания APE_CCL.1-6

Оценщик должен проверить, что «Утверждения о соответствии» содержит «Утверждение о соответствии ПЗ», идентифицирующее все ПЗ, о соответствии которым утверждается в ПЗ.

Если в ПЗ не утверждается соответствие ПЗ другим ПЗ, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик выносит заключение о том, что любой ПЗ, на который ссылаются, однозначно идентифицирован (например названием и номером версии или идентификацией, включенной во введение этого ПЗ).

Оценщику следует помнить, что утверждения частичного соответствия ПЗ недопустимы.

8.4.1.3.7 Шаг оценивания APE_CCL.1-7

Оценщик должен проверить, что «Утверждение о соответствии» содержит «Утверждение о соответствии пакетам требований», идентифицирующее все пакеты, о соответствии которым утверждается в ПЗ.

Если в ПЗ не утверждается соответствие какому-либо пакету требований, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик выносит заключение о том, что любой пакет требований, на который ссылаются, однозначно идентифицирован (например названием и номером версии или идентификацией, включенной во введение этого пакета).

Оценщику следует помнить, что утверждения частичного соответствия некоторому пакету требований недопустимы.

ИСО/МЭК 15408-3 APE_CCL.1.6C: *В «Утверждении о соответствии ПЗ пакету требований» должно приводиться описание любого соответствия ПЗ некоторому пакету требований; ПЗ либо описывается как соответствующий пакету требований, либо как содержащий расширенные по отношению к пакету требования.*

8.4.1.3.8 Шаг оценивания APE_CCL.1-8

Оценщик должен проверить, что для каждого идентифицированного пакета «Утверждения о соответствии» содержит утверждение либо о соответствии именованному пакету, либо о соответствии пакету, усиленному относительно именованного пакета.

Если в ПЗ не утверждается о соответствии какому-либо пакету требований, то этот шаг оценивания не применим и считается удовлетворенным.

Если в «Утверждении о соответствии ПЗ пакету требований» содержится утверждение о соответствии именованному пакету, оценщик делает заключение о том, что:

a) Если пакет является пакетом требований доверия, то ПЗ содержит все ТДБ, включенные в пакет, но не содержит дополнительных ТДБ.

b) Если пакет является функциональным, то ПЗ содержит все ФТБ, включенные в пакет, но не содержит дополнительных ФТБ.

Если в «Утверждении о соответствии ПЗ пакету требований» содержится утверждение о соответствии расширенному пакету требований относительно именованного, оценщик делает заключение о том, что:

a) Если пакет является пакетом доверия, то ПЗ содержит все ТДБ, включенные в пакет, и по крайней мере одно дополнительное ТДБ или одно ТДБ, которое является иерархическим к ТДБ в пакете.

b) Если пакет является функциональным, то ПЗ содержит все ФТБ, включенные в пакет, и по крайней мере одно дополнительное ФТБ или одно ФТБ, которое является иерархическим к ФТБ в пакете.

ИСО/МЭК 15408-3 APE_CCL.1.7C: *В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что тип ОО согласуется с типом ОО в тех ПЗ, о соответствии которым утверждается.*

8.4.1.3.9 Шаг оценивания APE_CCL.1-9

Оценщик должен исследовать «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что тип ОО согласуется со всеми типами ОО в ПЗ.

Если в ПЗ не утверждается о соответствии ПЗ другому ПЗ, то этот шаг оценивания не применим и считается удовлетворенным.

Отношение между типами может быть простым: например в ПЗ межсетевого экрана утверждается о соответствии другому ПЗ межсетевого экрана или более сложным: например в ПЗ смарт-карты утверждается о соответствии многим другим ПЗ одновременно — ПЗ интегральной схемы, ПЗ для ОС смарт-карты и двум ПЗ двух приложений на смарт-карте.

ИСО/МЭК 15408-3 APE_CCL.1.8C: *В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение определения проблемы безопасности согласуется с изложением определения проблемы безопасности тех ПЗ, о соответствии которым утверждается.*

8.4.1.3.10 Шаг оценивания APE_CCL.1-10

Оценщик должен исследовать «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что в соответствии с изложением «Утверждений о соответствии» в ПЗ изложение определения проблемы безопасности согласуется с изложениями определения проблемы безопасности в тех ПЗ, для которых требуется соответствие, как определено в заявлении о соответствии ПЗ.

Если в оцениваемом ПЗ не утверждается о соответствии другим ПЗ, то этот шаг оценивания не применим и считается удовлетворенным.

Если в ПЗ, о соответствии которому утверждается, не включено изложение «Определения проблемы безопасности», то этот шаг оценивания не применим и считается удовлетворенным.

Если требуется строгое соответствие ПЗ, о соответствии которому утверждается, тогда не требуется «Обоснование утверждений о соответствии». Вместо этого оценщик делает заключение о том, является ли:

a) набор угроз в оцениваемом ПЗ расширенным или идентичным по отношению к перечню угроз в ПЗ, о соответствии которому утверждается;

b) набор ПБОр в оцениваемом ПЗ расширенным или идентичным по отношению к ПБОр в ПЗ, о соответствии которому утверждается;

c) набор предположений в оцениваемом ПЗ идентичным по отношению к предположениям в ПЗ, о соответствии которому утверждается.

Если требуется возможность продемонстрировать соответствие тем ПЗ, о соответствии которым требуется продемонстрировать соответствие, оценщик исследует «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что оно демонстрирует, что изложение «Определения проблемы безопасности» в оцениваемом ПЗ эквивалентное или более ограничительное, чем «Определение проблемы безопасности» в ПЗ, о соответствии которому утверждается.

В качестве руководства о том, что считать «эквивалентным или более ограничительным» изложением, см. ИСО/МЭК 15408-1 приложение D «Соответствие ПЗ».

ИСО/МЭК 15408-3 APE_CCL.1.9C: *В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение «Целей безопасности» согласуется с изложением «Целей безопасности» в тех ПЗ, о соответствии которым утверждается.*

8.4.1.3.11 Шаг оценивания APE_CCL.1-11

Оценщик должен исследовать «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что изложение «Целей безопасности» согласуется с изложением «Целей безопасности» в тех ПЗ, о соответствии которым утверждается.

Если в ПЗ не утверждается о соответствии ПЗ другому ПЗ, то этот шаг оценивания не применим и считается удовлетворенным.

Если требуется строгое соответствие ПЗ, о соответствии которому утверждается, тогда не требуется «Обоснование утверждений о соответствии». Вместо этого оценщик делает заключение о том, содержит ли:

- оцениваемый ПЗ все цели безопасности для ОО того ПЗ, о соответствии которому утверждается. Следует отметить, что в оцениваемом ПЗ допускается наличие дополнительных целей безопасности для ОО;

- оцениваемый ПЗ абсолютно все цели безопасности для среды функционирования (за одним исключением, которое описано в следующем абзаце). Следует отметить, что в оцениваемом ПЗ не допускается наличие дополнительных целей безопасности для среды функционирования;

- оцениваемый ПЗ утверждение о том, что некоторые цели безопасности для среды функционирования того ПЗ, о соответствии которому утверждается, являются целями безопасности для ОО в оцениваемом ПЗ. Это — имеющее силу исключение из предыдущего абзаца.

Если тому ПЗ, о соответствии которому утверждается, требуется демонстрируемое соответствие, оценщик исследует «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что оно демонстрирует, что изложение «Целей безопасности» в оцениваемом ПЗ эквивалентное или более ограничительное, чем изложение «Целей безопасности» в ПЗ, о соответствии которому утверждается.

В качестве руководства о том, что считать «эквивалентным или более ограничительным» изложением, см. ИСО/МЭК 15408-1 приложение D «Соответствие ПЗ».

ИСО/МЭК 15408-3 APE_CCL.1.10C: *В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение «Требований безопасности» согласуется с изложением «Требований безопасности» в тех ПЗ, о соответствии которым утверждается.*

8.4.1.3.12 Шаг оценивания APE_CCL.1-12

Оценщик должен исследовать ПЗ, чтобы сделать заключение о том, что в соответствии с изложением соответствия в этом ПЗ он согласуется со всеми требованиями безопасности в тех ПЗ, о соответствии которым утверждается.

Если в ПЗ не утверждается о соответствии другому ПЗ, то этот шаг оценивания не применим и считается выполненным успешно.

Если требуется строгое соответствие ПЗ, о соответствии которому утверждается, тогда не требуется «Обоснование утверждений о соответствии». Вместо этого оценщик делает заключение о том, является ли изложение «Требований безопасности» в оцениваемом ПЗ расширенным или идентичным изложению «Требований безопасности» в ПЗ, о соответствии которому утверждается (для строгого соответствия).

Если требуется демонстрируемое соответствие тем ПЗ, о соответствии которому утверждается, оценщик исследует «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что оно демонстрирует, что изложение «Требований безопасности» в оцениваемом ПЗ эквивалентное или более ограничительное, чем изложение «Требований безопасности» в ПЗ, о соответствии которому утверждается.

В качестве руководства о том, что считать «эквивалентным или более ограничительным» изложением, см. ИСО/МЭК 15408-1 приложение D «Соответствие ПЗ».

ИСО/МЭК 15408-3 APE_CCL.1.11C: *«Изложение соответствия» должно содержать описание соответствия, требуемого любыми ПЗ/ЗБ данному профилю защиты в виде строгого или демонстрируемого соответствия.*

8.4.1.3.13 Шаг оценивания APE_CCL.1-13

Оценщик должен проверить, что изложение соответствия ПЗ содержит утверждение о строгом или демонстрируемом соответствии ПЗ.

8.5 Определение проблемы безопасности (APE_SPD)

8.5.1 Подвид деятельности по оценке (APE_SPD.1)

8.5.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, что проблема безопасности, которая должна решаться применением ОО и его средой функционирования, четко определена.

8.5.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.5.1.3 Действие APE_SPD.1.1E

ИСО/МЭК 15408-3 APE_SPD.1.1C: *«Определение проблемы безопасности» должно включать в себя описание угроз.*

8.5.1.3.1 Шаг оценивания APE_SPD.1-1

Оценщик должен проверить, что «Определение проблемы безопасности» описывает угрозы.

Если все цели безопасности получены из предположений и/или только из ПБОр, изложение угроз не обязательно должно присутствовать в ПЗ. В этом случае этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что «Определение проблемы безопасности» описывает угрозы, которым должен противостоять ОО и/или его среда функционирования.

ИСО/МЭК 15408-3 APE_SPD.1.2C: *Описание всех угроз должно проводиться в терминах источника угрозы, активов и негативного воздействия.*

8.5.1.3.2 Шаг оценивания APE_SPD.1-2

Оценщик должен исследовать «Определение проблемы безопасности», чтобы сделать заключение о том, что все угрозы описаны с указанием источника угрозы, негативного воздействия и активов.

Если все цели безопасности получены из предположений и/или только из ПБОр, изложение угроз не обязательно должно присутствовать в ПЗ. В этом случае этот шаг оценивания не применим и считается удовлетворенным.

Источники угрозы могут быть описаны более подробно с указанием таких аспектов, как уровень навыков и способностей нарушителя, доступные ему ресурсы, возможности и мотивация.

ИСО/МЭК 15408-3 APE_SPD.1.3C: *В «Определение проблемы безопасности» должно быть включено описание ПБОр.*

8.5.1.3.3 Шаг оценивания APE_SPD.1-3

Оценщик должен проверить, что «Определение проблемы безопасности» описывает ПБОр.

Если все цели безопасности получены из предположений и/или только из ПБОр, изложение угроз не обязательно должно присутствовать в ПЗ. В этом случае этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что изложения ПБОр сформулированы в терминах правил или руководств, которые должны выполняться ОО и/или его средой функционирования.

Оценщик делает заключение о том, что каждая ПБОр объясняется и/или интерпретируется достаточно подробно для её однозначного и ясного понимания; ясное представление изложений политик безопасности необходимо для возможности сопоставления их с целями безопасности.

ИСО/МЭК 15408-3 APE_SPD.1.4C: *«Определение проблемы безопасности» должно содержать описание предположений относительно среды функционирования ОО.*

8.5.1.3.4 Шаг оценивания APE_SPD.1-4

Оценщик должен исследовать «Определение проблемы безопасности», чтобы сделать заключение о том, что оно включает в себя описание предположений относительно среды функционирования ОО.

Если нет никаких предположений, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что каждое предположение относительно среды функционирования ОО объясняется достаточно подробно для того, чтобы пользователи могли сделать заключение

о том, соответствует ли их среда функционирования ОО данным предположениям. Если предположения неверно поняты, это может привести к тому, что ОО будет использоваться в среде функционирования, не обеспечивающей возможности его безопасного функционирования.

8.6 Цели безопасности (APE_OBJ)

8.6.1 Подвид деятельности по оценке (APE_OBJ.1)

8.6.1.1 Цели

Цель этого подвида деятельности — сделать заключение о том, четко ли определены цели безопасности для среды функционирования.

8.6.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.6.1.3 Действие APE_OBJ.1.1E

ИСО/МЭК 15408-3 APE_OBJ.1.1C: *Изложение «Целей безопасности» должно включать в себя описание целей безопасности для среды функционирования ОО.*

8.6.1.3.1 Шаг оценивания APE_OBJ.1-1

Оценщик должен проверить, определены ли в изложении «Целей безопасности» цели безопасности для среды функционирования ОО.

Оценщик проверяет, что цели безопасности для среды функционирования ОО однозначно идентифицированы.

8.6.2 Подвид деятельности по оценке (APE_OBJ.2)

8.6.2.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение, в полной ли мере и целесообразно ли «Цели безопасности» сопоставлены определению проблемы безопасности и четко ли определено разделение данной проблемы между ОО и его средой функционирования.

8.6.2.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.6.2.3 Действие APE_OBJ.2.1E

ИСО/МЭК 15408-3 APE_OBJ.2.1C: *Изложение «Целей безопасности» должно включать в себя описание целей безопасности для ОО и для среды функционирования ОО.*

8.6.2.3.1 Шаг оценивания APE_OBJ.2-1

Оценщик должен проверить, что изложение «Целей безопасности» определяет «Цели безопасности для ОО» и «Цели безопасности для среды функционирования ОО».

Оценщик проверяет, что обе категории «Целей безопасности» ясно идентифицированы и отделены друг от друга.

ИСО/МЭК 15408-3 APE_OBJ.2.2C: *В «Обосновании целей безопасности» каждая цель безопасности для ОО должна быть прослежена к угрозам, на противостояние которым направлена эта цель безопасности, и к ПБОр, на осуществление которых направлена эта цель безопасности.*

8.6.2.3.2 Шаг оценивания APE_OBJ.2-2

Оценщик должен проверить, что в «Обосновании целей безопасности» представлено прослеживание всех целей безопасности для ОО к угрозам, на противостояние которым направлены эти цели безопасности, и/или к ПБОр, на осуществление которых направлены эти цели.

Каждая цель безопасности для ОО может быть прослежена к угрозам или ПБОр или к комбинации угроз и ПБОр, но должна быть прослежена по крайней мере к одной угрозе или ПБОр.

Неудача при попытке такого прослеживания свидетельствует о том, что либо «Обоснование целей безопасности» является неполным, либо «Определение проблемы безопасности» является неполным, либо цель безопасности для ОО является бесполезной.

ИСО/МЭК 15408-3 APE_OBJ.2.3C: *В «Обосновании целей безопасности» каждая цель безопасности для ОО должна быть прослежена к угрозам, на противостояние которым направлена эта цель безопасности, к ПБОр, на осуществление которых направлена эта цель безопасности, а также к предположениям, поддерживаемым данной целью безопасности.*

8.6.2.3.3 Шаг оценивания APE_OBJ.2-3

Оценщик должен проверить, что в «Обосновании целей безопасности» представлено прослеживание каждой цели безопасности для среды функционирования к угрозам, на противостояние которым направлена эта цель безопасности, к ПБОр, на осуществление которых направлена эта цель безопасности, и к предположениям, поддерживаемым этой целью безопасности.

Каждая цель безопасности для среды функционирования ОО может быть прослежена к угрозам, ПБОр, предположениям или к комбинации угроз, ПБОр и/или предположений, но должна быть прослежена по крайней мере к одной угрозе, ПБОр или одному предположению.

Неудача при попытке такого прослеживания свидетельствует о том, что либо «Обоснование целей безопасности» является неполным, либо «Определение проблемы безопасности» является неполным, либо цель безопасности для среды функционирования является бесполезной.

ИСО/МЭК 15408-3 APE_OBJ.2.4C: *В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности направлены на противостояние всем идентифицированным угрозам.*

8.6.2.3.4 Шаг оценивания APE_OBJ.2-4

Оценщик должен исследовать «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждой угрозы приемлемое логическое обоснование того, что цели безопасности пригодны для противостояния данной угрозе.

Если ни одна цель безопасности не прослежена к конкретной угрозе, то результат данного шага оценивания отрицательный (выносится отрицательный вердикт).

Оценщик делает заключение, демонстрирует ли обоснование угрозы, что угроза устранена или снижена до приемлемого уровня, либо последствия её реализации в достаточной мере компенсированы.

Оценщик делает заключение, демонстрирует ли логическое обоснование для угрозы то, что цели безопасности достаточны: если все цели безопасности, прослеживаемые к угрозе, достигнуты, то угроза либо устранена, либо снижена до приемлемого уровня, либо последствия ее реализации в достаточной мере компенсированы.

Следует отметить, что прослеживание целей безопасности к угрозам в «Обосновании целей безопасности» может быть частью логического обоснования, но само по себе оно не является логическим обоснованием. Даже в том случае, когда цель безопасности является просто заявлением, отражающим намерение предотвратить реализацию конкретной угрозы, то все равно требуется логическое обоснование, хотя в этом случае оно может быть минимальным и иметь вид: «Цель безопасности X непосредственно противостоит Угрозе Y».

Оценщик также делает заключение, действительно ли каждая цель безопасности, которая прослежена к угрозе, является необходимой и при достижении вносит вклад в устранение, снижение или компенсацию последствий реализации данной угрозы.

ИСО/МЭК 15408-3 APE_OBJ.2.5C: *В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности направлены на осуществление всей ПБОр.*

8.6.2.3.5 Шаг оценивания APE_OBJ.2-5

Оценщик должен исследовать «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждой ПБОр логическое обоснование того, что цели безопасности пригодны для обеспечения осуществления данной ПБОр.

Если ни одна цель безопасности не прослежена к определенной ПБОр, то результат данного шага оценивания отрицательный (выносится отрицательный вердикт).

Оценщик делает заключение, демонстрирует ли логическое обоснование для ПБОр то, что цели безопасности достаточны: если все цели безопасности, прослеженные к этой ПБОр, достигнуты, то ПБОр реализована.

Оценщик также делает заключение, действительно ли каждая цель безопасности, которая прослежена к некоторой ПБОр, необходима и что она при достижении вносит вклад в реализацию ПБОр.

Следует отметить, что прослеживание целей безопасности к ПБОр в «Обосновании целей безопасности» может быть частью логического обоснования, но само по себе оно не является логическим обоснованием. Даже в том случае, когда цель безопасности является просто заявлением, отражающим намерение реализовать конкретную ПБОр, то все равно требуется логическое обоснование, хотя в этом случае оно может быть минимальным и иметь вид: «Цель безопасности X непосредственно обеспечивает осуществление ПБОр Y».

ИСО/МЭК 15408-3 APE_OBJ.2.6C: *В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности для среды функционирования поддерживают все предположения.*

8.6.2.3.6 Шаг оценивания APE_OBJ.2-6

Оценщик должен исследовать «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждого предположения для среды функционирования приемлемое логическое обоснование того, что цели безопасности для среды функционирования пригодны для обеспечения выполнения данного предположения.

Если ни одна цель безопасности для среды функционирования не прослежена к определенному предположению, то результат данного шага оценивания отрицательный (выносится отрицательный вердикт).

Оценщик делает заключение, демонстрирует ли логическое обоснование для предположения относительно среды функционирования ОО то, что цели безопасности достаточны: если все цели безопасности для среды функционирования, прослеженные к данному предположению, достигнуты, то среда функционирования обеспечивает выполнение предположения.

Оценщик также делает заключение, действительно ли каждая цель безопасности для среды функционирования, прослеживаемая к некоторому предположению относительно среды функционирования ОО, является необходимой и при достижении действительно вносит вклад в обеспечение выполнения средой функционирования этого предположения.

Следует отметить, что прослеживание целей безопасности для среды функционирования к предположениям в «Обосновании целей безопасности» может быть частью логического обоснования, но само по себе оно не является логическим обоснованием. Даже в том случае, когда цель безопасности для среды функционировании представляет собой просто перефразированное предположение, то все равно требуется логическое обоснование, хотя в этом случае оно может быть минимальным и иметь вид: «Цель безопасности X непосредственно поддерживает выполнение Предположения Y».

8.7 Определение расширенных компонентов (APE_ECD)

8.7.1 Подвид деятельности по оценке (APE_ECD.1)

8.7.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, определены ли расширенные компоненты ясно и однозначно и необходимы ли они, то есть не могут ли они быть ясно выражены с использованием существующих компонентов ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3.

8.7.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.7.1.3 Действие APE_ECD.1.1E

ИСО/МЭК 15408-3 APE_ECD.1.1C: *В изложении «Требований безопасности» должны быть идентифицированы все расширенные требования безопасности.*

8.7.1.3.1 Шаг оценивания APE_ECD.1-1

Оценщик должен проверить, что все требования безопасности в изложении «Требований безопасности», которые не идентифицированы как расширенные требования, присутствуют в ИСО/МЭК 15408-2 или в ИСО/МЭК 15408-3.

ИСО/МЭК 15408-3 APE_ECD.1.2C: *В «Определении расширенных компонентов» должен определяться расширенный компонент для каждого расширенного требования безопасности.*

8.7.1.3.2 Шаг оценивания APE_ECD.1-2

Оценщик должен проверить, что «Определение расширенных компонентов» определяет расширенный компонент для каждого расширенного требования безопасности.

Если ПЗ не содержит расширенные требования безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Один расширенный компонент может быть использован для определения многократно повторяющегося расширенного требования безопасности, не обязательно повторять это определение для каждой итерации данного требования.

ИСО/МЭК 15408-3 APE_ECD.1.3C: *В «Определении расширенных компонентов» должно указываться, как каждый расширенный компонент связан с существующими компонентами, семействами и классами ИСО/МЭК 15408.*

8.7.1.3.3 Шаг оценивания APE_ECD.1-3

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что оно описывает, как каждый расширенный компонент вписывается в существующие в стандарте ИСО/МЭК 15408 компоненты, семейства и классы.

Если ПЗ не содержит расширенные требования безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что каждый расширенный компонент является:

a) компонентом семейства ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, или

b) компонентом нового семейства, определенного в ПЗ.

Если расширенный компонент представляет собой компонент существующего семейства ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, оценщик делает заключение о том, что «Определение рас-

ширенных компонентов» в должной мере описывает, почему расширенному компоненту следует быть компонентом этого семейства и как он связан с другими компонентами семейства.

Если расширенный компонент представляет компонент нового семейства, определенного в ПЗ, оценщик подтверждает, что расширенный компонент не подходит ни к одному из существующих семейств.

Если в ПЗ определяются новые семейства, оценщик делает заключение о том, что каждое новое семейство является либо:

a) семейством существующего класса ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, или

b) семейством нового класса, определенного в ПЗ.

Если семейство представляет собой семейство класса ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, оценщик делает заключение о том, что «Определение расширенных компонентов» в достаточной мере описывает, почему семейству следует входить в этот класс и как оно связано с другими семействами этого класса.

Если семейство представляет собой семейство нового класса, определенного в ПЗ, оценщик подтверждает, что семейство не подходит ни к одному из существующих классов.

8.7.1.3.4 Шаг оценивания APE_ECD.1-4

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждое определение расширенного компонента идентифицирует все применимые зависимости этого компонента.

Если ПЗ не содержит расширенные требования безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик подтверждает, что никакие применимые зависимости не были пропущены автором ПЗ.

ИСО/МЭК 15408-3 APE_ECD.1.4C: *В «Определении расширенных компонентов» в качестве модели представления должны использоваться компоненты, семейства, классы и методология ИСО/МЭК 15408.*

8.7.1.3.5 Шаг оценивания APE_ECD.1-5

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждый расширенный функциональный компонент использует существующие компоненты ИСО/МЭК 15408-2 в качестве модели представления.

Если ПЗ не содержит расширенные функциональные требования безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что расширенный функциональный компонент согласуется с пунктом 6.1.3 «Структура компонента» ИСО/МЭК 15408-2.

Если в расширенном функциональном компоненте используются операции, оценщик делает заключение о том, что расширенный функциональный компонент согласуется с подразделом 7.1 «Операции» ИСО/МЭК 15408-1.

Если расширенный функциональный компонент находится в иерархической зависимости по отношению к существующему функциональному компоненту, оценщик делает заключение о том, что расширенный функциональный компонент согласуется с пунктом 6.2.1 «Выделение изменений в компоненте» ИСО/МЭК 15408-2.

8.7.1.3.6 Шаг оценивания APE_ECD.1-6

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждое определение нового функционального семейства использует существующие функциональные семейства ИСО/МЭК 15408 в качестве модели представления.

Если в ПЗ не определяются новые функциональные семейства, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что все новые функциональные семейства совместимы с пунктом 6.1.2 «Структура семейства» ИСО/МЭК 15408-2.

8.7.1.3.7 Шаг оценивания APE_ECD.1-7

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждое определение нового функционального класса использует существующие функциональные классы ИСО/МЭК 15408 в качестве модели представления.

Если в ПЗ не определяются новые функциональные классы, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что все новые функциональные классы согласуются с пунктом 6.1.1 «Структура класса» ИСО/МЭК 15408-2.

8.7.1.3.8 Шаг оценивания APE_ECD.1-8

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждое определение расширенного компонента требований доверия использует существующие компоненты ИСО/МЭК 15408-3 в качестве модели представления.

Если в ПЗ не содержатся расширенные требования доверия к безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что «Определение расширенных компонентов» согласуется с пунктом 6.1.3 «Структура компонента» ИСО/МЭК 15408-3.

Если в расширенном компоненте доверия используются операции, оценщик делает заключение о том, что расширенный компонент доверия согласуется с подразделом 7.1 «Операции» ИСО/МЭК 15408-1.

Если расширенный компонент доверия находится в иерархической зависимости по отношению к существующему компоненту доверия, оценщик делает заключение о том, что расширенный компонент доверия согласуется с пунктом 6.1.3 «Структура компонента» ИСО/МЭК 15408-3.

8.7.1.3.9 Шаг оценивания APE_ECD.1-9

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что, для каждого определенного расширенного компонента доверия предоставлена соответствующая методология.

Если ПЗ не содержит расширенные требования доверия к безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что для каждого элемента действий оценщика по каждому расширенному ТДБ представлены один или более шагов оценивания, и что успешное выполнение всех шагов оценивания для данного элемента действий оценщика продемонстрирует, что элемент был выполнен.

8.7.1.3.10 Шаг оценивания APE_ECD.1-10

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждое определение нового семейства доверия использует существующие семейства доверия ИСО/МЭК 15408 в качестве модели представления.

Если в ПЗ не определяются новые семейства доверия, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что все новые семейства доверия совместимы с пунктом 6.1.2 «Структура семейства» ИСО/МЭК 15408-3.

8.7.1.3.11 Шаг оценивания APE_ECD.1-11

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждое определение нового класса доверия использует существующие классы доверия ИСО/МЭК 15408 в качестве модели представления.

Если в ПЗ не определяются новые классы доверия, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что все новые классы доверия согласуются с пунктом 6.1.1 «Структура класса» ИСО/МЭК 15408-3.

ИСО/МЭК 15408-3 APE_ECD.1.5C: *Расширенные компоненты должны состоять из измеримых объективных элементов, чтобы была возможность продемонстрировать соответствие или несоответствие этим элементам.*

8.7.1.3.12 Шаг оценивания APE_ECD.1-12

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждый элемент в каждом расширенном компоненте измерим и излагает объективные требования оценки, чтобы была возможность продемонстрировать соответствие или несоответствие этим элементам.

Если ПЗ не содержит расширенные требования безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что элементы расширенных функциональных компонентов изложены таким способом, что их можно протестировать и проследить к соответствующим представлениям ФБО.

Оценщик также делает заключение о том, что для элементов расширенных компонентов доверия не требуется субъективное суждение оценщика.

Оценщику следует помнить, что хотя требование измеримости и объективности применимо для всех критериев оценки, однако считается, что нет формального метода доказательства таких свойств. Поэтому существующие функциональные компоненты и компоненты доверия в ИСО/МЭК

15408 должны использоваться в качестве модели для определения того, что составляет соответствие этому требованию.

8.7.1.4 Действие APE_ECD.1.2E

8.7.1.4.1 Шаг оценивания APE_ECD.1-13

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждый расширенный компонент не может быть четко выражен при использовании существующих компонентов.

Если ПЗ не содержит расширенные требования доверия к безопасности, этот шаг оценивания не применим, и считается удовлетворенным.

Оценщику при вынесении данного заключения следует принимать во внимание компоненты ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3, другие расширенные компоненты, которые были определены в ПЗ, комбинации этих компонентов, возможные операции над этими компонентами.

Оценщику следует помнить, что роль этого шага оценивания заключается в устранении ненужного дублирования компонентов в случае, если эти компоненты могут быть ясно выражены при помощи других компонентов. Оценщику не следует предпринимать исчерпывающий поиск всех возможных комбинаций компонентов, включая операции, пытаясь найти способ выразить расширенный компонент при помощи существующих компонентов.

8.8 Требования безопасности (APE_REQ)

8.8.1 Подвид деятельности по оценке (APE_REQ.1)

8.8.1.1 Цели

Цель этого подвида деятельности — сделать заключение, является ли описание требований безопасности (как функциональных требований безопасности, так и требований доверия к безопасности) четким, недвусмысленным, полным и внутренне непротиворечивым.

8.8.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.8.1.3 Действие APE_REQ.1.1E

ИСО/МЭК 15408-3 APE_REQ.1.1C: *Изложение «Требований безопасности» должно содержать описание ФТБ и ТДБ.*

8.8.1.3.1 Шаг оценивания APE_REQ.1-1

Оценщик должен проверить, что изложение «Требований безопасности» описывает функциональные требования безопасности.

Оценщик делает заключение о том, что каждое ФТБ идентифицировано одним из следующих способов:

a) ссылкой на конкретный компонент ИСО/МЭК 15408-2;
b) ссылкой на расширенный компонент в «Определении расширенных компонентов» ПЗ;
c) ссылкой на ПЗ, о соответствии с которым утверждается в ПЗ;
d) ссылкой на пакет требований безопасности, о соответствии с которым утверждается в ПЗ;
e) с помощью воспроизведения в ПЗ.

Не обязательно использовать одинаковые способы идентификации для всех ФТБ.

8.8.1.3.2 Шаг оценивания APE_REQ.1-2

Оценщик должен проверить, что изложение «Требований безопасности» описывает требования доверия к безопасности.

Оценщик делает заключение о том, что каждое ТДБ идентифицировано одним из следующих способов:

a) ссылкой на конкретный компонент ИСО/МЭК 15408-3;
b) ссылкой на расширенный компонент в «Определении расширенных компонентов» ПЗ;
c) ссылкой на ПЗ, о соответствии с которым утверждается в ПЗ;
d) ссылкой на пакет требований безопасности, о соответствии с которым утверждается в ПЗ;
e) с помощью воспроизведения отображения в ПЗ.

Не обязательно использовать одинаковые способы идентификации для всех ТДБ.

ИСО/МЭК 15408-3 APE_REQ.1.2C: *Все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, используемые в ФТБ и ТДБ, должны быть определены.*

8.8.1.3.3 Шаг оценивания APE_REQ.1-3

Оценщик должен исследовать ПЗ для того, чтобы сделать заключение о том, что все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, используемые в ФТБ и ТДБ, определены.

Оценщик делает заключение о том, что ПЗ определяет все:

- субъекты и объекты (их типы), которые используются в ФТБ;
- атрибуты безопасности (их типы) субъектов, пользователей, объектов, информации, сеансов и/или ресурсов, возможные значения, которые могут принимать данные атрибуты и любые отношения между этими значениями (например «Совершенно секретно» выше, чем «Секретно»);
- операции (их типы), которые используются в ФТБ, включая результаты выполнения этих операций;
- типы внешних сущностей в ФТБ;
- прочие элементы, которые введены в ФТБ и/или ТДБ путем выполнения операций, если эти элементы не являются ясными без дополнительного объяснения или используются вне их словарных значений.

Цель этого шага оценивания состоит в том, чтобы удостовериться, что ФТБ и ТДБ были четко определены и что не может произойти их неправильного понимания из-за употребления неопределенных терминов. При выполнении этого шага оценивания не следует доходить до крайностей, вынуждая автора ПЗ определять каждое слово. Предполагается, что у широкой аудитории, на которую рассчитан набор требований безопасности, есть понимание ИТ в целом, основ информационной безопасности и знание «Критериев оценки безопасности информационных технологий».

Все вышеупомянутое может быть представлено по группам, классам, ролям, типам или другим классификациям и спецификациям, облегчающим понимание.

Оценщику следует помнить, что эти списки и определения не должны быть частью изложения «Требований безопасности», но могут быть размещены (частично или полностью) в различных подразделах оного. Это может быть особенно полезным, если эти же элементы используются в остальной части ПЗ.

ИСО/МЭК 15408-3 APE_REQ.1.3C: *В изложении «Требований безопасности» должны быть идентифицированы все выполняемые над требованиями безопасности операции.*

8.8.1.3.4 Шаг оценивания APE_REQ.1-4

Оценщик должен проверить, идентифицированы ли все операции над требованиями безопасности в изложении «Требований безопасности».

Оценщик делает заключение, все ли операции (это относится и к завершенным и незавершенным операциям) идентифицированы в каждом ФТБ и ТДБ, где они используются. Идентификация может проводиться различными способами, например путем введения типографических различий, особого выделения в сопутствующем тексте или других средств различия.

ИСО/МЭК 15408-3 APE_REQ.1.4C: *Все операции должны выполняться правильно.*

8.8.1.3.5 Шаг оценивания APE_REQ.1-5

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «назначение» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

8.8.1.3.6 Шаг оценивания APE_REQ.1-6

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «итерация» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

8.8.1.3.7 Шаг оценивания APE_REQ.1-7

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «выбор» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

8.8.1.3.8 Шаг оценивания APE_REQ.1-8

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «уточнение» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

ИСО/МЭК 15408-3 APE_REQ.1.5C: *Каждая зависимость от «Требований безопасности» должна быть либо удовлетворена, либо должно приводиться обоснование неудовлетворения данной зависимости.*

8.8.1.3.9 Шаг оценивания APE_REQ.1-9

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что каждая зависимость требований безопасности или удовлетворена или приведено обоснование неудовлетворения данной зависимости.

Зависимость удовлетворяется включением соответствующего компонента (или того, который является иерархическим к нему) в изложение «Требований безопасности». Компонент, используемый для удовлетворения зависимости, при необходимости следует изменить операциями, чтобы обеспечить удовлетворение зависимости.

В логическом обосновании того, что зависимость не удовлетворена, следует указывать либо:

a) почему зависимость не является полезной или необходимой, в этом случае не требуется предоставлять дополнительную информацию; либо

b) что зависимость обеспечивается средой функционирования ОО, в этом случае в логическое обоснование следует включить описание того, как цели безопасности для среды функционирования обеспечивают выполнение этой зависимости.

ИСО/МЭК 15408-3 APE_REQ.1.6C: *Изложение «Требований безопасности» должно быть внутренне непротиворечивым.*

8.8.1.3.10 Шаг оценивания APE_REQ.1-10

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что оно внутренне непротиворечиво.

Оценщик делает заключение о том, является ли объединенный набор всех ФТБ и ТДБ внутренне непротиворечивым.

Оценщик делает заключение о том, что во всех случаях, когда различные требования безопасности применяются к одним и тем же типам свидетельств разработчика, событий, операций, данных, необходимых тестирований и т. д. или ко «всем объектам», «всем субъектам» и т. д., эти требования не противоречат друг другу.

Некоторые примеры возможных конфликтов:

a) расширенное ТДБ определяет, что проект некоторого криптографического алгоритма должен содержаться в секрете, а другое расширенное ТДБ предписывает свободный доступ к просмотру его исходных кодов;

b) компонент FAU_GEN.1 «Генерация данных аудита безопасности» определяет, что идентификатор субъекта должен регистрироваться в журнале; компонент FDP_ACC.1 «Ограниченное управление доступом» определяет, кто имеет права доступа к этим журналам, а компонент FPR_UNO.1 «Скрытность» определяет, что не рекомендуется, чтобы некоторые действия субъектов были доступны для просмотра другим субъектам. Если субъект, которому не следует иметь возможность видеть действия других субъектов, может получить доступ к журналам регистрации данных действий, эти ФТБ являются конфликтующими;

c) в компоненте FDP_RIP.1 «Ограниченная защита остаточной информации» указывается, что удаление остаточной информации более не требуется, а в компоненте FDP_ROL.1 «Базовый откат» определяется, что ОО может быть возвращен к предыдущему состоянию. Если информация, которая необходима для отката к предыдущему состоянию, была удалена, эти требования являются конфликтующими;

d) многократные итерации компонента FDP_ACC.1 «Ограниченное управление доступом», особенно если некоторые итерации касаются одних и тех же субъектов, объектов или операций. Если одно ФТБ по управлению доступом позволяет субъекту выполнять операцию над объектом, тогда как другое ФТБ по управлению доступом не позволяет это, эти требования являются конфликтующими.

8.8.2 Подвид деятельности по оценке (APE_REQ.2)

8.8.2.1 Цели

Цель этого подвида деятельности — сделать заключение, являются ли описание требований безопасности (как функциональных требований безопасности, так и требований доверия к безопасности) четким, недвусмысленным, полным и внутренне непротиворечивым и соответствуют ли ФТБ целям безопасности ОО.

8.8.2.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.8.2.3 Действие APE_REQ.2.1E

ИСО/МЭК 15408-3 APE_REQ.2.1C: *Изложение «Требований безопасности» должно содержать описание ФТБ и ТДБ.*

8.8.2.3.1 Шаг оценивания APE_REQ.2-1

Оценщик должен проверить, что изложение «Требований безопасности» содержит описание функциональных требований безопасности.

Оценщик делает заключение о том, что каждое ФТБ идентифицировано одним из следующих способов:

a) ссылкой на конкретный компонент ИСО/МЭК 15408-2;

b) ссылкой на расширенный компонент в «Определении расширенных компонентов» ПЗ;

c) ссылкой на конкретный компонент ПЗ, о соответствии с которым утверждается в ПЗ;

d) ссылкой на конкретный компонент в пакете требований безопасности, о соответствии с которым утверждается в ПЗ;

e) с помощью воспроизведения в ПЗ.

Не обязательно использовать одинаковые способы идентификации для всех ФТБ.

8.8.2.3.2 Шаг оценивания APE_REQ.2-2

Оценщик должен проверить, что изложение «Требований безопасности» содержит описание требований доверия к безопасности.

Оценщик делает заключение о том, что каждое ТДБ идентифицировано одним из следующих способов:

a) ссылкой на конкретный компонент ИСО/МЭК 15408-3;

b) ссылкой на расширенный компонент в «Определении расширенных компонентов» ПЗ;

c) ссылкой на конкретный компонент ПЗ, о соответствии с которым утверждается в ПЗ;

d) ссылкой на конкретный компонент в пакете требований безопасности, о соответствии с которым утверждается в ПЗ;

e) с помощью воспроизведения в ПЗ.

Не обязательно использовать одинаковые способы идентификации для всех ТДБ.

ИСО/МЭК 15408-3 APE_REQ.2.2C: *Все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, используемые в ФТБ и ТДБ, должны быть определены.*

8.8.2.3.3 Шаг оценивания APE_REQ.2-3

Оценщик должен исследовать ПЗ для того, чтобы сделать заключение о том, что все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, используемые в ФТБ и ТДБ, определены.

Оценщик делает заключение о том, что ПЗ определяет все:

- субъекты и объекты (их типы), используемые в ФТБ;
- атрибуты безопасности субъектов (их типы), пользователей, объектов, информации, сеансов и/или ресурсов, возможные значения, которые могут принимать данные атрибуты и любые отношения между этими значениями (например «Совершенно секретно» выше, чем «Секретно»);
- операции (их типы), которые используются в ФТБ, включая результаты выполнения этих операций;
- внешние сущности (их типы) в ФТБ;
- прочие понятия, которые введены в ФТБ и ТДБ путем выполнения операций, если эти понятия не являются ясными без дополнительного объяснения или используются вне их словарных значений.

Цель этого шага оценивания состоит в том, чтобы удостовериться, что ФТБ и ТДБ четко определены и что не может произойти их неправильного понимания из-за употребления неопределенных терминов. При выполнении этого шага оценивания не следует доходить до крайностей, вынуждая автора ПЗ определять каждое слово. Предполагается, что у широкой аудитории, на которую рассчитан набор требований безопасности, есть понимание ИТ в целом, основ информационной безопасности и знание «Критериев оценки безопасности информационных технологий».

Все вышеупомянутое может быть представлено по группам, классам, ролям, типам или другим классификациям и спецификациям, облегчающим понимание.

Оценщику следует помнить, что эти списки и определения не должны быть частью изложения «Требований безопасности», но могут быть размещены (частично или полностью) в различных подпунктах оного. Это может быть особенно полезным, если эти же понятия используются в остальной части ПЗ.

ИСО/МЭК 15408-3 APE_REQ.2.3C: *В изложении «Требований безопасности» должны быть идентифицированы все операции над требованиями безопасности.*

8.8.2.3.4 Шаг оценивания APE_REQ.2-4

Оценщик должен проверить, идентифицированы ли все операции над требованиями безопасности в изложении «Требований безопасности».

Оценщик делает заключение, все ли операции (это относится и к завершенным и незавершенным) идентифицированы в каждом ФТБ и ТДБ, где они используются. Идентификация может проводиться различными способами, например путем введения типографических различий, особого выделения в сопутствующем тексте или других средств различия.

ИСО/МЭК 15408-3 APE_REQ.2.4C: *Все операции должны быть выполнены правильно.*

8.8.2.3.5 Шаг оценивания APE_REQ.2-5

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «назначение» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

8.8.2.3.6 Шаг оценивания APE_REQ.2-6

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «итерация» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

8.8.2.3.7 Шаг оценивания APE_REQ.2-7

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «выбор» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

8.8.2.3.8 Шаг оценивания APE_REQ.2-8

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «уточнение» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

ИСО/МЭК 15408-3 APE_REQ.2.5C: *Каждая зависимость от «Требований безопасности» должна быть либо удовлетворена, либо должно приводиться обоснование неудовлетворения зависимости.*

8.8.2.3.9 Шаг оценивания APE_REQ.2-9

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что каждая зависимость требований безопасности или удовлетворена или приведено обоснование неудовлетворения зависимости.

Зависимость удовлетворена включением соответствующего компонента (или того, который является иерархическим к нему) в изложение «Требований безопасности». Компонент, используемый для удовлетворения зависимости, при необходимости следует изменить операциями, чтобы обеспечить удовлетворение зависимости.

В логическом обосновании того, что зависимость не удовлетворена, следует указать либо:

a) почему зависимость не является полезной или необходимой, в этом случае не требуется предоставлять дополнительную информацию; либо

b) что зависимость обеспечивается средой функционирования ОО. В этом случае в логическое обоснование следует включить описание того, как цели безопасности для среды функционирования обеспечивают выполнение этой зависимости.

ИСО/МЭК 15408-3 APE_REQ.2.6C: *В «Обосновании требований безопасности» должно быть представлено прослеживание соответствия каждого ФТБ к целям безопасности для ОО.*

8.8.2.3.10 Шаг оценивания APE_REQ.2-10

Оценщик должен проверить, прослежено ли каждое функциональное требование безопасности в «Обосновании требований безопасности» к целям безопасности для ОО.

Оценщик делает заключение, прослежено ли каждое функциональное требование безопасности по крайней мере к одной цели безопасности для ОО.

Неудача при попытке такого прослеживания означает, что либо «Обоснование требований безопасности» является неполным, либо «Цели безопасности» для ОО являются неполными, либо функциональное требование безопасности является бесполезным.

ИСО/МЭК 15408-3 APE_REQ.2.7C: *В «Обосновании требований безопасности» должно быть продемонстрировано, что ФТБ обеспечивают выполнение всех целей безопасности для ОО.*

8.8.2.3.11 Шаг оценивания APE_REQ.2-11

Оценщик должен исследовать «Обоснование требований безопасности», чтобы сделать заключение, содержится ли в нем для каждой цели безопасности для ОО логическое обоснование того, что ФТБ пригодны для достижения данной цели безопасности для ОО.

Если никакие ФТБ не прослежены к определенной цели безопасности для ОО, то результат данного шага оценивания отрицательный (выносится отрицательный вердикт).

Оценщик делает заключение, демонстрирует ли «Обоснование целей безопасности» для ОО то, что ФТБ достаточны: если все ФТБ, прослеженные к определенной цели безопасности ОО, выполняются, то цель безопасности для ОО достигнута.

Если в ФТБ, прослеженных к цели безопасности для ОО, есть какие-либо незавершенные операции назначения или незавершенные/неполные операции выбора, оценщик делает заключение о том, что для каждого возможного завершения операции или для комбинации завершений этих операций цель безопасности достигается.

Оценщик также делает заключение, действительно ли каждое ФТБ, прослеженное к некоторой цели безопасности для ОО, необходимо и при выполнении оно фактически вносит вклад в достижение данной цели безопасности.

Следует отметить, что прослеживание от ФТБ к целям безопасности для ОО, представленное в «Обосновании требований безопасности», может быть частью логического обоснования, но само по себе оно не является логическим обоснованием.

ИСО/МЭК 15408-3 APE_REQ.2.8C: *В «Обосновании требований безопасности» должно приводиться пояснение того, почему выбраны определенные ТДБ.*

8.8.2.3.12 Шаг оценивания APE_REQ.2-12

Оценщик должен проверить, что «Обоснование требований безопасности» объясняет, почему выбраны определенные ТДБ.

Оценщику следует помнить, что любое объяснение правильно, пока оно составлено четко и ясно, и ни в ТДБ, ни в объяснении нет очевидных несогласованностей с прочими частями ПЗ.

Пример очевидной несогласованности между ТДБ и остальными частями ПЗ — когда имеются источники угроз, обладающие большими возможностями, но ТДБ в семействе AVA_VAN не обеспечивают защиту от этих источников угроз.

ИСО/МЭК 15408-3 APE_REQ.2.9C: *Изложение «Требований безопасности» должно быть внутренне непротиворечивым.*

8.8.2.3.13 Шаг оценивания APE_REQ.2-13

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение, что оно внутренне непротиворечиво.

Оценщик делает заключение о том, является ли объединенный набор всех ФТБ и ТДБ внутренне непротиворечивым.

Оценщик делает заключение о том, что во всех случаях, когда различные требования безопасности применяются к одним и тем же типам свидетельств разработчика, событий, операций, данных, необходимых тестирований и т. д. или ко «всем объектам», «всем субъектам» и т. д., эти требования не противоречат друг другу.

Некоторые примеры возможных конфликтов:

a) расширенное ТДБ определяет, что проект некоторого криптографического алгоритма должен содержаться в секрете, а другое расширенное ТДБ предписывает свободный доступ к просмотру его исходных кодов;

b) компонент FAU_GEN.1 «Генерация данных аудита безопасности» определяет, что идентификатор субъекта должен регистрироваться в журнале; компонент FDP_ACC.1 «Ограниченное управление доступом» определяет, кто имеет права доступа к этим журналам, а компонент FPR_UNO.1 «Скрытность» определяет, что не рекомендуется, чтобы некоторые действия субъектов были доступны для просмотра другим субъектам. Если субъект, которому не следует иметь возможность видеть действия других субъектов, может получить доступ к журналам регистрации данных действий, эти ФТБ являются конфликтующими;

c) в компоненте FDP_RIP.1 «Ограниченная защита остаточной информации» указывается, что удаление остаточной информации более не требуется, а в компоненте FDP_ROL.1 «Базовый откат» определяется, что ОО может быть возвращен к предыдущему состоянию. Если информация, которая необходима для отката к предыдущему состоянию, была удалена, эти требования являются конфликтующими;

d) многократные итерации компонента FDP_ACC.1 «Ограниченное управление доступом» особенно, если некоторые итерации касаются одних и тех же субъектов, объектов или операций. Если одно ФТБ по управлению доступом позволяет субъекту выполнять операцию над объектом, тогда как другое ФТБ по управлению доступом не позволяет это, эти требования являются конфликтующими.

9 Класс ASE: Оценка задания по безопасности

9.1 Введение

Этот раздел описывает оценку ЗБ. Оценку ЗБ следует начинать до начала каких-либо других подвидов деятельности по оценке ОО, так как ЗБ является основой и определяет условия выполнения данных подвидов деятельности.

Методология оценки в этом разделе основана на требованиях к ЗБ, определенных в классе ASE «Оценка ЗБ» из ИСО/МЭК 15408-3.

Данный раздел следует использовать вместе с приложениями A, B и C в ИСО/МЭК 15408-1, поскольку в этих приложениях разъясняются приведенные здесь понятия и приводятся многочисленные примеры.

9.2 Замечания по применению

9.2.1 Использование результатов оценки сертифицированных ПЗ

При осуществлении оценки ЗБ, которое основано на одном или нескольких сертифицированных ПЗ, есть возможность использовать тот факт, что данные ПЗ были сертифицированы. Возможность повторного использования результата оценки сертифицированных ПЗ больше, если оцениваемое ЗБ не добавляет угроз, ПБОр, предположений, целей и/или требований безопасности этим ПЗ. Если в ЗБ содержится намного больше угроз, ПБОр, предположений, целей и/или требований безопасности, чем в сертифицированном ПЗ, повторное использование результатов сертификации может вообще быть бесполезным.

Оценщику разрешается повторно использовать результаты оценки ПЗ, выполняя определенные исследования только частично или вовсе не выполняя их, если эти исследования или их части были проведены в рамках оценки ПЗ. Делая это, оценщику следует предположить, что анализ ПЗ был проведен правильно.

Примером может служить случай, когда ПЗ содержит набор требований безопасности, и по ним в процессе оценки ПЗ было получено заключение, что они являются внутренне непротиворечивыми. Если в ЗБ используются эти же требования, анализ непротиворечивости не обязательно повторно проводить во время оценки ЗБ. Если же ЗБ добавляет одно или более требований или выполняет операции над этими требованиями, анализ необходимо повторить. Однако есть возможность сократить объем работ при анализе непротиворечивости, используя тот факт, что исходные требования внутренне непротиворечивы. Если исходные требования внутренне непротиворечивы, оценщик должен только сделать заключение о том, что:

a) набор новых и/или измененных требований внутренне непротиворечив, и

b) набор всех новых и/или измененных требований не противоречит исходным требованиям.

Оценщик отмечает в ТОО каждый случай, где исследования не сделаны или сделаны только частично по этой причине.

9.3 Введение ЗБ (ASE_INT)

9.3.1 Подвид деятельности по оценке (ASE_INT.1)

9.3.1.1 Цели

Цель этого подвида деятельности — сделать заключение о том, правильно ли идентифицированы ЗБ и ОО, правильно ли описан ОО по трем уровням представления («Ссылка на ОО», «Аннотация ОО» и «Описание ОО») и согласованы ли данные описания друг с другом.

9.3.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.3.1.3 Действие ASE_INT.1.1E

ИСО/МЭК 15408-3 ASE_INT.1.1C: *«Введение ЗБ» должно содержать «Ссылку на ЗБ», «Ссылку на ОО», «Аннотацию ОО» и «Описание ОО».*

9.3.1.3.1 Шаг оценивания ASE_INT.1-1

Оценщик должен проверить, содержит ли «Введение ЗБ» «Ссылку на ЗБ», «Ссылку на ОО», «Аннотацию ОО» и «Описание ОО».

ИСО/МЭК 15408-3 ASE_INT.1.2C: *«Ссылка на ЗБ» должна однозначно идентифицировать ЗБ.*

9.3.1.3.2 Шаг оценивания ASE_INT.1-2

Оценщик должен исследовать «Ссылку на ЗБ», чтобы сделать заключение о том, уникально ли в ней идентифицировано ЗБ.

Оценщик делает заключение о том, что «Ссылка на ЗБ» идентифицирует ЗБ так, чтобы его можно было легко отличить от других ЗБ, и что она также уникально идентифицирует каждую версию ЗБ, например благодаря включению номера версии и/или даты публикации.

При проведении оценок с использованием системы управления конфигурацией, оценщик может проверить уникальность ссылки путем проверки списка конфигурации. В других случаях в ЗБ рекомендуется наличие некоторой системы ссылок с поддержкой уникальных ссылок (например с использованием номеров, букв или даты публикации).

ИСО/МЭК 15408-3 ASE_INT.1.3C: *«Ссылка на ОО» должна однозначно идентифицировать ОО.*

9.3.1.3.3 Шаг оценивания ASE_INT.1-3

Оценщик должен исследовать «Ссылку на ОО», чтобы сделать заключение о том, что она однозначно идентифицирует ОО.

Оценщик выносит заключение о том, что «Ссылка на ОО» идентифицирует ОО так, что ясно, к какому ОО относится ЗБ, и что она идентифицирует версию ОО, например благодаря включению номера версии/даты выпуска/создания.

9.3.1.3.4 Шаг оценивания ASE_INT.1-4

Оценщик должен исследовать «Ссылку на ОО», чтобы сделать заключение о том, что она не вводит в заблуждение.

Если ОО связан с одним или более широко известными продуктами, допускается отразить этот факт в «Ссылке на ОО». Однако это не следует использовать для введения пользователей в заблуждение: не позволяется допускать ситуации, когда в «Ссылке на ОО» не отражено, что оценена только небольшая часть продукта.

ИСО/МЭК 15408-3 ASE_INT.1.4C: *В «Аннотации ОО» должна быть представлена краткая информация о его использовании и основных функциональных возможностях безопасности ОО.*

9.3.1.3.5 Шаг оценивания ASE_INT.1-5

Оценщик должен исследовать «Аннотацию ОО», чтобы сделать заключение о том, что она описывает использование и основные характеристики безопасности ОО.

В «Аннотации ОО» следует приводить краткое (несколько параграфов) описание использования ОО и основные характеристики безопасности ОО. Рекомендуется, чтобы «Аннотация ОО» предоставляла потенциальным пользователям возможность быстро сделать заключение о том, подходит ли данный ОО их потребностям в безопасности.

В «Аннотации ОО» в ЗБ для составных ОО следует представить описание использования и основных характеристик безопасности для составного ОО, а не для отдельных ОО в его составе.

Оценщик делает заключение о том, является ли аннотация достаточно ясной для пользователей ОО и достаточной для получения ими общего понимания назначения ОО и его основных характеристик безопасности.

ИСО/МЭК 15408-3 ASE_INT.1.5C: *В «Аннотации ОО» должен быть идентифицирован тип ОО.*

9.3.1.3.6 Шаг оценивания ASE_INT.1-6

Оценщик должен проверить, идентифицирован ли в «Аннотации ОО» тип ОО.

9.3.1.3.7 Шаг оценивания ASE_INT.1-7

Оценщик должен исследовать «Аннотацию ОО», чтобы сделать заключение о том, что тип ОО не вводит в заблуждение.

Случаются ситуации, когда пользователь ожидает от ОО наличия определенных функциональных возможностей из-за того, что ОО относится к тому или иному типу. Если эти функциональные возможности отсутствуют в ОО, оценщик делает заключение о том, что в «Аннотации ОО» в достаточной мере поясняется отсутствие данных функциональных возможностей.

Пользователь также может ожидать, что ОО способен работать в определенной среде функционирования из-за того, что ОО относится к тому или иному типу. Если ОО не может работать в такой среде функционирования, оценщик делает заключение о том, что это в достаточной мере поясняется в «Аннотации ОО».

ИСО/МЭК 15408-3 ASE_INT.1.6C: *В «Аннотации ОО» должны быть идентифицированы любые не входящие в ОО аппаратные, программные, а также программно-аппаратные средства, требуемые ОО.*

9.3.1.3.8 Шаг оценивания ASE_INT.1-8

Оценщик должен исследовать «Аннотацию ОО», чтобы сделать заключение о том, что в ней идентифицированы любые не входящие в ОО аппаратные, программные, программно-аппаратные средства, требуемые ОО.

В то время как некоторые ОО являются автономными, другим ОО (особенно если ОО является программным средством) для работы необходимы дополнительные аппаратные, программные или программно-аппаратные средства. Если ОО не требуется каких-либо аппаратных, программных, программно-аппаратных средств, этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что в «Аннотации ОО» идентифицированы все аппаратные/программные/программно-аппаратные средства, которые необходимы для функционирования ОО. Это перечисление не обязательно должно быть исчерпывающим, но должно быть достаточно подробным для того, чтобы потенциальные пользователи ОО могли определить, могут ли имеющиеся у них аппаратные, программные, программно-аппаратные средства поддерживать использование данного ОО, и если нет, то какие дополнительные аппаратные, программные, программно-аппаратные средства для этого требуются.

ИСО/МЭК 15408-3 ASE_INT.1.7C: *«Описание ОО» должно включать описание физических границ ОО.*

9.3.1.3.9 Шаг оценивания ASE_INT.1-9

Оценщик должен исследовать «Описание ОО», чтобы сделать заключение о том, что оно включает описание физических границ ОО.

Оценщик делает заключение о том, что «Описание ОО» содержит перечисление аппаратных, программных, программно-аппаратных средств и части руководств, которые составляют ОО, и содержит их описание на уровне детализации, достаточном для того, чтобы предоставить читателю общее понимание об этих частях ОО.

Оценщик также делает заключение о том, что не может возникнуть недопонимание относительно того, являются ли какие-либо аппаратные, программные, программно-аппаратные средства, а также части руководств составной частью ОО или же не являются.

ИСО/МЭК 15408-3 ASE_INT.1.8C: *«Описание ОО» должно включать описание логических границ ОО.*

9.3.1.3.10 Шаг оценивания ASE_INT.1-10

Оценщик должен исследовать «Описание ОО», чтобы сделать заключение о том, что оно включает описание логических границ ОО.

Оценщик делает заключение о том, что в «Описании ОО» указываются логические характеристики безопасности, предлагаемые ОО, на достаточном уровне детализации для того, чтобы предоставить читателю общее понимание этих характеристик.

Оценщик также делает заключение о том, что не может возникнуть недопонимание относительно того, присуща ли та или иная логическая характеристика безопасности данному ОО или нет.

ЗБ для составного ОО может ссылаться на представленное в ЗБ для ОО-компонентов описание их логических границ для предоставления большей части описания составного ОО. Однако оценщик делает заключение о том, что в ЗБ составного ОО ясно указывается, какие характеристики отдельных компонентов не включаются в составной ОО и потому не являются его характеристиками.

9.3.1.4 Действие ASE_INT.1.2E

9.3.1.4.1 Шаг оценивания ASE_INT.1-11

Оценщик должен исследовать «Ссылку на ОО», «Аннотацию ОО» и «Описание ОО» для того, чтобы сделать заключение, согласуются ли они друг с другом.

9.4 Утверждения о соответствии (ASE_CCL)

9.4.1 Подвид деятельности по оценке (ASE_CCL.1)

9.4.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы определить правомерность различных утверждений о соответствии. Он описывает, каким образом ЗБ и ОО соответствует ИСО/МЭК 15408, и как ЗБ соответствует ПЗ и пакетам требований.

9.4.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности являются:

a) ЗБ;

b) другие ПЗ, о соответствии которым утверждается в ЗБ;

c) пакеты требований, о соответствии которым утверждается в ЗБ.

9.4.1.3 Действие ASE_CCL.1.1E

ИСО/МЭК 15408-3 ASE_CCL.1.1C: *В «Утверждения о соответствии» должно быть включено «Утверждение о соответствии ИСО/МЭК 15408», которое определяет, для какой редакции ИСО/МЭК 15408 утверждается соответствие ЗБ и ОО.*

9.4.1.3.1 Шаг оценивания ASE_CCL.1-1

Оценщик должен проверить, что в «Утверждении о соответствии» включено «Утверждение о соответствии ИСО/МЭК 15408», которое определяет, для какой редакции ИСО/МЭК 15408 утверждается о соответствии в ЗБ и ОО.

Оценщик делает заключение о том, что в «Утверждении о соответствии ИСО/МЭК 15408» идентифицируется редакция ИСО/МЭК 15408, которая использовалась для разработки данного ЗБ. В «Утверждение» следует включать номер редакции ИСО/МЭК 15408 и, если не использовалась международная редакция стандарта ИСО/МЭК 15408 на английском языке, то в нем должен быть указан язык используемой редакции ИСО/МЭК 15408.

Для составного ОО оценщик должен рассмотреть любые отличия между редакцией ИСО/МЭК 15408, о соответствии которой утверждается в ОО-компоненте, и редакцией ИСО/МЭК 15408, о соответствии которой утверждается в составном ОО. Если редакции отличаются, оценщик должен определить, приведут ли различия между редакциями к противоречивым утверждениям.

Для случаев, где «Утверждения о соответствии ИСО/МЭК 15408» для базового ОО и зависимого ОО относятся к различным основным редакциям ИСО/МЭК 15408 (например в одном ОО-компоненте утверждается о соответствии второй редакции ИСО/МЭК 15408, а в другом — утверждается о соответствии третьей редакции ИСО/МЭК 15408), «Утверждение о соответствии» для составного ОО будет определяться по более ранней редакции ИСО/МЭК 15408, поскольку при разработке ИСО/МЭК 15408 преследовалась цель обеспечения обратной совместимости (хотя иногда такая совместимость не может быть достигнута в строгом смысле этого определения, предполагается, что в принципе она достижима).

ИСО/МЭК 15408-3 ASE_CCL.1.2C: *В «Утверждении о соответствии ИСО/МЭК 15408» должно приводиться описание соответствия ЗБ ИСО/МЭК 15408-2; ЗБ либо описывается как соответствующее требованиям ИСО/МЭК 15408-2, либо как содержащее расширенные по отношению к ИСО/МЭК 15408-2 требования.*

9.4.1.3.2 Шаг оценивания ASE_CCL.1-2

Оценщик должен проверить, что «Утверждение о соответствии ИСО/МЭК 15408» описывает соответствие ЗБ ИСО/МЭК 15408-2; ЗБ либо описывается как соответствующее требованиям ИСО/МЭК 15408-2, либо как содержащее расширенные по отношению к ИСО/МЭК 15408-2 требования.

Для составного ОО оценщик рассматривает, совместимо ли «Утверждение о соответствии» не только с ИСО/МЭК 15408-2, но и с «Утверждениями о соответствии ИСО/МЭК 15408-2» каждого из ОО-компонентов составного ОО. Т. е. если в одном или более ОО-компонентах утверждается, что ЗБ содержит расширенные по отношению к ИСО/МЭК 15408-2 требования, то и в составном ОО тоже следует приводить утверждение о соответствии расширению относительно ИСО/МЭК 15408-2.

«Утверждение о соответствии ИСО/МЭК 15408» для составного ОО может включать утверждение о соответствии расширению ИСО/МЭК 15408-2, даже если ОО-компоненты соответствуют ИСО/МЭК 15408-2, в случае, если к базовому ОО предъявляются расширенные ФТБ (см. Руководство по составным ОО для ASE_CCL.1.6C).

ИСО/МЭК 15408-3 ASE_CCL.1.3C: *В «Утверждении о соответствии ИСО/МЭК 15408» должно приводиться описание соответствия ПЗ ИСО/МЭК 15408-3; ЗБ либо описывается как соответствующее требованиям ИСО/МЭК 15408-3, либо как содержащее расширенные по отношению к ИСО/МЭК 15408-3 требования.*

9.4.1.3.3 Шаг оценивания ASE_CCL.1-3

Оценщик должен проверить, что в «Утверждении о соответствии ИСО/МЭК 15408» в ЗБ описывает соответствие ЗБ ИСО/МЭК 15408-3; ЗБ либо описывается как соответствующее требованиям ИСО/МЭК 15408-3, либо как содержащее расширенные по отношению к ИСО/МЭК 15408-3 требования.

ИСО/МЭК 15408-3 ASE_CCL.1.4C: *«Утверждение о соответствии ИСО/МЭК 15408» должно согласовываться с «Определением расширенных компонентов».*

9.4.1.3.4 Шаг оценивания ASE_CCL.1-4

Оценщик должен исследовать «Утверждение о соответствии ИСО/МЭК 15408-2», чтобы сделать заключение о том, что оно согласуется с «Определением расширенных компонентов».

Если в «Утверждении о соответствии ИСО/МЭК 15408» указывается о соответствии ИСО/МЭК 15408-2, оценщик делает заключение о том, что «Определение расширенных компонентов» не определяет функциональные компоненты.

Если в «Утверждении о соответствии ИСО/МЭК 15408» указывается о соответствии расширению ИСО/МЭК 15408-2, оценщик делает заключение о том, что «Определение расширенных компонентов» определяет хотя бы один расширенный функциональный компонент.

9.4.1.3.5 Шаг оценивания ASE_CCL.1-5

Оценщик должен исследовать «Утверждение о соответствии ИСО/МЭК 15408» в отношении ИСО/МЭК 15408-3, чтобы сделать заключение о его согласованности с «Определением расширенных компонентов».

Если в «Утверждении о соответствии ИСО/МЭК 15408» указывается о соответствии ИСО/МЭК 15408-3, оценщик делает заключение о том, что «Определение расширенных компонентов» не определяет компоненты требований доверия.

Если в «Утверждении о соответствии ИСО/МЭК 15408» указывается о соответствии расширению ИСО/МЭК 15408-3, оценщик делает заключение о том, что «Определение расширенных компонентов» определяет хотя бы один расширенный компонент требований доверия.

ИСО/МЭК 15408-3 ASE_CCL.1.5C: *В «Утверждении о соответствии» должны быть идентифицированы все ПЗ и пакеты требований безопасности, о соответствии которым утверждается в ЗБ.*

9.4.1.3.6 Шаг оценивания ASE_CCL.1-6

Оценщик должен проверить, что в «Утверждении о соответствии» содержится «Утверждение о соответствии ПЗ», идентифицирующее все ПЗ, о соответствии которым утверждается в ЗБ.

Если в ЗБ не утверждается о соответствии ПЗ, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что все ПЗ, на которые имеется ссылка, однозначно идентифицированы (например названием и номером версии или идентификацией, включенной во введение этого ПЗ).

Оценщику следует помнить, что утверждения о частичном соответствии ПЗ недопустимы. Поэтому, соответствие ПЗ, требующее составного решения, может быть указано в ЗБ для составного ОО. Соответствие такому ПЗ не было бы возможно в процессе оценки ОО-компонентов, так как такие ОО не удовлетворяют составному решению. Возможность такого соответствия будет иметься только в тех случаях, когда «составной» ПЗ допускает использование подхода к оценке композиции (использование компонентов класса АСО «Композиция»).

В ЗБ для составного ОО будут идентифицированы ЗБ ОО-компонентов, из которых складывается составное ЗБ. В составном ОО по существу утверждается о соответствии ЗБ всех ОО-компонентов.

9.4.1.3.7 Шаг оценивания ASE_CCL.1-7

Оценщик должен проверить, что в «Утверждении о соответствии» содержится «Утверждение о соответствии пакетам требований», идентифицирующее все пакеты, о соответствии которым утверждается в ЗБ.

Если в ЗБ не утверждается о соответствии ЗБ какому-либо пакету требований, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что любые пакеты требований, на которые ссылаются, однозначно идентифицированы (например названием и номером версии или идентификацией, включенной во введение этого пакета).

Оценщик делает заключение о том, что ЗБ ОО-компонентов, из которых состоит составной ОО, также однозначно идентифицированы.

Оценщику следует помнить, что утверждения о частичном соответствии некоторому пакету требований недопустимы.

ИСО/МЭК 15408-3 ASE_CCL.1.6C: *В «Утверждении о соответствии ЗБ пакету требований» должно приводиться описание любого соответствия ЗБ некоторому пакету требований; ЗБ либо описывается как соответствующее пакету требований, либо как содержащее расширенные по отношению к пакету требования.*

9.4.1.3.8 Шаг оценивания ASE_CCL.1-8

Оценщик должен проверить, что для каждого идентифицированного пакета требований в «Утверждении о соответствии» приведено описание соответствия ЗБ именованному пакету требований; ЗБ либо описывается как соответствующее именованному пакету требований, либо как содержащее расширенные по отношению к пакету требования.

Если в ЗБ не утверждается о соответствии ЗБ какому-либо пакету требований, то этот шаг оценивания не применим и считается удовлетворенным.

Если в утверждении о соответствии пакетам содержится утверждение о соответствии именованному пакету, оценщик делает заключение о том, что:

а) если пакет является пакетом требований доверия, то ЗБ содержит все ТДБ, включенные в пакет, но не содержит дополнительных ТДБ.

b) если пакет является функциональным, то ЗБ содержит все ФТБ, включенные в пакет, но не содержит дополнительных ФТБ.

Если в утверждении о соответствии пакетам содержится утверждение о соответствии расширению относительно именованного пакета, оценщик делает заключение о том, что:

a) если пакет является пакетом требований доверия, то ЗБ содержит все ТДБ, включенные в пакет, и по крайней мере одно дополнительное ТДБ или по крайней мере одно ТДБ, которое является иерархическим к ТДБ в пакете.

b) если пакет является функциональным, то ЗБ содержит все включенные в пакет ФТБ, и по крайней мере одно дополнительное ФТБ, или по крайней мере одно ФТБ, которое является иерархическим к ФТБ в пакете.

ИСО/МЭК 15408-3 ASE_CCL.1.7C: *В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что тип ОО согласуется с типом ОО в тех ПЗ, о соответствии которым утверждается.*

9.4.1.3.9 Шаг оценивания ASE_CCL.1-9

Оценщик должен исследовать «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что тип ОО согласуется со всеми типами ОО в ПЗ.

Если в ЗБ не утверждается о соответствии ПЗ, то этот шаг оценивания не применим и считается удовлетворенным.

Отношение между типами может быть простым: например в ЗБ межсетевого экрана утверждается о соответствии некоторому ПЗ межсетевого экрана или более сложным: например в ЗБ смарт-карты утверждается о соответствии нескольким ПЗ одновременно — ПЗ интегральной схемы, ПЗ для ОС смарт-карты, и двум ПЗ двух приложений на смарт-карте.

Для составного ОО оценщик выносит заключение о том, демонстрирует ли «Обоснование утверждений о соответствии», что типы ОО-компонентов соответствуют типу составного ОО. Это не означает, что и ОО-компоненты, и составной ОО должны быть одного типа, а означает, что ОО-компоненты возможно интегрировать в составной ОО. В ЗБ составного ОО следует ясно определить, какие ФТБ включены только как результат композиции составных частей и не были исследованы как ФТБ в ходе оценки базового и зависимого ОО (например по какому-либо ОУД).

ИСО/МЭК 15408-3 ASE_CCL.1.8C: *В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение определения проблемы безопасности согласуется с изложением определения проблемы безопасности в тех ПЗ, о соответствии которым утверждается.*

9.4.1.3.10 Шаг оценивания ASE_CCL.1-10

Оценщик должен исследовать «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что оно демонстрирует, что изложение определения проблемы безопасности согласуется с изложениями определений проблем безопасности тех ПЗ, о соответствии которым утверждается.

Если в ЗБ не утверждается о соответствии ПЗ, то этот шаг оценивания не применим и считается удовлетворенным.

Если ПЗ не содержит изложение определения проблемы безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Если требуется строгое соответствие ПЗ, соответствие которому утверждается, тогда не требуется «Обоснование утверждений о соответствии». Вместо этого оценщик делает заключение о том, является ли:

a) набор угроз в ЗБ расширенным или идентичным по отношению к перечню угроз в ПЗ, соответствие которому утверждается;

b) набор ПБОр в ЗБ расширенным или идентичным по отношению к ПБОр в ПЗ, соответствие которому утверждается;

c) набор предположений в ЗБ идентичным по отношению к предположениям в ПЗ, соответствие которому утверждается.

Если требуется демонстрируемое соответствие ПЗ, оценщик исследует «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что оно демонстрирует, что изложение определения проблемы безопасности в ЗБ эквивалентное или более ограничительное, чем изложение определения проблемы безопасности в ПЗ, соответствие которому утверждается.

В качестве руководства о том, что считать «эквивалентным или более ограничительным» изложением, см. ИСО/МЭК 15408-1, приложение D «Соответствие ПЗ».

Для составного ОО оценщик рассматривает, соответствует ли «Определение проблемы безопасности» составного ОО приведенному в ЗБ ОО-компонентов. Заключение об этом делается в виде де-

монстрируемого соответствия. В частности, оценщик исследует «Обоснование утверждений о соответствии», чтобы сделать заключение, что:

a) изложение угроз и ПБОр в ЗБ составного ОО не противоречат изложениям в ЗБ ОО-компонентов;

b) любые предположения, сделанные в ЗБ ОО-компонента, поддерживаются в ЗБ составного ОО. Таким образом, либо предположение следует также включить в составное ЗБ, либо следует обеспечить успешное выполнение предположения в составном ЗБ. Успешное выполнение предположения можно обеспечить с помощью спецификации требований в составном ОО для обеспечения функциональных возможностей, выполняющих условия, изложенные в предположении.

ИСО/МЭК 15408-3 ASE_CCL.1.9C: *В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение «Целей безопасности» согласуется с изложением «Целей безопасности» в тех ПЗ, о соответствии которым утверждается.*

9.4.1.3.11 Шаг оценивания ASE_CCL.1-11

Оценщик должен исследовать «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что изложение «Целей безопасности» в ПЗ согласуется с изложением «Целей безопасности» в тех ПЗ, о соответствии которым утверждается.

Если в ЗБ не утверждается о соответствии ПЗ, то этот шаг оценивания не применим и считается удовлетворенным.

Если требуется строгое соответствие ПЗ, тогда не требуется «Обоснование утверждений о соответствии». Вместо этого оценщик делает заключение о том, содержит ли:

- ЗБ все цели безопасности для ОО того ПЗ, о соответствии которому утверждается. Следует отметить, что в оцениваемом ЗБ могут быть дополнительные цели безопасности для ОО;
- ЗБ абсолютно все цели безопасности для среды функционирования (за одним исключением, которое описано в следующем абзаце). Следует отметить, что в оцениваемом ЗБ не может быть дополнительных целей безопасности для среды функционирования;
- ЗБ утверждение о том, что некоторые цели безопасности для среды функционирования того ПЗ, о соответствии которому утверждается, являются целями безопасности для ОО в ЗБ. Это — имеющее силу исключение из предыдущего абзаца.

Если требуется демонстрируемое соответствие ПЗ, о соответствии которому утверждается, оценщик исследует «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что оно демонстрирует, что изложение «Целей безопасности» в ЗБ эквивалентное или более ограничительное, чем изложение «Целей безопасности» в ПЗ, о соответствии которому утверждается.

В качестве руководства о том, что считать «эквивалентным или более ограничительным» изложением, см. ИСО/МЭК 15408-1, приложение D «Соответствие ПЗ».

Для составного ОО оценщик рассматривает, соответствуют ли «Цели безопасности» составного ОО определенным в ЗБ для ОО-компонентов. Заключение делается в виде демонстрируемого соответствия. В частности, оценщик исследует «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что:

a) изложение «Целей безопасности» в ЗБ зависимого ОО, относящегося к любой ИТ в среде функционирования, согласуется с изложением «Целей безопасности» для ОО в ЗБ основного ОО. При этом не ожидается, что изложение «Целей безопасности» для среды функционирования в ЗБ зависимых ОО будет перекрывать все аспекты изложения «Целей безопасности» для ОО в ЗБ базового ОО.

b) изложение «Целей безопасности» в составном ЗБ согласуется с изложением «Целей безопасности» в ЗБ ОО-компонентов.

Если требуется демонстрируемое соответствие ПЗ, оценщик исследует «Обоснование утверждений о соответствии», чтобы сделать заключение, что в нём продемонстрировано, что изложение «Целей безопасности» в ЗБ, по крайней мере, эквивалентно изложению «Целей безопасности» в ПЗ или ЗБ ОО-компонентов в случае оценки ЗБ составного ОО.

ИСО/МЭК 15408-3 ASE_CCL.1.10C: *В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение «Требований безопасности» согласуется с изложением «Требований безопасности» в тех ПЗ, о соответствии которым утверждается.*

9.4.1.3.12 Шаг оценивания ASE_CCL.1-12

Оценщик должен исследовать ЗБ, чтобы сделать заключение о том, что оно, в соответствии с изложением соответствия в ПЗ, согласуется с требованиями безопасности в тех ПЗ, о соответствии которым утверждается.

Если в ЗБ не утверждается о соответствии профилю защиты, то этот шаг оценивания не применим и считается удовлетворенным.

Если требуется строгое соответствие ПЗ, тогда не требуется «Обоснование утверждений о соответствии». Вместо этого оценщик делает заключение о том, является ли набор требований безопасности в ПЗ расширенным или идентичным набору требований безопасности в ПЗ, о соответствии которому утверждается (для строгого соответствия).

Если требуется демонстрируемое соответствие ПЗ, о соответствии которому утверждается, оценщик исследует «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что в нём продемонстрировано, что изложение «Требований безопасности» в ЗБ эквивалентное или более ограничительное, чем изложение «Требований безопасности» в ПЗ, о соответствии которому утверждается.

В качестве руководства о том, что считать «эквивалентным или более ограничительным» изложением, см. ИСО/МЭК 15408-1, приложение D «Соответствие ПЗ».

Для составного ОО оценщик рассматривает, соответствуют ли цели безопасности составного ОО целям, определенным в ЗБ для ОО-компонентов. Заключение делается в виде демонстрируемого соответствия. В частности, оценщик исследует «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что:

a) изложение «Требований безопасности» в ЗБ зависимых ОО, относящихся к любой ИТ в среде функционирования, согласуется с изложением «Требований безопасности» в ЗБ основного ОО. При этом не ожидается, что изложение «Требований безопасности» для среды функционирования в ЗБ зависимых ОО будет перекрывать все аспекты изложения «Требований безопасности» для ОО в ЗБ базового ОО, так как, возможно, понадобится добавить некоторые ФТБ к изложению «Требований безопасности» для ОО в ЗБ базового ОО. Однако рекомендуется, чтобы изложение «Требований безопасности» в базовом компоненте поддерживало функционирование зависимого компонента.

b) изложение «Целей безопасности» в ЗБ зависимых ОО, относящихся к любой ИТ в среде функционирования, согласуется с изложением «Целей безопасности» в ЗБ основного ОО. При этом не ожидается, что изложение «Целей безопасности» для среды функционирования в ЗБ зависимых ОО будет перекрывать все аспекты изложения «Требований безопасности» для ОО в ЗБ базового ОО.

c) изложение «Требований безопасности» в составном ЗБ согласуется с изложением «Требований безопасности» в ЗБ ОО-компонентов.

Если требуется демонстрируемое соответствие ПЗ, оценщик исследует «Обоснование утверждений о соответствии», чтобы сделать заключение о том, что в нём продемонстрировано, что изложение «Требований безопасности» в ЗБ по крайней мере эквивалентно изложению «Требований безопасности» в ПЗ или в ЗБ ОО-компонентов в случае оценки ЗБ составного ОО.

9.5 «Определение проблемы безопасности» (ASE_SPD)

9.5.1 Подвид деятельности по оценке (ASE_SPD.1)

9.5.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, что проблема безопасности, которая должна решаться применением ОО и его средой функционирования, четко определена.

9.5.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.5.1.3 Действие ASE_SPD.1.1E

ИСО/МЭК 15408-3 ASE_SPD.1.1C: *«Определение проблемы безопасности» должно содержать описание угроз.*

9.5.1.3.1 Шаг оценивания ASE_SPD.1-1

Оценщик должен проверить, что «Определение проблемы безопасности» включает описание угроз.

Если все цели безопасности получены из предположений и/или только из ПБОр, изложение угроз не обязательно должно присутствовать в ЗБ. В этом случае этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что «Определение проблемы безопасности» описывает угрозы, которым должен противостоять ОО и/или его среда функционирования.

ИСО/МЭК 15408-3 ASE_SPD.1.2C: *Описание всех угроз должно проводиться в терминах источника угрозы, активов и негативного действия.*

9.5.1.3.2 Шаг оценивания ASE_SPD.1-2

Оценщик должен исследовать «Определение проблемы безопасности», чтобы сделать заключение о том, что все угрозы описаны в терминах источника угрозы, негативного действия и активов.

Если все цели безопасности получены из предположений и/или только из ПБОр, изложение угроз не обязательно должно присутствовать в ЗБ. В этом случае этот шаг оценивания не применим и считается удовлетворенным.

Источники угроз могут быть описаны более подробно, с указанием таких аспектов, как уровень навыков и способностей нарушителя, доступные ему ресурсы, возможности и мотивация.

ИСО/МЭК 15408-3 ASE_SPD.1.3C: *В «Определение проблемы безопасности» должно быть включено описание ПБОр.*

9.5.1.3.3 Шаг оценивания ASE_SPD.1-3

Оценщик должен проверить, что «Определение проблемы безопасности» включает описание ПБОр.

Если все цели безопасности получены из предположений и/или только из ПБОр, изложение угроз не обязательно должно присутствовать в ЗБ. В этом случае этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что изложения ПБОр приведены в виде правил или руководств, которые должен выполнять ОО и/или его среда функционирования.

Оценщик делает заключение о том, что каждая ПБОр объясняется и/или интерпретируется с достаточной степенью детализации для того, чтобы она была однозначно понятной; четкое представление изложений политик безопасности необходимо для сопоставления их с целями безопасности.

ИСО/МЭК 15408-3 ASE_SPD.1.4C: *«Определение проблемы безопасности» должно содержать описание предположений относительно среды функционирования ОО.*

9.5.1.3.4 Шаг оценивания ASE_SPD.1-4

Оценщик должен исследовать «Определение проблемы безопасности», чтобы сделать заключение о том, что она включает в себя предположения о среде функционирования ОО.

Если нет никаких предположений, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что каждое предположение о среде функционирования ОО объяснено с достаточной степенью детализации для того, чтобы позволить пользователям сделать заключение о том, соответствует ли их среда функционирования ОО данному предположению. Если предположения неверно поняты и интерпретированы, может возникнуть ситуация, при которой ОО используется в среде функционирования, в которой он не будет функционировать безопасным способом.

9.6 Цели безопасности (ASE_OBJ)

9.6.1 Подвид деятельности по оценке (ASE_OBJ.1)

9.6.1.1 Цели

Цель данного подвида деятельности — сделать заключение о том, четко ли определены цели безопасности для среды функционирования.

9.6.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.6.1.3 Действие ASE_OBJ.1.1E

ИСО/МЭК 15408-3 ASE_OBJ.1.1C: *Изложение «Целей безопасности» должно включать в себя описание целей безопасности для среды функционирования ОО.*

9.6.1.3.1 Шаг оценивания ASE_OBJ.1-1

Оценщик должен проверить, определены ли в изложении «Целей безопасности» цели безопасности для среды функционирования.

Оценщик должен проверить, что цели безопасности для среды функционирования ОО определены.

9.6.2 Подвид деятельности по оценке (ASE_OBJ.2)

9.6.2.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, адекватно и полностью ли цели безопасности охватывают «Определение проблемы безопасности» и четко ли определено разделение данной проблемы между ОО и его средой функционирования.

9.6.2.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.6.2.3 Действие ASE_OBJ.2.1E

ИСО/МЭК 15408-3 ASE_OBJ.2.1C: *Изложение «Целей безопасности» должно включать в себя описание целей безопасности для ОО и для среды функционирования ОО.*

9.6.2.3.1 Шаг оценивания ASE_OBJ.2-1

Оценщик должен проверить, что изложение «Целей безопасности» определяет цели безопасности для ОО и цели безопасности для среды функционирования ОО.

Оценщик проверяет, что обе категории «Целей безопасности» ясно идентифицированы и отделены друг от друга.

ИСО/МЭК 15408-3 ASE_OBJ.2.2C: *В «Обосновании целей безопасности» каждая цель безопасности для ОО должна быть прослежена к угрозам, на противостояние которым направлена эта цель безопасности, и к ПБОр, на осуществление которых направлена эта цель безопасности.*

9.6.2.3.2 Шаг оценивания ASE_OBJ.2-2

Оценщик должен проверить, что в «Обосновании целей безопасности» представлено, прослежены ли все цели безопасности для среды к идентифицированным угрозам, на противостояние которым направлены данные цели, и/или к ПБОр, на осуществление которых направлены эти цели.

Каждая цель безопасности для ОО может быть прослежена к угрозам или ПБОр или к сочетанию угроз и ПБОр, и должна быть прослежена по крайней мере к одной угрозе или ПБОр.

Неудача при попытке такого прослеживания свидетельствует о том, что либо «Обоснование целей безопасности» является неполным, либо изложение «Определения проблемы безопасности» является неполным, либо цель безопасности для ОО является бесполезной.

ИСО/МЭК 15408-3 ASE_OBJ.2.3C: *В «Обосновании целей безопасности» каждая цель безопасности для ОО должна быть прослежена к угрозам, на противостояние которым направлена эта цель безопасности, к ПБОр, на осуществление которых направлена эта цель безопасности, а также к предположениям, поддерживаемым данной целью безопасности.*

9.6.2.3.3 Шаг оценивания ASE_OBJ.2-3

Оценщик должен проверить «Обоснование целей безопасности», чтобы сделать заключение, прослежены ли цели безопасности для среды функционирования к идентифицированным угрозам, на противостояние которым направлена эта цель безопасности, к ПБОр, на осуществление которых направлена эта цель безопасности, и/или к предположениям, которые поддерживаются этой целью безопасности.

Каждая цель безопасности для среды функционирования может быть прослежена к угрозам, ПБОр, предположениям или к сочетанию угроз, ПБОр и/или предположений, и должна быть прослежена по крайней мере к одной угрозе, ПБОр или предположению.

Неудача при попытке такого прослеживания свидетельствует о том, что либо «Обоснование целей безопасности» является неполным, либо «Определение проблемы безопасности» является неполным, либо цель безопасности для среды функционирования является бесполезной.

ИСО/МЭК 15408-3 ASE_OBJ.2.4C: *В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности направлены на противостояние всем идентифицированным угрозам.*

9.6.2.3.4 Шаг оценивания ASE_OBJ.2-4

Оценщик должен проверить «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждой угрозы логическое обоснование того, что цели безопасности пригодны для противостояния данной угрозе.

Если ни одна цель безопасности не прослежена к конкретной угрозе, то результат данного шага оценивания отрицательный (выносится отрицательный вердикт).

Оценщик делает заключение, демонстрирует ли обоснование угрозы то, что угроза устранена или снижена до приемлемого уровня, либо последствия её реализации в достаточной мере компенсированы.

Оценщик делает заключение, демонстрирует ли логическое обоснование угрозы то, что все цели безопасности достаточны: если все цели безопасности, прослеживаемые к угрозе, достигнуты, то угроза либо устранена, либо снижена до приемлемого уровня, либо последствия ее реализации в достаточной мере компенсированы.

Следует отметить, что прослеживание целей безопасности к угрозам в «Обосновании целей безопасности» может быть частью логического обоснования, но само по себе оно не является логическим обоснованием. Даже в том случае, когда цель безопасности является просто заявлением, отражающим намерение предотвратить реализацию конкретной угрозы, то все равно требуется логическое обоснование, хотя в этом случае оно может быть минимальным и иметь вид: «Цель безопасности X непосредственно противостоит Угрозе Y».

Оценщик также делает заключение, действительно ли каждая цель безопасности, которая прослежена к угрозе, является необходимой и при достижении вносит вклад в устранение, снижение или уменьшение данной угрозы.

ИСО/МЭК 15408-3 ASE_OBJ.2.5C: *В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности направлены на осуществление всех ПБОр.*

9.6.2.3.5 Шаг оценивания ASE_OBJ.2-5

Оценщик должен исследовать «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждой ПБОр логическое обоснование того, что цели безопасности пригодны для обеспечения осуществления этой ПБОр.

Если ни одна цель безопасности не прослежена к определенной ПБОр, то результат данного шага оценивания отрицательный (выносится отрицательный вердикт).

Оценщик делает заключение, демонстрирует ли логическое обоснование для ПБОр то, что цели безопасности достаточны: если все цели безопасности, прослеженные к этой ПБОр, достигнуты, то ПБОр осуществляется.

Оценщик также делает заключение, действительно ли каждая цель безопасности, которая прослежена к ПБОр, необходима и при достижении её вносит вклад в осуществление ПБОр.

Следует отметить, что прослеживание целей безопасности к ПБОр в «Обосновании целей безопасности» может быть частью логического обоснования, но само по себе оно не является логическим обоснованием. Даже в том случае, когда цель безопасности является просто заявлением, отражающим намерение реализовать конкретную ПБОр, то все равно требуется логическое обоснование, хотя в этом случае оно может быть минимальным и иметь вид: «Цель безопасности X непосредственно обеспечивает осуществление ПБОр Y».

ИСО/МЭК 15408-3 ASE_OBJ.2.6C: *В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности для среды функционирования поддерживают все предположения.*

9.6.2.3.6 Шаг оценивания ASE_OBJ.2-6

Оценщик должен исследовать «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждого предположения для среды функционирования приемлемое логическое обоснование того, что цели безопасности для среды функционирования пригодны для обеспечения выполнения данного предположения.

Если ни одна цель безопасности для среды функционирования не прослежена к определенному предположению, то результат данного шага оценивания отрицательный (выносится отрицательный вердикт).

Оценщик делает заключение, демонстрирует ли логическое обоснование для предположения относительно среды функционирования ОО то, что цели безопасности достаточны: если все цели безопасности для среды функционирования, прослеженные к данному предположению, достигнуты, то среда функционирования обеспечивает выполнение предположения.

Оценщик также делает заключение, действительно ли каждая цель безопасности для среды функционирования, прослеживаемая к некоторому предположению относительно среды функционирования ОО, является необходимой и что при её достижении действительно вносится вклад в обеспечение выполнения этого предположения средой функционирования.

Следует отметить, что прослеживание целей безопасности для среды функционирования к предположениям в «Обосновании целей безопасности» может быть частью логического обоснования, но само по себе оно не является логическим обоснованием. Даже в том случае, когда цель безопасности для среды функционирования представляет собой просто перефразированное предположение, то все равно требуется логическое обоснование, хотя в этом случае оно может быть минимальным и иметь вид: «Цель безопасности X непосредственно обеспечивает выполнение Предположения Y».

9.7 Определение расширенных компонентов (ASE_ECD)

9.7.1 Подвид деятельности по оценке (ASE_ECD.1)

9.7.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, определены ли расширенные компоненты ясно и однозначно, и необходимы ли они, то есть не могут ли они быть ясно выражены с использованием существующих компонентов ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3.

9.7.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.7.1.3 Действие ASE_ECD.1.1E

ИСО/МЭК 15408-3 ASE_ECD.1.1C: *В изложении «Требований безопасности» должны быть идентифицированы все расширенные требования безопасности.*

9.7.1.3.1 Шаг оценивания ASE_ECD.1-1

Оценщик должен проверить, что все требования безопасности в изложении «Требований безопасности», которые не идентифицированы как расширенные требования, присутствуют в ИСО/МЭК 15408-2 или в ИСО/МЭК 15408-3.

ИСО/МЭК 15408-3 ASE_ECD.1.2C: *В «Определении расширенных компонентов» должен определяться расширенный компонент для каждого расширенного требования безопасности.*

9.7.1.3.2 Шаг оценивания ASE_ECD.1-2

Оценщик должен проверить, что «Определение расширенных компонентов» определяет расширенный компонент для каждого расширенного требования безопасности.

Если ЗБ не содержит расширенные требования безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Единственный расширенный компонент может быть использован для определения множественных итераций расширенного требования безопасности, не обязательно повторять это определение для каждой итерации данного требования.

ИСО/МЭК 15408-3 ASE_ECD.1.3C: *В «Определении расширенных компонентов» должно указываться, как каждый расширенный компонент связан с существующими компонентами, семействами и классами ИСО/МЭК 15408.*

9.7.1.3.3 Шаг оценивания ASE_ECD.1-3

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что оно описывает, как каждый расширенный компонент связан с существующими в стандарте ИСО/МЭК 15408 компонентами, семействами и классами.

Если ЗБ не содержит расширенные требования безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что каждый расширенный компонент является:

a) компонентом семейства ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, или

b) компонентом нового семейства, определенного в ЗБ.

Если расширенный компонент является компонентом существующего семейства ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, оценщик делает заключение о том, что «Определение расширенных компонентов» в достаточной мере описывает, почему расширенному компоненту следует быть компонентом этого семейства и как это касается других компонентов семейства.

Если расширенный компонент является компонентом нового семейства, определенного в ЗБ, то оценщик подтверждает, что расширенный компонент не подходит ни к одному из существующих семейств.

Если ЗБ определяет новые семейства, оценщик делает заключение о том, что каждое новое семейство или:

a) входит в состав существующего класса ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, или

b) входит в состав нового класса, определенного в ЗБ.

Если семейство является семейством класса ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, то оценщик делает заключение о том, что «Определение расширенных компонентов» в достаточной мере описывает, почему семейству следует входить в этот класс и как оно связано с другими семействами этого класса.

Если семейство является семейством нового класса, определенного в ЗБ, оценщик подтверждает, что семейство не подходит ни к одному из существующих классов.

9.7.1.3.4 Шаг оценивания ASE_ECD.1-4

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждое определение расширенного компонента идентифицирует все соответствующие зависимости этого компонента.

Если ЗБ не содержит расширенные требования безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик подтверждает, что никакие соответствующие зависимости не были пропущены автором ЗБ.

ИСО/МЭК 15408-3 ASE_ECD.1.4C: *В «Определении расширенных компонентов» должны использоваться в качестве модели представления компоненты, семейства, классы и методология ИСО/МЭК 15408.*

9.7.1.3.5 Шаг оценивания ASE_ECD.1-5

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждый расширенный функциональный компонент использует существующие компоненты ИСО/МЭК 15408-2 в качестве модели представления.

Если ЗБ не содержит расширенные функциональные требования безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что расширенный функциональный компонент согласуется с пунктом 6.1.3 «Структура компонента» ИСО/МЭК 15408-2.

Если расширенный функциональный компонент использует операции, оценщик делает заключение о том, что расширенный функциональный компонент согласуется с подразделом 7.1 «Операции» ИСО/МЭК 15408-1.

Если расширенный функциональный компонент находится в иерархической зависимости по отношению к существующему функциональному компоненту, оценщик делает заключение о том, что расширенный функциональный компонент согласуется с пунктом 6.2.1 «Выделение изменений в компоненте» ИСО/МЭК 15408-2.

9.7.1.3.6 Шаг оценивания ASE_ECD.1-6

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждое определение нового функционального семейства использует существующие функциональные семейства ИСО/МЭК 15408 в качестве модели представления.

Если ЗБ не определяет расширенные функциональные семейства, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что все новые функциональные семейства определяются в соответствии с пунктом 6.1.2 «Структура семейства» ИСО/МЭК 15408-2.

9.7.1.3.7 Шаг оценивания ASE_ECD.1-7

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждое определение нового функционального класса использует существующие функциональные классы ИСО/МЭК 15408 в качестве модели представления.

Если ЗБ не определяет расширенные функциональные классы, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что все новые функциональные классы определяются в соответствии с пунктом 6.1.1 «Структура класса» ИСО/МЭК 15408-2.

9.7.1.3.8 Шаг оценивания ASE_ECD.1-8

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждое определение расширенного компонента требований доверия использует существующие компоненты ИСО/МЭК 15408-3 в качестве модели представления.

Если ЗБ не содержит расширенные ТДБ, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что «Определение расширенных компонентов» согласуется с пунктом 6.1.3 «Структура компонента» ИСО/МЭК 15408-3.

Если расширенный компонент доверия использует операции, оценщик делает заключение о том, что расширенный компонент доверия согласуется с подразделом 7.1 «Операции» ИСО/МЭК 15408-1.

Если расширенный компонент доверия находится в иерархической зависимости по отношению к существующему компоненту доверия, оценщик делает заключение о том, что расширенный компонент доверия согласуется с пунктом 6.1.3 «Структура компонента» ИСО/МЭК 15408-3.

9.7.1.3.9 Шаг оценивания ASE_ECD.1-9

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что для каждого определенного расширенного компонента требований доверия предоставлена соответствующая методология.

Если ЗБ не содержит расширенные ТДБ, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что для каждого элемента действий оценщика каждого расширенного ТДБ один или более шагов оценивания обеспечиваются, и что успешное выполнение всех шагов оценивания для данного элемента действий оценщика демонстрирует, что элемент был выполнен.

9.7.1.3.10 Шаг оценивания ASE_ECD.1-10

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждое определение нового семейства требований доверия использует существующие семейства требований доверия ИСО/МЭК 15408 в качестве модели представления.

Если ЗБ не определяет новые семейства доверия, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что все новые семейства требований доверия определяются в соответствии с пунктом 6.1.2 «Структура семейства» ИСО/МЭК 15408-3.

9.7.1.3.11 Шаг оценивания ASE_ECD.1-11

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждое определение нового класса доверия использует существующие классы доверия ИСО/МЭК 15408 в качестве модели представления.

Если ЗБ не определяет новые классы доверия, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что все новые классы доверия определяются в соответствии с пунктом 6.1.1 «Структура класса» ИСО/МЭК 15408-3.

ИСО/МЭК 15408-3 ASE_ECD.1.5C: *Расширенные компоненты должны состоять из измеримых объективных элементов, чтобы была возможность продемонстрировать соответствие или несоответствие этим элементам.*

9.7.1.3.12 Шаг оценивания ASE_ECD.1-12

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждый элемент в каждом расширенном компоненте измерим и излагает объективные требования оценки, чтобы была возможность продемонстрировать соответствие или несоответствие этим элементам.

Если ЗБ не содержит расширенные требования безопасности, то этот шаг оценивания не применим и считается удовлетворенным.

Оценщик делает заключение о том, что элементы расширенных функциональных компонентов заявлены таким способом, что их можно протестировать и проследить к соответствующим представлениям ФБО.

Оценщик также делает заключение о том, что для элементов расширенных компонентов доверия не требуется субъективное суждение оценщика.

Оценщику следует помнить, что хотя требование измеримости и объективности применимо для всех критериев оценки, нет формального метода доказательства таких свойств. Поэтому существующие функциональные компоненты и компоненты доверия в ИСО/МЭК 15408 должны использоваться в качестве модели для того, чтобы определить соответствие этому требованию.

9.7.1.4 Действие ASE_ECD.1.2E

9.7.1.4.1 Шаг оценивания ASE_ECD.1-13

Оценщик должен исследовать «Определение расширенных компонентов», чтобы сделать заключение о том, что каждый расширенный компонент не может быть точно выражен при использовании существующих компонентов.

Если ЗБ не содержит расширенные требования безопасности, этот шаг оценивания не применим, и считается удовлетворенным.

Оценщику при вынесении данного заключения следует принимать во внимание компоненты ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3, другие расширенные компоненты, которые были определены в ЗБ, комбинации этих компонентов и возможные операции над этими компонентами.

Оценщику следует помнить, что роль этого шага оценивания заключается в устранении ненужного дублирования компонентов в случае, если эти компоненты могут быть ясно выражены при помощи других компонентов. Оценщику не следует предпринимать исчерпывающий поиск всех возможных комбинаций компонентов, включая операции, пытаясь найти способ выразить расширенный компонент при помощи существующих компонентов.

9.8 Требования безопасности ИТ (ASE_REQ)

9.8.1 Подвид деятельности по оценке (ASE_REQ.1)

9.8.1.1 Цели

Цель данного подвида деятельности — сделать заключение, является ли описание ФТБ и ТДБ ясным, четким, полным и внутренне непротиворечивым.

9.8.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.8.1.3 Действие ASE_REQ.1.1E

ИСО/МЭК 15408-3 ASE_REQ.1.1C: *В изложении «Требований безопасности» должно быть включено описание ФТБ и ТДБ.*

9.8.1.3.1 Шаг оценивания ASE_REQ.1-1

Оценщик должен проверить, что изложение «Требований безопасности» содержит описание ФТБ.

Оценщик делает заключение о том, что каждое ФТБ идентифицировано одним из следующих способов:

a) ссылкой на конкретный компонент ИСО/МЭК 15408-2;

b) ссылкой на расширенный компонент в «Определении расширенных компонентов» ЗБ;

c) ссылкой на ПЗ, с которым утверждается соответствие в ЗБ;

d) ссылкой на пакет требований безопасности, с которым утверждается соответствие ЗБ;

e) с помощью воспроизведения в ЗБ.

Не обязательно использовать одинаковые способы идентификации для всех ФТБ.

9.8.1.3.2 Шаг оценивания ASE_REQ.1-2

Оценщик должен проверить, что изложение «Требований безопасности» содержит описание ТДБ.

Оценщик делает заключение о том, что каждое ТДБ идентифицировано одним из следующих способов:

a) ссылкой на конкретный компонент ИСО/МЭК 15408-3;

b) ссылкой на расширенный компонент в «Определении расширенных компонентов» ЗБ;

c) ссылкой на ПЗ, с которым утверждается соответствие в ЗБ;

d) ссылкой на пакет требований безопасности, с которым утверждается соответствие ЗБ;

e) с помощью воспроизведения в ЗБ.

Не обязательно использовать одинаковые способы идентификации для всех ТДБ.

ИСО/МЭК 15408-3 ASE_REQ.1.2C: *Все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, используемые в ФТБ и ТДБ, должны быть определены.*

9.8.1.3.3 Шаг оценивания ASE_REQ.1-3

Оценщик должен исследовать ЗБ для того, чтобы сделать заключение о том, что все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, используемые в ФТБ и ТДБ, определены.

Оценщик делает заключение о том, что ЗБ определяет все:

- субъекты и объекты (их типы), используемые в ФТБ;

- атрибуты безопасности субъектов (их типы), пользователей, объектов, информации, сеансов и/или ресурсов, возможные значения, которые могут принимать данные атрибуты и любые отношения между этими значениями (например «Совершенно секретно» выше, чем «Секретно»);

- операции (их типы), которые используются в ФТБ, включая результаты этих операций;

- внешние сущности (их типы) в ФТБ;

- прочие понятия, которые введены в ФТБ и/или ТДБ путем выполнения операций, если эти понятия не являются ясными без объяснения или использованы вне их словарных значений.

Цель этого шага оценивания состоит в том, чтобы удостовериться, чтобы ФТБ и ТДБ были четко определены и что нет возможности их недопонимания или неверной интерпретации из-за употребления неопределенных терминов. При выполнении этого шага оценивания не следует доходить до крайностей, вынуждая автора ЗБ определять каждое слово. Предполагается, что у широкой аудитории, на которую рассчитан набор требований безопасности, есть понимание ИТ в целом, основ информационной безопасности и знание «Критериев оценки безопасности информационных технологий».

Все вышеупомянутое может быть представлено по группам, классам, ролям, типам или другим классификациям и спецификациям, облегчающим понимание.

Оценщику следует помнить, что эти списки и определения не должны быть частью изложения «Требований безопасности», но могут быть размещены (частично или полностью) в различных подразделах оного. Это может быть особенно полезным, если одни и те же понятия используются в остальной части ЗБ.

ИСО/МЭК 15408-3 ASE_REQ.1.3C: *Изложение «Требований безопасности» должно идентифицировать все выполненные над требованиями безопасности операции.*

9.8.1.3.4 Шаг оценивания ASE_REQ.1-4

Оценщик должен проверить, идентифицированы ли все операции над требованиями безопасности в изложении «Требований безопасности».

Оценщик делает заключение, все ли операции идентифицированы в каждом ФТБ и ТДБ, где они используются. Идентификация может проводиться с помощью типографических различий или особого выделения в сопутствующем тексте или других средств различия.

ИСО/МЭК 15408-3 ASE_REQ.1.4C: *Все операции должны выполняться правильно.*

9.8.1.3.5 Шаг оценивания ASE_REQ.1-5

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «назначение» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

9.8.1.3.6 Шаг оценивания ASE_REQ.1-6

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «итерация» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

9.8.1.3.7 Шаг оценивания ASE_REQ.1-7

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «выбор» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

9.8.1.3.8 Шаг оценивания ASE_REQ.1-8

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «уточнение» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

ИСО/МЭК 15408-3 ASE_REQ.1.5C: *Каждая зависимость от требований безопасности должна быть либо удовлетворена, либо должно приводиться обоснование неудовлетворения данной зависимости.*

9.8.1.3.9 Шаг оценивания ASE_REQ.1-9

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что каждая зависимость требований безопасности или удовлетворена, или приведено обоснование неудовлетворения данной зависимости.

Зависимость удовлетворяется включением соответствующего компонента (или того, который является иерархическим к нему) в изложение «Требований безопасности». Компонент, используемый для удовлетворения зависимости, при необходимости следует изменить операциями, чтобы обеспечить выполнение данной зависимости.

В логическом обосновании того, что зависимость не удовлетворена, следует указывать либо:

a) почему зависимость не является полезной или необходимой, в этом случае не требуется предоставлять дополнительную информацию; либо

b) что зависимость обеспечивается средой функционирования ОО, в этом случае в логическое обоснование следует включить описание того, как цели безопасности для среды функционирования обеспечивают выполнение этой зависимости.

ИСО/МЭК 15408-3 ASE_REQ.1.6C: *Изложение «Требований безопасности» должно быть внутренне непротиворечивым.*

9.8.1.3.10 Шаг оценивания ASE_REQ.1-10

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что оно внутренне непротиворечиво.

Оценщик делает заключение о том, является ли объединенный набор всех ФТБ и ТДБ внутренне непротиворечивым.

Оценщик делает заключение о том, что во всех случаях, когда различные требования безопасности применимы к одним и тем же типам свидетельств разработчика, событий, операций, данных, проводимых тестирований и т. д. или относятся ко «всем объектам», «всем субъектам» и т. д., эти требования не противоречат друг другу.

Некоторые примеры возможных конфликтов:

a) расширенное ТДБ определяет, что проект некоторого криптографического алгоритма должен содержаться в секрете, а другое расширенное ТДБ предписывает свободный доступ к просмотру его исходных кодов;

b) компонент FAU_GEN.1 «Генерация данных аудита безопасности» определяет, что идентификатор субъекта должен регистрироваться в журнале; компонент FDP_ACC.1 «Ограниченное управление доступом» определяет, кто имеет права доступа к этим журналам, а компонент FPR_UNO.1 «Скрытность» определяет, что рекомендуется, чтобы некоторые действия субъектов не были доступны для просмотра другим субъектам. Если субъект, которому не следует иметь возможность видеть действия других субъектов, может получить доступ к журналам регистрации данных действий, эти ФТБ являются конфликтующими;

c) в компоненте FDP_RIP.1 «Ограниченная защита остаточной информации» указывается, что удаление остаточной информации более не требуется, а в компоненте FDP_ROL.1 «Базовый откат» определяется, что ОО может быть возвращен к предыдущему состоянию. Если информация, которая необходима для отката к предыдущему состоянию, была удалена, эти требования являются конфликтующими;

d) многократные итерации компонента FDP_ACC.1 «Ограниченное управление доступом», особенно если некоторые итерации касаются одних и тех же субъектов, объектов или операций. Если одно ФТБ по управлению доступом позволяет субъекту выполнять операцию над объектом, тогда как другое ФТБ по управлению доступом не позволяет это, эти требования являются конфликтующими.

9.8.2 Подвид деятельности по оценке (ASE_REQ.2)

9.8.2.1 Цели

Цель данного подвида деятельности — сделать заключение, является ли описание ФТБ и ТДБ ясным, однозначным, полным и внутренне непротиворечивым и обеспечивают ли ФТБ достижение целям безопасности ОО.

9.8.2.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.8.2.3 Действие ASE_REQ.2.1E

ИСО/МЭК 15408-3 ASE_REQ.2.1C: *Изложение «Требований безопасности» должно содержать описание ФТБ и ТДБ.*

9.8.2.3.1 Шаг оценивания ASE_REQ.2-1

Оценщик должен проверить, что изложение «Требований безопасности» содержит описание ФТБ.

Оценщик делает заключение о том, что каждое ФТБ идентифицировано одним из следующих способов:

a) ссылкой на конкретный компонент ИСО/МЭК 15408-2;

b) ссылкой на расширенный компонент в «Определении расширенных компонентов» ЗБ;

c) ссылкой на конкретный компонент ПЗ, о соответствии с которым утверждается в ЗБ;

d) ссылкой на конкретный компонент в пакете требований безопасности, о соответствии с которым утверждается в ЗБ;

e) с помощью воспроизведения в ЗБ.

Не обязательно использовать одинаковые способы идентификации для всех ФТБ.

9.8.2.3.2 Шаг оценивания ASE_REQ.2-2

Оценщик должен проверить, что изложение «Требований безопасности» содержит описание ТДБ.

Оценщик делает заключение о том, что каждое ТДБ идентифицировано одним из следующих способов:

a) ссылкой на конкретный компонент ИСО/МЭК 15408-3;

b) ссылкой на расширенный компонент в «Определении расширенных компонентов» ЗБ;

c) ссылкой на конкретный компонент в ПЗ, о соответствии с которым утверждается в ЗБ;

d) ссылкой на конкретный компонент в пакете требований безопасности, о соответствии с которым утверждается в ЗБ;

e) с помощью воспроизведения в ЗБ.

Не обязательно использовать одинаковые способы идентификации для всех ТДБ.

ИСО/МЭК 15408-3 ASE_REQ.2.2C: *Все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, используемые в ФТБ и ТДБ, должны быть определены.*

9.8.2.3.3 Шаг оценивания ASE_REQ.2-3

Оценщик должен исследовать ЗБ, чтобы сделать заключение о том, что все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, используемые в ФТБ и ТДБ, определены.

Оценщик делает заключение о том, что ЗБ определяет все:

- субъекты и объекты (их типы), используемые в ФТБ;
- атрибуты безопасности субъектов (их типы), пользователей, объектов, информации, сеансов и/или ресурсов, возможные значения, которые могут принимать данные атрибуты и любые отношения между этими значениями (например «Совершенно секретно» выше, чем «Секретно»);
- операции (их типы), которые используются в ФТБ, включая результаты выполнения этих операций;
- внешние сущности (их типы) в ФТБ;
- прочие понятия, которые введены в ФТБ и ТДБ путем выполнения операций, если эти понятия не являются ясными без дополнительного объяснения или используются вне их словарных значений.

Цель этого шага оценивания состоит в том, чтобы удостовериться, что ФТБ и ТДБ четко определены и что не может произойти их неправильного понимания из-за употребления неопределенных терминов. При выполнении этого шага оценивания не следует доходить до крайностей, вынуждая автора

ЗБ определять каждое слово. Предполагается, что у широкой аудитории, на которую рассчитан набор требований безопасности, есть понимание ИТ в целом, основ информационной безопасности и знание «Критериев оценки безопасности информационных технологий».

Все вышеупомянутое может быть представлено по группам, классам, ролям, типам или другим классификациям и спецификациям, облегчающим понимание.

Оценщику следует помнить, что эти списки и определения не должны быть частью изложения «Требований безопасности», но могут быть размещены (частично или полностью) в различных подразделах оного. Это может быть особенно полезным, если эти же понятия используются в остальной части ЗБ.

ИСО/МЭК 15408-3 ASE_REQ.2.3C: *В изложении «Требований безопасности» должны быть идентифицированы все выполненные над требованиями безопасности операции.*

9.8.2.3.4 Шаг оценивания ASE_REQ.2-4

Оценщик должен проверить, идентифицированы ли все возможные операции над требованиями безопасности в изложении «Требований безопасности».

Оценщик делает заключение, все ли операции (это относится и к завершенным и к незавершенным) идентифицированы в каждом ФТБ и ТДБ, где они используются. Идентификация может проводиться различными способами, например путем введения типографических различий, особого выделения в сопутствующем тексте или других средств различия.

ИСО/МЭК 15408-3 ASE_REQ.2.4C: *Все операции должны выполняться правильно.*

9.8.2.3.5 Шаг оценивания ASE_REQ.2-5

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «назначение» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

9.8.2.3.6 Шаг оценивания ASE_REQ.2-6

Оценщик должен исследовать изложение требований безопасности, чтобы сделать заключение о том, что все операции типа «итерация» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

9.8.2.3.7 Шаг оценивания ASE_REQ.2-7

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что все операции типа «выбор» выполняются правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

9.8.2.3.8 Шаг оценивания ASE_REQ.2-8

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, выполняются ли все операции типа «уточнение» правильно.

Руководство по правильному выполнению операций представлено в приложении С «Руководство по выполнению операций» ИСО/МЭК 15408-1.

ИСО/МЭК 15408-3 ASE_REQ.2.5C: *Каждая зависимость от «Требований безопасности» должна быть либо удовлетворена, либо должно приводиться обоснование неудовлетворения зависимости.*

9.8.2.3.9 Шаг оценивания ASE_REQ.2-9

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что каждая зависимость требований безопасности или удовлетворена, или приведено обоснование неудовлетворения зависимости.

Зависимость удовлетворяется включением соответствующего компонента (или того, который является иерархическим к нему) в изложение «Требований безопасности». Компонент, используемый для удовлетворения зависимости, при необходимости, следует изменить операциями, чтобы обеспечить фактическое удовлетворение данной зависимости.

В логическом обосновании того, что зависимость не удовлетворена, следует указать либо:

a) то, почему зависимость не является полезной или необходимой, при этом не требуется предоставлять дополнительную информацию; либо

b) то, что зависимость обеспечивается средой функционирования ОО, в этом случае в логическое обоснование следует включить описание того, как цели безопасности для среды функционирования обеспечивают выполнение зависимости.

ИСО/МЭК 15408-3 ASE_REQ.2.6C: *В «Обосновании требований безопасности» должно быть представлено прослеживание каждого ФТБ к целям безопасности для ОО.*

9.8.2.3.10 Шаг оценивания ASE_REQ.2-10

Оценщик должен проверить, прослежены ли ФТБ в «Обосновании требований безопасности» к целям безопасности для ОО.

Оценщик делает заключение, прослежено ли каждое ФТБ по крайней мере к одной цели безопасности для ОО.

Неудача при попытке такого прослеживания означает, что либо «Обоснование требований безопасности» является неполным, либо цели безопасности для ОО являются неполными, либо ФТБ являются бесполезными.

ИСО/МЭК 15408-3 ASE_REQ.2.7C: *В «Обосновании требований безопасности» должно быть продемонстрировано, что ФТБ обеспечивают выполнение всех целей безопасности для ОО.*

9.8.2.3.11 Шаг оценивания ASE_REQ.2-11

Оценщик должен исследовать «Обоснование требований безопасности», чтобы сделать заключение, содержится ли в нем для каждой цели безопасности для ОО логическое обоснование того, что ФТБ пригодны для достижения данной цели безопасности для ОО.

Если никакие ФТБ не прослежены к конкретной цели безопасности для ОО, то результат данного шага оценивания отрицательный (выносится отрицательный вердикт).

Оценщик делает заключение о том, демонстрирует ли логическое обоснование целей безопасности для ОО, что ФТБ достаточны: если все ФТБ, прослеженные к данной цели, удовлетворены, то цель безопасности для ОО достигнута.

Оценщик также делает заключение, действительно ли каждое требование безопасности ОО, прослеженное к цели безопасности для ОО, необходимо и при успешном выполнении вносит вклад в достижение данной цели безопасности.

Следует отметить, что прослеживание от ФТБ к целям безопасности для ОО, представленное в «Обосновании требований безопасности», может быть частью логического обоснования, но само по себе оно не является логическим обоснованием.

ИСО/МЭК 15408-3 ASE_REQ.2.8C: *В «Обосновании требований безопасности» должно приводиться пояснение того, почему выбраны определенные ТДБ.*

9.8.2.3.12 Шаг оценивания ASE_REQ.2-12

Оценщик должен проверить, что в «Обосновании требований безопасности» объясняется, почему выбраны определенные ТДБ.

Оценщику следует помнить, что любое объяснение является правильным, пока оно составлено четко и ясно, и ни в ТДБ, ни в объяснении нет очевидных несогласованностей с прочими частями ЗБ.

Пример очевидной несогласованности между ТДБ и остальными частями ЗБ — когда имеются источники угроз, обладающие большими возможностями для атаки, но ТДБ в семействе AVA_VAN не обеспечивают мер защиты от этих источников угроз.

ИСО/МЭК 15408-3 ASE_REQ.2.9C: *Изложение «Требований безопасности» должно быть внутренне непротиворечивым.*

9.8.2.3.13 Шаг оценивания ASE_REQ.2-13

Оценщик должен исследовать изложение «Требований безопасности», чтобы сделать заключение о том, что оно внутренне непротиворечиво.

Оценщик делает заключение о том, является ли объединенный набор всех ФТБ и ТДБ внутренне непротиворечивым.

Оценщик делает заключение о том, что во всех случаях, когда различные требования безопасности применяются к одним и тем же типам свидетельств разработчика, событий, операций, данных, проводимых тестирований и т. д. или ко «всем объектам», «всем субъектам» и т. д., эти требования не противоречат друг другу.

Некоторые примеры возможных конфликтов:

a) в расширенном ТДБ определяется, что проект некоторого криптографического алгоритма должен содержаться в секрете, а другое расширенное ТДБ предписывает общий доступ к этим данным;

b) компонент FAU_GEN.1 «Генерация данных аудита» определяет, что некая сущность субъекта должна регистрироваться в журнале; FDP_ACC.1 «Ограниченное управление доступом» определяет, у кого есть право доступа к этим журналам и FPR_UNO.1; «Скрытность», определяет, что рекомендуется, чтобы некоторые действия субъектов не были доступны для просмотра другим субъектам. Если субъект, которому не следует иметь возможность видеть действия других субъектов, может получить доступ к журналам данных действий, эти ФТБ являются конфликтующими;

c) в компоненте FDP_RIP.1 «Ограниченная защита остаточной информации» указывается, что удаление остаточной информации более не является необходимостью, а в FDP_ROL.1; «Базовый

откат» определяется, что ОО может быть возвращен к предыдущему состоянию. Если информация, которая необходима для отката к предыдущему состоянию, была удалена, эти требования являются конфликтующими;

d) многократные итерации FDP_ACC.1 «Ограниченное управление доступом», особенно, если некоторые итерации касаются одних и тех же субъектов, объектов или операций. Если одно ФТБ по управлению доступом позволяет субъекту выполнять операцию над объектом, тогда как другое ФТБ по управлению доступом не позволяет это, эти требования являются конфликтующими.

9.9 Краткая спецификация ОО (ASE_TSS)

9.9.1 Подвид деятельности по оценке (ASE_TSS.1)

9.9.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы определить, обращается ли краткая спецификация ОО ко всем ФТБ и совместима ли краткая спецификация ОО с другими описаниями ОО, в том числе составленными в повествовательной форме.

9.9.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.9.1.3 Действие ASE_TSS.1.1E

ИСО/МЭК 15408-3 ASE_TSS.1.1C: *Краткая спецификация ОО должна описывать, каким образом ОО выполняет каждое ФТБ.*

9.9.1.3.1 Шаг оценивания ASE_TSS.1-1

Оценщик должен исследовать краткую спецификацию ОО, чтобы сделать заключение о том, что она описывает, каким образом ОО соответствует каждому ФТБ.

Оценщик делает заключение о том, что краткая спецификация ОО предоставляет для каждого ФТБ из изложения «Требований безопасности» описание того, каким образом удовлетворяется это ФТБ.

Оценщику следует помнить, что цель каждого описания состоит в том, чтобы предоставить потенциальным пользователям ОО представление верхнего уровня о том, как разработчик собирается выполнить каждое ФТБ, и поэтому описаниям не следует быть чрезмерно детализированными.

Для составного ОО оценщик также делает заключение о том, ясно ли, какой компонент или группа компонентов обеспечивает выполнение каждого ФТБ.

9.9.1.4 Действие ASE_TSS.1.1E

9.9.1.4.1 Шаг оценивания ASE_TSS.1-2

Оценщик должен исследовать краткую спецификацию ОО, чтобы сделать заключение о том, что она согласуется с «Аннотацией ОО» и «Описанием ОО».

«Аннотация ОО», «Описание ОО» и краткая спецификация ОО описывают ОО в повествовательной форме с последовательным увеличением уровня детализации. Поэтому эти описания должны быть непротиворечивыми.

9.9.2 Подвид деятельности по оценке (ASE_TSS.2)

9.9.2.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, обращается ли краткая спецификация ОО ко всем ФТБ, обращается ли краткая спецификация ОО к вмешательству, логическому искажению, обходу защиты, и совместима ли краткая спецификация ОО с другими описаниями ОО, в том числе составленными в повествовательной форме.

9.9.2.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.9.2.3 Действие ASE_TSS.2.1E

ИСО/МЭК 15408-3 ASE_TSS.2.1C: *Краткая спецификация ОО должна описывать, каким образом ОО выполняет каждое ФТБ.*

9.9.2.3.1 Шаг оценивания ASE_TSS.2-1

Оценщик должен исследовать краткую спецификацию ОО, чтобы сделать заключение о том, что она описывает, каким образом ОО соответствует каждому ФТБ.

Оценщик делает заключение о том, что краткая спецификация ОО предоставляет для каждого ФТБ из изложения «Требований безопасности» описание того, каким образом удовлетворяется это ФТБ.

Оценщику следует помнить, что цель каждого описания состоит в том, чтобы предоставить потенциальным пользователям ОО представление верхнего уровня о том, как разработчик собирается выполнить каждое ФТБ, и поэтому описаниям не следует быть чрезмерно детализированными.

Для составного ОО оценщик также делает заключение о том, ясно ли, какой компонент или группа компонентов обеспечивает выполнение каждого ФТБ.

ИСО/МЭК 15408-3 ASE_TSS.2.2C: *Краткая спецификация ОО должна описывать, каким образом ОО противостоит попыткам вмешательства и логического искажения.*

9.9.2.3.2 Шаг оценивания ASE_TSS.2-2

Оценщик должен исследовать краткую спецификацию ОО, чтобы сделать заключение о том, что она описывает, каким образом ОО может противостоять вмешательству и логическому искажению.

Оценщику следует помнить, что цель каждого описания состоит в том, чтобы предоставить потенциальным пользователям ОО представление верхнего уровня о том, как разработчик собирается обеспечить защиту ОО от вмешательства и логического искажения, и поэтому описаниям не следует быть чрезмерно детализированными.

Для составного ОО оценщик также делает заключение о том, ясно ли, какой компонент или группа компонентов обеспечивает защиту.

ИСО/МЭК 15408-3 ASE_TSS.2.3C: *Краткая спецификация ОО должна описывать, каким образом ОО противостоит попыткам обхода защиты.*

9.9.2.3.3 Шаг оценивания ASE_TSS.2-3

Оценщик должен исследовать краткую спецификацию ОО, чтобы сделать заключение о том, что она описывает, каким образом ОО может противостоять попыткам обхода защиты.

Оценщику следует помнить, что цель каждого описания состоит в том, чтобы предоставить потенциальным пользователям ОО представление верхнего уровня о том, как разработчик собирается обеспечить защиту ОО от попыток обхода защиты, и поэтому описаниям не следует быть чрезмерно детализированными.

Для составного ОО оценщик также делает заключение о том, ясно ли, какой компонент или группа компонентов обеспечивает защиту.

9.9.2.4 Действие ASE_TSS.2.2E

9.9.2.4.1 Шаг оценивания ASE_TSS.2-4

Оценщик должен исследовать краткую спецификацию ОО, чтобы сделать заключение о том, что она совместима с «Аннотацией ОО» и «Описанием ОО».

«Аннотация ОО», «Описание ОО» и краткая спецификация ОО описывают ОО в повествовательной форме с последовательным увеличением уровня детализации. Поэтому эти описания должны быть непротиворечивыми.

10 Класс ADV: Разработка

10.1 Введение

Вид деятельности «Разработка» предназначен для того, чтобы оценить проектную документацию на предмет ее достаточности для понимания того, каким образом ФБО удовлетворяют ФТБ и возможно ли исказить или обойти реализацию этих ФТБ. Это понимание достигается путем исследования описаний в проектной документации ФБО, предоставляемых с увеличением детализации и качества описаний. Проектная документация состоит из функциональной спецификации (которая описывает интерфейсы ФБО), описания проекта ОО (которое описывает архитектуру ФБО с точки зрения того, как она обеспечивает выполнение функций, связанных с заявленными ФТБ), и описания реализации (описание на уровне исходного кода). Кроме того, в неё включается «Описание архитектуры безопасности» (которое описывает архитектурные свойства ФБО в целях объяснения того, каким образом обеспечение безопасности не может быть скомпрометировано или обойдено), описание внутреннего состава (которое описывает, как ФБО спроектированы в манере, обеспечивающей их понимание), а также модель политики безопасности (которая формально описывает политику безопасности, осуществляемую ФТБ).

10.2 Замечания по применению

Требования ИСО/МЭК 15408 к проектной документации ранжированы по количеству и уровню детализации представленной информации, а также по степени формализации представления информации. На более низких уровнях наиболее критические для безопасности части ФБО описаны с большей детализацией, в то время как для менее критических по отношению к безопасности частей ФБО приводятся только краткие описания; дополнительное доверие приобретается путем увеличения количества предоставляемой информации о наиболее критических по отношению к безопасности частях ФБО и повышения уровня детализации описаний менее критических по отношению к безопасности частях

ФБО. Наиболее высокий уровень доверия достигается тогда, когда предоставляется полная и детализированная информация обо всех частях ФБО.

В ИСО/МЭК 15408 рассматриваются следующие иерархические степени формализации документа: неформальный, полуформальный, формальный. Неформальный документ — это документ, который составлен на естественном языке. Методология не предписывает использовать какой-либо конкретный язык; этот вопрос остается за системой оценки. Следующие абзацы дифференцируют содержание различных неформальных документов.

Функциональная спецификация включает описание назначения и метода использования интерфейсов ФБО. Например, если операционная система предоставляет пользователю средства идентификации пользователя, создания, модификации или удаления файлов, установления разрешения другим пользователям на доступ к файлам и взаимодействия с удаленными машинами, то ее функциональная спецификация, как правило, содержит описание каждой из этих функций и того, как они реализуются через взаимодействие с внешне видимыми интерфейсами ФБО. Если имеются также функции аудита, связанные с обнаружением и регистрацией таких событий, то описание этих функций аудита также обычно включается в состав функциональной спецификации; и хотя пользователь формально не обращается к этим функциям непосредственно через внешний интерфейс, на них определенно влияет все то, что происходит на уровне внешнего пользовательского интерфейса.

Описание проекта выражается в терминах логических единиц деления (подсистем и модулей), которые предоставляют доступные для понимания сервисы или функции. Например, межсетевой экран может состоять из подсистем фильтрации пакетов, удаленного администрирования, аудита, фильтрации на уровне соединения. Описание проекта межсетевого экрана обычно включает описание предпринимаемых действий, а именно того, какие действия предпринимает каждая подсистема, когда входящий пакет приходит на межсетевой экран.

10.3 Архитектура безопасности (ADV_ARC)

10.3.1 Подвид деятельности по оценке (ADV_ARC.1)

10.3.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, структурированы ли ФБО таким образом, что в них нельзя вмешаться или их обойти, и изолируют ли ФБО, предоставляющие домены безопасности, эти домены друг от друга.

10.3.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности являются:

a) ЗБ;
b) функциональная спецификация;
c) проект ОО;
d) описание архитектуры безопасности;
e) представление реализации (при наличии);
f) руководство пользователя по эксплуатации.

10.3.1.3 Замечания по применению

Понятия обеспечения собственной защиты, разделения доменов и невозможности обхода функциональных возможностей безопасности отличаются от функций безопасности, выраженных в ФТБ второй части стандарта ИСО/МЭК 15408, потому что в большинстве случаев ФБО не предоставляют непосредственно видимый интерфейс для обеспечения собственной защиты и невозможности обхода функциональных возможностей безопасности. Скорее, они являются свойствами ФБО, которые достигаются посредством проекта ОО и осуществляются правильной реализацией этого проекта. Кроме того, оценка этих свойств проводится менее целенаправленно, чем оценка механизмов; труднее проверить отсутствие функциональных возможностей, чем их наличие. Однако заключение о том, что эти свойства удовлетворены, так же критически важно, как и вынесение заключения о том, что механизмы реализованы правильно.

Общий подход состоит в том, что разработчик предоставляет ФБО, которые соответствуют вышеупомянутым свойствам, и документальные свидетельства, которые могут быть проанализированы, чтобы показать, что свойства действительно реализованы. Оценщик несет ответственность за просмотр свидетельств и вынесение на основе этих и других полученных для ОО свидетельств заключения о том, что свойства реализованы. Шаги оценивания могут быть охарактеризованы как те, которые детализируют вопросы того, какая информация должна быть предоставлена, и те, которые относятся к фактическому анализу, выполняемому оценщиком.

В «Описании архитектуры безопасности» представлена информация о том, как определены домены и каким образом ФБО обеспечивают их разделение. Представлено и описание механизмов, которые препятствуют изменению ФБО недоверяемыми процессами, а также тех, которые обеспечивают адекватную защиту ресурсов под контролем ФБО и выполнения ФБО роли промежуточного звена при осуществлении всех действий, связанных с ФТБ. Также объясняется роль среды функционирования в каком-либо из этих процессов (например если предполагается, что среда функционирования правильно вызывается базовой средой, то каким образом приводятся в действие функции безопасности). По сути, в «Описании архитектуры безопасности» приводится объяснение того, каким образом предполагается, что ОО предоставляет тот или иной сервис безопасности.

Исследования, которые выполняет оценщик, должны быть выполнены на основании всех предоставленных по ОО свидетельств разработки, с учетом уровня детализации представленных свидетельств. На более низких уровнях доверия не следует ожидать, что, например проведен полный анализ собственной защиты ФБО, потому что оценщику будут доступны только представления проекта верхнего уровня. Оценщику следует быть уверенным в том, что он при выполнении оценки свойств, исследуемых на последующих шагах оценки, использует информацию, собранную при проведении других частей анализа (например при анализе проекта ОО).

10.3.1.4 Действие ADV_ARC.1.1E

ИСО/МЭК 15408-3 ADV_ARC.1.1C: *Уровень детализации «Описания архитектуры безопасности» должен соответствовать представленному в проектной документации по ОО описанию абстракций (элементов представления ОО), осуществляющих выполнение ФТБ.*

10.3.1.4.1 Шаг оценивания ADV_ARC.1-1

Оценщик должен исследовать «Описание архитектуры безопасности», чтобы сделать заключение о том, что информация, предоставленная в свидетельствах, представлена на уровне детализации, соразмерном с описаниями осуществляющих выполнение ФТБ обобщений, содержащихся в функциональной спецификации и в документированном проекте ОО.

Относительно функциональной спецификации оценщику следует удостовериться, что описанные в ней функции собственной защиты охватывают те эффекты, которые явно представлены в ИФБО. Такое описание может включать защиту исполняемых образов ФБО и защиту объектов (например файлов, используемых ФБО). Оценщик удостоверяется также в том, что функции, которые можно вызвать через ИФБО, описаны.

Если в оценку включается Подвид деятельности по оценке (ADV_TDS.1) или Подвид деятельности по оценке (ADV_TDS.2), оценщик удостоверяется в том, что «Описание архитектуры безопасности» содержит информацию о том, как функционируют подсистемы, которые способствуют разделению доменов ФБО.

Если в оценку включается Подвид деятельности по оценке (ADV_TDS.3) или выше, оценщик удостоверяется в том, что «Описание архитектуры безопасности» также содержит информацию, зависящую от реализации. Например, такое описание может содержать информацию, имеющую отношение к стандартам оформления кода для проверки параметра, предотвращающего компрометацию ФБО (например переполнение буфера), а также информацию об управлении стеком для операций вызова и возврата. Оценщик проверяет описания механизмов, чтобы удостовериться, что уровень детализации таков, что не допускает возникновения двусмысленности между описаниями механизмов в «Описании архитектуры безопасности» и в представлении реализации.

По действию оценщика, связанному с этим шагом оценивания, выносится отрицательный вердикт, если в «Описании архитектуры безопасности» упоминается какой-либо модуль, подсистема или интерфейс, которые не описаны в функциональной спецификации или «Проекте ОО».

ИСО/МЭК 15408-3 ADV_ARC.1.2C: *В «Описании архитектуры безопасности» должно быть включено описание доменов безопасности, обеспеченных согласованностью ФБО с ФТБ.*

10.3.1.4.2 Шаг оценивания ADV_ARC.1-2

Оценщик должен исследовать «Описание архитектуры безопасности», чтобы сделать заключение о том, что в ней описаны домены безопасности, обеспеченные ФБО.

Домены безопасности относятся к средам, предоставляемым ФБО для использования потенциально опасными сущностями: например типовая операционная система в защищенном исполнении поставляет набор ресурсов (адресное пространство, переменные окружения процесса) для использования процессами с ограниченными правами доступа и свойствами безопасности. Оценщик делает заключение о том, что описание разработчиком доменов безопасности учитывает все ФТБ, заявленные для ОО.

Для некоторых ОО не существует таких доменов, поскольку все взаимодействия, доступные пользователям, строго ограничены ФБО. Фильтрующий пакеты межсетевой экран — пример такого ОО. Пользователи LAN или WAN не взаимодействуют с ОО, поэтому не требуется никаких доменов безопасности; имеются только структуры данных, обеспечиваемые ФБО, для хранения пакетов разных пользователей отдельно друг от друга. Оценщик удостоверяется, что любое утверждение о том, что для ОО нет доменов безопасности, поддерживается свидетельствами, и что такие домены действительно недоступны.

ИСО/МЭК 15408-3 ADV_ARC.1.3C: *«Описание архитектуры безопасности» должно предоставлять информацию о том, насколько процесс инициализации ФБО является защищенным.*

10.3.1.4.3 Шаг оценивания ADV_ARC.1-3

Оценщик должен исследовать «Описание архитектуры безопасности», чтобы сделать заключение о том, что процесс инициализации обеспечивает безопасность.

Информация, предоставленная в «Описании архитектуры безопасности» относительно инициализации ФБО, направлена на компоненты ОО, которые вовлечены в приведение ФБО в начальное безопасное состояние (то есть, когда все части ФБО функционируют), при применении включения или сброса. Следует, чтобы описание в «Описании архитектуры безопасности» перечисляло компоненты инициализации системы и ту обработку, которая происходит при переходе от «нерабочего» состояния к начальному безопасному состоянию.

Часто случается, что компоненты, которые выполняют эту функцию инициализации, недоступны после того, как безопасное состояние достигнуто; в этом случае «Описание архитектуры безопасности» идентифицирует компоненты и объясняет, что они недоступны для недоверенных сущностей после установления ФБО. В этом отношении необходимо сохранить свойство этих компонентов, заключающееся в том, что они либо 1) недоступны для недоверенных сущностей после достижения безопасного состояния, либо 2) в случае, если они предоставляют интерфейсы недоверенным сущностям, эти ИФБО не могут быть использованы для вмешательства в ФБО.

В этом случае, компоненты ОО, связанные с инициализацией ФБО, рассматриваются как часть ФБО и анализируются с этой точки зрения. Следует отметить, что хотя их рассматривают как часть ФБО, скорее всего, может быть сделано логическое обоснование (что допускается семейством ADV_INT «Внутренняя структура ФБО») о том, что эти компоненты не должны отвечать требованиям по внутренней структуре из ADV_INT.

ИСО/МЭК 15408-3 ADV_ARC.1.4C: *В «Описании архитектуры безопасности» должно быть продемонстрировано, что ФБО обеспечивают собственную защиту от вмешательства.*

10.3.1.4.4 Шаг оценивания ADV_ARC.1-4

Оценщик должен исследовать «Описание архитектуры безопасности», чтобы сделать заключение о том, что ФБО обеспечивают собственную защиту от вмешательства недоверенных активных сущностей.

«Собственная защита» относится к способности ФБО защитить себя от действий внешних сущностей, которые могут привести к изменениям ФБО. Для ОО, у которых есть зависимости от других сущностей ИТ, часто имеет место ситуация, когда ОО для выполнения своих функций использует сервисы, поставляемые другой сущностью ИТ. В таких случаях ФБО не могут обеспечить собственную защиту, потому что часть защиты обеспечивается другой сущностью ИТ. В целях «Описания архитектуры безопасности» понятие «собственная защита» применяется только к сервисам, предоставляемым ФБО посредством их ИФБО, а не к сервисам, предоставляемым базовыми сущностями ИТ, которые используются этим ИФБО.

Собственная защита, как правило, достигается множеством средств, от физических и логических ограничений на доступ к ОО до аппаратных (например «колец защиты» и средств, поддерживающих функции управления памятью) и программных средств (например осуществляющих проверку вводимых данных на доверенном сервере). Оценщик делает заключение о том, что все такие механизмы описаны.

Оценщик делает заключение о том, что описание проекта охватывает вопрос того, как ввод данных пользователем обрабатывается ФБО таким способом, при котором ФБО защищены от внесения в них искажений вводимыми данными. Например, ФБО могут реализовать понятие «привилегии» и защитить себя от искажений при вводе пользователем данных при помощи ограничения возможностей пользователя в зависимости от его привилегий. ФБО могут использовать механизмы разделения, реализуемые процессором, например уровни привилегий (мандаты) или «кольца защиты». ФБО могут реализовать компоненты программной защиты или стандарты оформления кода, которые способствуют реализации

разделения программных доменов, например путем разграничения системного и пользовательского адресного пространства. Также ФБО могут зависеть от среды, которая предоставляет некоторую поддержку по защите ФБО.

Все механизмы, способствующие выполнению функциональных возможностей разделения доменов, описываются. Оценщику следует использовать сведения, полученные из других свидетельств (функциональная спецификация, проект ОО, описание внутренней структуры ФБО, другие части «Описания архитектуры безопасности» или представления реализации, как включается в пакет доверия для ОО) при вынесении заключения о том, описаны ли функциональные возможности, способствующие собственной защите, которые отсутствуют в «Описании архитектуры безопасности».

Точность описания механизмов собственной защиты является свойством описания правильно описывать реализованное. Оценщику следует использовать другие свидетельства (функциональную спецификацию, проект ОО, описание внутренней структуры ФБО, другие части «Описания архитектуры безопасности» или представления реализации, как включается в ЗБ для ОО) при вынесении заключения о том, есть ли противоречия в каких-либо описаниях механизмов собственной защиты. Если «Представление реализации» (ADV_IMP) включается в пакет доверия для ОО, то оценщик проведет выборку представления реализации; оценщику следует также удостовериться, что описания в этой выборке являются точными. Если оценщик не может понять, каким образом работает или способен работать конкретный механизм собственной защиты ФБО в рамках архитектуры системы, это может быть случаем, когда описание не является точным.

ИСО/МЭК 15408-3 ADV_ARC.1.5C: *В «Описании архитектуры безопасности» должно быть продемонстрировано, что ФБО не допускают возможности обхода функциональных возможностей, осуществляющих выполнение ФТБ.*

10.3.1.4.5 Шаг оценивания ADV_ARC.1-5

Оценщик должен исследовать «Описание архитектуры безопасности», чтобы сделать заключение о том, что в нем представлен анализ, адекватно описывающий, каким образом не допускается возможность обхода механизмов, осуществляющих выполнение ФТБ.

Невозможность обхода является свойством того, что функции безопасности ФБО (как специфицировано в ФТБ) всегда вызываются. Например, если управление доступом к файлам специфицировано как способность ФБО через ФТБ, не должно быть никаких интерфейсов, через которые к файлам можно получить доступ без вызова механизма управления доступом ФБО (например в виде интерфейса доступа к RAW-диску).

Описание того, каким образом обеспечивается невозможность обхода механизмов ФБО, обычно требует систематического доказательства, основанного на ФБО и ИФБО. Описание того, как работают ФБО (содержащееся в свидетельствах декомпозиции проекта, таких как функциональная спецификация, документация по проекту ОО) — наряду с информацией в краткой спецификации — предоставляет фоновую информацию, необходимую оценщику для понимания того, какие ресурсы защищаются и какие функции безопасности предоставляются. Функциональная спецификация предоставляет описания ИФБО, через которые можно получить доступ к ресурсам/функциям.

Оценщик оценивает предоставленное ему описание (и другую информацию, предоставленную разработчиком, например функциональную спецификацию), чтобы удостовериться, что никакой доступный интерфейс не может использоваться для обхода ФБО. Это означает, что каждый доступный интерфейс должен быть либо несвязанным с ФТБ, которые заявлены в ЗБ (и не должен взаимодействовать с чем-то, что используется для удовлетворения ФТБ) или, в ином случае, использует функцию безопасности, которая соответствующим образом описана в других свидетельствах разработки. Например, игра, скорее всего, не была бы связана с ФТБ, поэтому следовало бы привести объяснение тому, что она не может повлиять на безопасность. Доступ к пользовательским данным, однако, скорее всего, будет связан с ФТБ по управлению доступом, поэтому в объяснении следовало бы описать, как работают функции безопасности, когда они вызываются через интерфейсы доступа к данным. Такое описание необходимо приводить для каждого доступного интерфейса.

Можно привести следующий пример описания. Предположим, что ФБО обеспечивают защиту файлов. Также предположим, что, хотя «традиционный» системный вызов ИФБО для открытия, чтения и записи в файл вызывает механизм защиты файла, описанный в проекте ОО, существует ИФБО, который позволяет получить доступ к средству обработки пакетных заданий (создающему пакетные задания, удаляющему задания, изменяющему неотработанные задания). Оценщику следует быть в состоянии сделать на основании предоставленного производителями описания заключение о том, что этот ИФБО вызывает такие же механизмы защиты, что и «традиционные» интерфейсы. Это может быть

сделано, например путем ссылки на соответствующие подразделы проекта ОО, где указано, каким образом ИФБО средства обработки пакетных заданий достигает своих целей безопасности.

На этом же примере предположим, что есть ИФБО, единственное назначение которого состоит в том, чтобы показывать время суток. Оценщику следует сделать заключение о том, что в описании адекватно утверждается, что этот ИФБО не может управлять какими-либо защищенными ресурсами и не вызывает функции безопасности.

Другой пример обхода — это когда предполагается, что ФБО поддерживают конфиденциальность криптографического ключа (который допускается использовать для криптографических операций, но недопустимо производить операции по его чтению и записи). Если у злоумышленника есть возможность прямого физического доступа к устройству, он может быть в состоянии провести атаку по сторонним каналам, например атаку по энергопотреблению, атаку по времени или даже по электромагнитному излучению от устройства, и на основании этих данных вывести ключ.

Если такие сторонние каналы присутствуют, в демонстрацию следует включить адресацию к препятствующим возникновению этих сторонних каналов механизмам, таким как рандомизированные внутренние часы, технология двойной линии и т. д. Верификация таких механизмов проводится на комбинации доводов, основанных только на проектной документации, и результатов тестирования.

В качестве последнего примера использования функций безопасности, а не защищенного ресурса, рассмотрим ЗБ, которое содержит раздел FCO_NRO.2 «Принудительное доказательство отправления», где представлено требование, чтобы в ФБО были представлены свидетельства отправления для типов информации, определенных в ЗБ. Предположим, что к «типам информации» относится вся информация, которую ОО посылает через электронную почту. В этом случае оценщику следует исследовать описание, чтобы удостовериться, что все ИФБО, которые могут быть вызваны для отправки электронного письма, осуществляют функцию «свидетельство отправления» с должной степенью детализации. Описание может ссылаться на руководство пользователя для выявления всех мест отправления писем электронной почты (например, почтовая программа, уведомления скриптов/пакетных заданий) и затем того, как каждое из этих мест вызывает функцию генерации свидетельств.

Оценщику также следует удостовериться, что описание является всесторонним, т. е. в нём каждый интерфейс проанализирован относительно всего набора предъявляемых ФТБ. От оценщика может потребоваться исследовать сопроводительную информацию (функциональную спецификацию, проект ОО, другие части «Описания архитектуры безопасности», руководство пользователя по эксплуатации, и, возможно, даже представление реализации, как предоставлено для ОО) для вынесения заключения о том, что в описании правильно отражены все аспекты интерфейса. Оценщику следует рассмотреть, на какие ФТБ может влиять тот или иной ИФБО (из описания ИФБО и его реализации в сопроводительной документации), а затем исследовать описание, чтобы вынести заключение о том, охвачены ли описанием эти аспекты.

10.4 Функциональная спецификация (ADV_FSP)

10.4.1 Подвид деятельности по оценке (ADV_FSP.1)

10.4.1.1 Цели

Цель данного подвида деятельности — сделать заключение, предоставил ли разработчик описание верхнего уровня хотя бы для осуществляющих и поддерживающих ФТБ ИФБО, в терминах описаний их параметров. Других свидетельств, от которых может ожидаться возможность измерения точности данных описаний, не требуется; оценщик только удостоверяется, что описания кажутся правдоподобными.

10.4.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) руководство пользователя по эксплуатации.

10.4.1.3 Действие ADV_FSP.1.1E

ИСО/МЭК 15408-3 ADV_FSP.1.1C: *В функциональной спецификации должны описываться назначение и метод использования для каждого из ИФБО, осуществляющего или поддерживающего выполнение ФТБ.*

10.4.1.3.1 Шаг оценивания ADV_FSP.1-1

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней указано назначение каждого из ИФБО, осуществляющего или поддерживающего выполнение ФТБ из осуществляющих и поддерживающих ИФБО.

Назначение ИФБО — это общее утверждение, кратко описывающее функциональные возможности, предоставляемые интерфейсом. Не подразумевается, что оно должно быть полным изложением всех действий и результатов, относящихся к интерфейсу, а, скорее, оно должно помочь читателю составить общее представление о предполагаемом использовании данного интерфейса. Оценщику следует не только сделать заключение о том, что такое назначение существует, но и что оно точно отражает ИФБО с учетом другой информации об интерфейсе, такой как описание его параметров; это может быть сделано вместе с другими шагами оценивания для этого компонента.

Если действие, доступное через интерфейс, играет роль в осуществлении какой-либо политики безопасности ОО (то есть, если одно из действий интерфейса может быть прослежено к одному из ФТБ, предъявляемому к ФБО), то этот интерфейс — осуществляющий ФТБ. Это относится не только к политикам управления доступом, но также и к любым функциям, определенным одним из ФТБ, содержащимся в ЗБ. Следует отметить, что у интерфейса могут быть различные действия и результаты его вызова, некоторые из которых могут быть осуществляющими ФТБ, а некоторые — нет.

Интерфейсы (или действия, доступные через связанный с ними интерфейс) тех действий, от которых зависят функции, осуществляющие выполнение ФТБ, но от которых требуется только правильное функционирование для поддержания выполнения политик безопасности ОО, называют интерфейсами, поддерживающими выполнение ФТБ. Интерфейсы действий, от которых никак не зависят функции, осуществляющие выполнение ФТБ, относятся к не влияющим на выполнение ФТБ.

Следует отметить, что для того, чтобы интерфейс был отнесен к поддерживающим или не влияющим на выполнение ФТБ, он не должен включать в себя действия и результаты, осуществляющие выполнение ФТБ. Напротив, осуществляющий выполнение ФТБ интерфейс может включать поддерживающие выполнение ФТБ действия (например возможность выставить время в системе может быть действием интерфейса, осуществляющего выполнение ФТБ, но если этот же интерфейс используется для отображения даты в системе, то этот сервис может быть только поддерживающим выполнение ФТБ). В качестве яркого примера интерфейса, исключительно поддерживающего выполнение ФТБ можно привести интерфейс системных вызовов, который используют как недоверенные пользователи, так и часть ФБО, запускаемых в пользовательском режиме.

На этом уровне представления маловероятно, что разработчик предпримет усилия для категорирования и идентификации интерфейсов как осуществляющих и поддерживающих выполнение ФТБ. В случае, если это все-таки было сделано, оценщику следует верифицировать, что в сопроводительной документации (например в руководстве пользователя по эксплуатации) допускается, что эта идентификация правильна. Следует отметить, что действия по идентификации необходимы для нескольких шагов оценивания этого компонента.

В более вероятном случае, когда разработчик не идентифицировал интерфейсы по указанным категориям, оценщик должен сначала самостоятельно осуществить их идентификацию, а затем определить, присутствует ли требуемая информация (для этого шага оценивания — информация о назначении). И в этом случае из-за нехватки сопутствующих свидетельств такая идентификация будет трудновыполнимой и будет иметь низкий уровень доверия тому, что все соответствующие интерфейсы правильно идентифицированы. Тем не менее оценщику следует исследовать другие доступные свидетельства по ОО, чтобы обеспечить как можно более полный и подробный охват.

10.4.1.3.2 Шаг оценивания ADV_FSP.1-2

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней содержится описание метода использования для каждого из осуществляющих и поддерживающих ИФБО.

См. пояснение по поводу идентификации осуществляющих и поддерживающих выполнение ФТБ интерфейсов в шаге оценивания ADV_FSP.1-1.

Метод использования для ИФБО предоставляет краткую информацию по поводу того, каким образом в результате управления интерфейсом вызывают действия и получают результаты, связанные с ИФБО. Оценщику следует посредством чтения материалов функциональной спецификации вынести заключение о том, как использовать каждый интерфейс. Это не обязательно означает, что для каждого ИФБО нужен отдельный метод использования, поскольку можно, например описать в общем, как происходит системный вызов ядра, а затем идентифицировать каждый интерфейс, используя общий для всех интерфейсов стиль. Различные типы интерфейсов требуют различных спецификаций по методу их использования. У интерфейсов программирования приложений, сетевых протоколов, параметров системной конфигурации и шины аппаратных средств абсолютно разные методы использования, и это следует учитывать разработчику при разработке функциональной спецификации, так же, как и оценщику при проведении её оценки.

Для администрирующих интерфейсов, функции которых документированы как недоступные недоверенным пользователям, оценщик удостоверяется в том, что метод, благодаря которому данные функции являются недоступными таким пользователям, описан в функциональной спецификации. Следует отметить, что разработчику необходимо протестировать эту недоступность при проведении испытаний.

ИСО/МЭК 15408-3 ADV_FSP.1.2C: *В функциональной спецификации должны быть идентифицированы все параметры, связанные с каждым ИФБО, осуществляющим или поддерживающим ФТБ.*

10.4.1.3.3 Шаг оценивания ADV_FSP.1-3

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, идентифицированы ли в ней все параметры, связанные с каждым ИФБО, осуществляющим или поддерживающим ФТБ.

См. пояснение по поводу идентификации осуществляющих и поддерживающих выполнение ФТБ интерфейсов в шаге оценивания ADV_FSP.1-1.

Оценщик исследует функциональную спецификацию, чтобы сделать заключение, что в ней описаны все параметры для идентифицированных ИФБО. Параметры — явные исходные данные или данные на выходе интерфейса, которые контролируют режим функционирования этого интерфейса. Например, параметрами являются: аргументы, поставляемые интерфейсу программирования приложений; различные поля в пакете для данного сетевого протокола; индивидуальные значения ключа в реестре Windows; сигналы, проходящие через контакты чипа и т. д.

В то время как трудно получить достаточно большую степень доверия, что все параметры для применяемого ИФБО были идентифицированы, оценщику следует также проверить другие свидетельства, предоставленные для оценки (например руководство пользователя по эксплуатации) на предмет того, есть ли там описания режима функционирования интерфейса или дополнительных параметров, отсутствующие в функциональной спецификации.

ИСО/МЭК 15408-3 ADV_FSP.1.3C: *В функциональной спецификации должно приводиться обоснование неявного категорирования интерфейсов как не влияющих на выполнение ФТБ.*

10.4.1.3.4 Шаг оценивания ADV_FSP.1-4

Оценщик должен исследовать обоснование, предоставленное разработчиком для неявной классификации интерфейсов как не влияющих на выполнение ФТБ, чтобы сделать заключение о том, что это обоснование является точным.

В случае, если разработчик предоставил соответствующую документацию для проведения анализа, требуемого по остальным шагам оценивания этого компонента, явно не идентифицируя ИФБО как осуществляющие или поддерживающие ФТБ, этот шаг оценивания следует считать удовлетворенным.

Этот шаг оценивания предназначен для тех случаев, когда разработчик не описал часть ИФБО, утверждая, что они не влияют на выполнение ФТБ и поэтому не являются предметом предъявления требований данного компонента. В этом случае разработчик предоставляет обоснование для этой характеристики с достаточной степенью детализации для понимания оценщиком обоснования, особенностей затрагиваемых интерфейсов (например их функции верхнего уровня в отношении ОО, такие как «управление палитрой цветов»), и то, что заявление о том, что интерфейсы являются не влияющими на выполнение ФТБ, поддержано. Учитывая уровень доверия, оценщику не следует ожидать более высокой степени детализации, чем при описании осуществляющих или поддерживающих ФТБ интерфейсов; фактически детализации следует быть намного меньшей. В большинстве случаев к отдельным интерфейсам не обязательно обращаться в предоставленном разработчиком подразделе «Обоснование».

ИСО/МЭК 15408-3 ADV_FSP.1.4C: *В прослеживании должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.*

10.4.1.3.5 Шаг оценивания ADV_FSP.1-5

Оценщик должен проверить, что прослеживание соотносит ФТБ с соответствующими ИФБО.

Прослеживание предоставляется разработчиком в качестве руководства по тому, какие ИФБО относятся к каким ФТБ. Это прослеживание может быть представлено в простом виде например в виде таблицы; оно используется в качестве исходных данных для оценщика при использовании в последующих шагах оценивания, в которых оценщик верифицирует полноту и точность этого прослеживания.

10.4.1.4 Действие ADV_FSP.1.2E

10.4.1.4.1 Шаг оценивания ADV_FSP.1-6

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она полным отображением ФТБ.

Чтобы удостовериться, что все ФТБ охвачены функциональной спецификацией, а также анализом покрытия тестами, оценщик может основываться на прослеживании, предоставленном разработчиком

(см. ADV_FSP.1-5 для прослеживания между ФТБ для ОО и ИФБО). Следует учесть, что такое прослеживание иногда необходимо представлять на уровне детализации ниже, чем уровень детализации компонента или даже элемента требований, из-за операций (назначения, уточнения, выбора), выполняемых над функциональным требованием автором ЗБ.

Например, компонент FDP_ACC.1 содержит элемент с операциями назначения. Если бы в ЗБ содержалось, например десять правил в отношении назначения для данного компонента FDP_ACC.1, и эти правила были бы охвачены тремя различными ИФБО, то для оценщика некорректно было бы проследить FDP_ACC.1 к ИФБО A, B и C и утверждать о завершении шага оценивания. Вместо этого оценщик должен был бы проследить FDP_ACC.1 (правило 1) к ИФБО A; FDP_ACC.1 (правило 2) к ИФБО B и т.д. Может иметь место и случай, когда интерфейс является интерфейсом адаптера (например IOCTL) и тогда прослеживание должно быть определенным к набору параметров для данного интерфейса.

Оценщик должен осознавать, что для требований, которые незначительно проявляются или не проявляются вовсе на границах ФБО (например FDP_RIP), не ожидается, что эти требования будут прослежены к ИФБО. Анализ таких требований будет выполняться в процессе анализа проекта ОО (ADV_TDS), когда он включен в ЗБ. Важно отметить, что так как параметры, связанные с ИФБО, должны быть полностью специфицированы, оценщику следует быть в состоянии сделать заключение о том, все ли аспекты ФТБ реализованы на интерфейсном уровне.

10.4.1.4.2 Шаг оценивания ADV_FSP.1-7

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, что она является точным отображением ФТБ.

Для каждого функционального требования в ЗБ, которое оказывает видимый эффект на границах ФБО, информация в связанном с ним ИФБО специфицирует требуемые функции, описанные в требовании. Например, если в ЗБ содержится требование наличия списков контроля доступа и единственный ИФБО, прослеживаемый к этому требованию, специфицирует функции Unix-подобных разрядов защиты, тогда функциональная спецификация не является точной в отношении требований.

Оценщик должен осознавать, что для требований, которые незначительно проявляются или не проявляются вовсе на границах ФБО (например FDP_RIP), не ожидается, что эти требования будут прослежены к ИФБО. Анализ таких требований будет выполняться в процессе анализа проекта ОО (ADV_TDS), когда он включается в ЗБ.

10.4.2 Подвид деятельности по оценке (ADV_FSP.2)

10.4.2.1 Цели

Цель данного подвида деятельности — сделать заключение, предоставил ли разработчик описание ИФБО в терминах их назначения, метода использования и параметров. Кроме того, для каждого осуществляющего ФТБ интерфейса ФБО описываются действия, результаты и сообщения об ошибках, осуществляющие выполнение ФТБ.

10.4.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности, требуемыми шагами оценивания, являются:

a) ЗБ;

b) функциональная спецификация;

c) проект ОО.

Свидетельствами оценки для этого подвида деятельности, которые используются в случае их включения в ЗБ по ОО, являются:

a) описание архитектуры безопасности;

b) руководство пользователя по эксплуатации.

10.4.2.3 Действие ADV_FSP.2.1E

ИСО/МЭК 15408-3 ADV_FSP.2.1C: *В функциональной спецификации должны быть полностью представлены ФБО.*

10.4.2.3.1 Шаг оценивания ADV_FSP.2-1

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней полностью представлены ФБО.

Идентификация ИФБО — необходимая предпосылка для всех действий данного подвида деятельности. Для идентификации ИФБО должны быть идентифицированы ФБО (в рамках шагов оценивания семейства ADV_TDS «Проект ОО»). Эта деятельность может быть проведена на высоком уровне, чтобы удостовериться, что не упущены крупные группы интерфейсов (сетевых протоколов, аппаратных средств, файлов конфигурации) или на низком уровне — как часть оценки функциональной спецификации.

При проведении данного шага оценивания оценщик делает заключение о том, что все части ФБО описаны в терминах интерфейсов, перечисленных в функциональной спецификации. Для всех частей ФБО следует иметь соответствующее описание интерфейсов или, при отсутствии соответствующих интерфейсов для части ФБО, оценщик делает заключение, что такое отсутствие допустимо и приемлемо.

ИСО/МЭК 15408-3 ADV_FSP.2.2C: *В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.*

10.4.2.3.2 Шаг оценивания ADV_FSP.2-2

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней указано назначение каждого ИФБО.

Назначение ИФБО — это общее утверждение, кратко описывающее функциональные возможности, предоставляемые интерфейсом. Не подразумевается, что оно должно быть полным изложением всех действий и результатов, относящихся к интерфейсу, а, скорее, оно должно помочь читателю составить общее представление о предполагаемом использовании данного интерфейса. Оценщику следует не только сделать заключение о том, что такое назначение существует, и что оно точно отражает ИФБО, с учетом другой информации об интерфейсе, такой как описание действий и сообщений об ошибках.

10.4.2.3.3 Шаг оценивания ADV_FSP.2-3

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней содержится описание метода использования для каждого ИФБО.

Метод использования для ИФБО предоставляет краткую информацию по поводу того, каким образом в результате управления интерфейсом вызывают действия и получают результаты, связанные с ИФБО. Оценщику следует посредством чтения материалов в функциональной спецификации вынести заключение о том, как использовать каждый интерфейс. Это не обязательно означает, что для каждого ИФБО нужен отдельный метод использования, поскольку можно, например описать в общем, как происходит системный вызов ядра, а затем идентифицировать каждый интерфейс, используя общий для всех интерфейсов стиль. Различные типы интерфейсов требуют различных спецификаций по методу их использования. У интерфейсов программирования приложений (API), сетевых протоколов, параметров системной конфигурации и шины аппаратных средств абсолютно разные методы использования, и это следует учитывать разработчику при разработке функциональной спецификации, так же, как и оценщику при проведении её оценки.

Для интерфейсов администрирования, функции которых документированы как недоступные недоверенным пользователям, оценщик удостоверяется в том, что метод, благодаря которому данные функции являются недоступными таким пользователям, описан в функциональной спецификации. Следует отметить, что разработчику необходимо протестировать эту недоступность при проведении испытаний.

Оценщику следует не только сделать заключение о существовании подмножества описаний методов использования, но и о том, что описания точно охватывают каждый ИФБО.

ИСО/МЭК 15408-3 ADV_FSP.2.3C: *В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.*

10.4.2.3.4 Шаг оценивания ADV_FSP.2-4

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение, полностью ли идентифицированы в нем все параметры, связанные с каждым ИФБО.

Оценщик исследует функциональную спецификацию, чтобы сделать заключение, что в ней описаны все параметры для каждого ИФБО. Параметры — явные исходные данные или данные на выходе интерфейса, которые контролируют режим функционирования этого интерфейса. Например, параметрами являются: аргументы, поставляемые интерфейсу программирования приложений; различные поля в пакете для данного сетевого протокола; индивидуальные значения ключа в реестре Windows; сигналы, проходящие через контакты чипа и т. д.

Для вынесения заключения о том, что все данные параметры присутствуют в ИФБО, оценщику следует исследовать остальные описания интерфейса (действия, сообщения об ошибках и т. д.) и сделать заключение, что эффекты этих параметров перечислены в описании. Оценщику следует также проверить другие свидетельства, предоставленные для оценки (например проект ОО, описание архитектуры безопасности, руководство пользователя по эксплуатации, представление реализации) на предмет того, есть ли там описания режимов функционирования интерфейса или дополнительных параметров, отсутствующие в функциональной спецификации.

10.4.2.3.5 Шаг оценивания ADV_FSP.2-5

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение, полно ли и точно ли описаны в нем все параметры, связанные с каждым ИФБО.

Как только все параметры идентифицированы, оценщику нужно удостовериться, что они описаны точно, и что описание параметров проведено полно. Описание параметра некоторым значащим образом определяет, что представляет собой данный параметр. Например, интерфейс *foo (i)* может быть описан как имеющий «параметр *i*, который является целым числом»; но такое описание параметра не приемлемо. Более приемлемое описание — «параметр *i* — целое число, указывающее на число пользователей, которые в настоящий момент зарегистрированы в системе».

Для вынесения заключения о том, что описание параметра является полным, оценщику следует исследовать остальные описания интерфейса (назначение, метод использования, действия интерфейса, сообщения об ошибках и т. д.) и сделать заключение о том, что описания этих параметров перечислены в описании. Оценщику следует также проверить другие предоставленные свидетельства (например проект ОО, проект архитектуры, руководство пользователя по эксплуатации, представление реализации) на предмет того, есть ли там описания режима функционирования интерфейса или его дополнительных параметров, отсутствующие в функциональной спецификации.

ИСО/МЭК 15408-3 ADV_FSP.2.4C: *Для каждого ИФБО, осуществляющего выполнение ФТБ, функциональная спецификация должна содержать описание связанных с данным ИФБО действий, осуществляющих выполнение ФТБ.*

10.4.2.3.6 Шаг оценивания ADV_FSP.2-6

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение о том, что в нем полно и точно описаны все осуществляющие выполнение ФТБ действия, связанные с осуществляющими выполнение ФТБ интерфейсами.

Если действие, доступное через интерфейс, может быть прослежено к одному из ФТБ по ФБО, то этот интерфейс является осуществляющим выполнение ФТБ. Это относится не только к политикам управления доступом, но также и к любым функциям, определенным одним из ФТБ, содержащимся в ЗБ. Следует отметить, что у интерфейса могут быть различные действия и результаты его вызова, некоторые из которых могут быть осуществляющими ФТБ, а некоторые — нет.

От разработчика не требуется «маркировать» интерфейсы как осуществляющие выполнение ФТБ, и также не требуется идентифицировать доступные через интерфейс действия как осуществляющие выполнение ФТБ. Оценщик обязан исследовать свидетельства, представленные разработчиком, и сделать заключение о том, что требуемая информация в них присутствует. В случае, если разработчик идентифицировал осуществляющие выполнение ФТБ ИФБО и доступные через эти ИФБО осуществляющие выполнение ФТБ действия, оценщик должен оценить полноту и точность данной идентификации, основываясь на информации, поставленной для оценки (например на проекте ОО, описании архитектуры безопасности, руководстве пользователя по эксплуатации) и информации, представленной для данных интерфейсов (параметры и описания этих параметров, сообщения об ошибках и т. д.).

В этом случае (когда разработчик предоставил только касающуюся осуществления выполнения ФТБ информацию для осуществляющих выполнение ФТБ интерфейсов) оценщик также удостоверяется в том, что все интерфейсы правильно категорированы путем исследования информации, предоставленной для оценки (например проекта ОО, описания архитектуры безопасности, руководства пользователя по эксплуатации), и информации по интерфейсам (параметров и описаний этих параметров например, не идентифицированным как осуществляющие выполнение ФТБ.

В случае, если разработчик предоставил информацию одинаковой степени полноты и детализации для всех интерфейсов, оценщик выполняет такой же анализ, описанный в предыдущих параграфах. Оценщику следует сделать заключение о том, какие интерфейсы являются осуществляющими выполнение ФТБ, а какие не являются, а затем удостовериться в том, что осуществляющие выполнение ФТБ аспекты осуществляющих выполнение ФТБ действий правильно описаны.

Осуществляющие выполнение ФТБ действия — это те, которые видимы в любом внешнем интерфейсе и предусматривают удовлетворение предъявляемых ФТБ. Например, если требования по аудиту включены в ЗБ, то связанные с аудитом действия являются осуществляющими выполнение ФТБ и поэтому должны быть описаны, даже если результат этого действия обычно невозможно наблюдать через вызванный интерфейс (при проведении аудита обычной является ситуация, когда пользовательское действие в одном интерфейсе производит контрольный отчет, видимый только через другой интерфейс).

Требуемый уровень описания — достаточный для того, чтобы читатель понял роль действий ИФБО по отношению к ФТБ. Оценщику следует иметь в виду, что рекомендуется, чтобы описание было детализировано в достаточной мере для поддержки создания (и оценки) тестовых ситуаций для данного интерфейса. Если описание неясно или недостаточно детализировано и поэтому значимое тести-

рование ИФБО не может быть проведено, скорее всего, описание является несоответствующим предъявляемым к нему требованиям.

ИСО/МЭК 15408-3 ADV_FSP.2.5C: *Для ИФБО, осуществляющих выполнение ФТБ, функциональная спецификация должна содержать описание сообщений о непосредственных ошибках, возникающих в результате функционирования, связанного с действиями, осуществляющими выполнение ФТБ.*

10.4.2.3.7 Шаг оценивания ADV_FSP.2-7

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение о том, что в нем полно и точно описаны сообщения о связанных с осуществляющими выполнение ФТБ интерфейсами ошибках, которые могут быть последствием действий, осуществляющих выполнение ФТБ.

Этот шаг оценивания следует выполнять вместе с шагом оценивания ADV_FSP.2-6 или после него, чтобы удостовериться, что набор осуществляющих выполнение ФТБ интерфейсов и осуществляющих выполнение ФТБ действий правильно идентифицирован. Разработчик может предоставить больше информации, чем требуется (например все сообщения об ошибках, связанные с каждым интерфейсом). В этом случае оценщику следует ограничиться при оценке полноты и точности этой информации рассмотрением только той информации, которая относится к осуществляющим выполнение ФТБ действиям осуществляющих выполнение ФТБ интерфейсов.

Ошибки могут принимать различные формы, в зависимости от описываемого интерфейса. В случае интерфейса программирования приложений интерфейс сам может вернуть код ошибки, установить состояние глобальной ошибки или определенный параметр с кодом ошибки. В случае файла конфигурации неправильно настроенный параметр может привести к появлению в системном журнале сообщения об ошибке. В случае аппаратных средств, например шины ввода/вывода, возникновение ошибки может подать на шину сигнал или вызвать особое состояние центрального процессора.

Ошибки (и связанные с ними сообщения об ошибках) проявляются через запрос интерфейса. Обработка, которая происходит в ответ на запрос интерфейса, может столкнуться с некоторыми условиями, вызывающими ошибку и сообщение об этой ошибке (путем определенного механизма, специфического для данной реализации). В некоторых случаях это может быть возвращаемое самим интерфейсом значение; в других случаях глобальное значение может быть назначено и проверено после запроса интерфейса. Скорее всего, в ОО будет много сообщений об ошибках низкого уровня, которые являются результатом фундаментальных условий для ресурсов, например «недостаточно места на диске» или «ресурс заблокирован». Несмотря на то, что эти сообщения об ошибках могут быть прослежены к большому количеству ИФБО, их можно использовать для выявления тех случаев, когда часть описания интерфейса была опущена. Например, если есть ИФБО, который выдает сообщение «недостаточно места на диске», но для которого не представлено ясное описание того, почему этому ИФБО следует позволять получение доступа к диску, оценщику может потребоваться исследовать другие свидетельства (семейств ADV_ARC «Архитектура безопасности», ADV_TDS «Проект ОО»), связанные с этим ИФБО, чтобы сделать заключение о том, является ли точным его описание.

Чтобы вынести заключение о том, что описание сообщений об ошибках ИФБО составлено точно и полно, оценщик сравнивает длину данного описания интерфейса с другими представленными для оценки свидетельствами (например с проектом ОО, описанием архитектуры безопасности, руководством пользователя по эксплуатации), а также с другими свидетельствами по данному ИФБО (его параметрами, результатами шага оценивания ADV_FSP.2-6).

ИСО/МЭК 15408-3 ADV_FSP.2.6C: *В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.*

10.4.2.3.8 Шаг оценивания ADV_FSP.2-8

Оценщик должен проверить, что прослеживание соотносит ФТБ с соответствующими ИФБО.

Прослеживание предоставляется разработчиком в качестве руководства для определения того, каким образом ФТБ связаны с ИФБО. Это прослеживание может быть представлено в простом вид например в виде таблицы; оно используется в качестве исходных данных для оценщика для использования в последующих шагах оценивания, в которых оценщик верифицирует полноту и точность этого прослеживания.

10.4.2.4 Действие ADV_FSP.2.2E

10.4.2.4.1 Шаг оценивания ADV_FSP.2-9

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она полным отображением ФТБ.

Чтобы удостовериться, что все ФТБ охвачены функциональной спецификацией, а также анализом покрытия тестами, оценщик может основываться на прослеживании, предоставленном разработчиком

(см. ADV_FSP.1-5 для прослеживания между ФТБ для ОО и ИФБО). Следует учесть, что такое прослеживание иногда необходимо представлять на уровне детализации ниже, чем уровень детализации компонента или даже элемента требований, из-за операций (назначения, уточнения, выбора), выполняемых над функциональным требованием автором ЗБ.

Например, компонент FDP_ACC.1 содержит элемент с операциями назначения. Если бы в ЗБ содержалось, например десять правил в отношении назначения для данного компонента FDP_ACC.1 и эти правила были бы охвачены тремя различными ИФБО, то для оценщика некорректно было бы проследить FDP_ACC.1 к ИФБО A, B и C и утверждать о завершении шага оценивания. Вместо этого оценщик должен был бы проследить FDP_ACC.1 (правило 1) к ИФБО A; FDP_ACC.1 (правило 2) к ИФБО B и т. д. Может иметь место и случай, когда интерфейс является интерфейсом адаптера (например IOCTL), и тогда прослеживание должно быть определенным к набору параметров для данного интерфейса.

Оценщик должен осознавать, что для требований, которые незначительно проявляются или не проявляются вовсе на границах ФБО (например FDP_RIP), не ожидается, что эти требования будут прослежены к ИФБО. Анализ таких требований будет выполняться в процессе анализа проекта ОО (ADV_TDS), когда он включен в ЗБ. Важно отметить, что, так как параметры, связанные с ИФБО, должны быть полностью специфицированы, оценщику следует быть в состоянии сделать заключение о том, все ли аспекты ФТБ реализованы на интерфейсном уровне.

10.4.2.4.2 Шаг оценивания ADV_FSP.2-10

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, что она является точным отображением ФТБ.

Для каждого функционального требования в ЗБ, которое оказывает видимый эффект на границах ФБО, информация в связанном с ним ИФБО специфицирует требуемые функции, описанные в требовании. Например, если в ЗБ содержится требование наличия списков контроля доступа и единственный ИФБО, прослеживаемый к этому требованию, специфицирует функции Unix-подобных разрядов защиты, тогда функциональная спецификация не является точной в отношении требований.

Оценщик должен осознавать, что для требований, которые незначительно проявляются или не проявляются вовсе на границах ФБО (например FDP_RIP), не ожидается, что эти требования будут прослежены к ИФБО. Анализ таких требований будет выполняться в процессе анализа проекта ОО (ADV_TDS), когда он включен в ЗБ.

10.4.3 Подвид деятельности по оценке (ADV_FSP.3)

10.4.3.1 Цели

Цель данного подвида деятельности — сделать заключение, предоставил ли разработчик описание ИФБО в терминах их назначения, метода использования и параметров. Кроме того, действия, результаты и сообщения об ошибках для каждого ИФБО описываются в достаточной мере для того, чтобы была возможность сделать заключение о том, являются ли они осуществляющими выполнение ФТБ, причем интерфейсы, осуществляющие выполнение ФТБ, описываются с большей степенью детализации, чем остальные ИФБО.

10.4.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности, требуемыми шагами оценивания, являются:

a) ЗБ;

b) функциональная спецификация;

c) проект ОО.

Свидетельствами оценки для этого подвида деятельности, которые используются в случае их включения в ЗБ по ОО, являются:

a) описание архитектуры безопасности;

b) представление реализации;

c) описание внутреннего состава ФБО;

d) руководство пользователя по эксплуатации.

10.4.3.3 Действие ADV_FSP.3.1E

ИСО/МЭК 15408-3 ADV_FSP.3.1C: *В функциональной спецификации должны быть полностью представлены ФБО.*

10.4.3.3.1 Шаг оценивания ADV_FSP.3-1

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней полностью представлены ФБО.

Идентификация ИФБО — необходимая предпосылка для всех действий данного подвида деятельности. Для идентификации ИФБО должны быть идентифицированы ФБО (в рамках шагов оценивания семейства ADV_TDS «Проект ОО»). Эта деятельность может быть проведена на высоком уровне, чтобы

удостовериться, что не упущены крупные группы интерфейсов (сетевых протоколов, аппаратных средств, файлов конфигурации) или на низком уровне — как часть оценки функциональной спецификации.

При проведении данного шага оценивания оценщик делает заключение о том, что все части ФБО описаны в терминах интерфейсов, перечисленных в функциональной спецификации. Для всех частей ФБО следует иметь соответствующее описание интерфейсов или, при отсутствии соответствующих интерфейсов для части ФБО, оценщик делает заключение, что такое отсутствие допустимо и приемлемо.

ИСО/МЭК 15408-3 ADV_FSP.3.2C: *В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.*

10.4.3.3.2 Шаг оценивания ADV_FSP.3-2

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней указано назначение каждого ИФБО.

Назначение ИФБО — это общее утверждение, кратко описывающее функциональные возможности, обеспеченные интерфейсом. Не подразумевается, что оно не должно быть полным изложением всех действий и результатов, относящихся к интерфейсу, а, скорее, оно должно помочь читателю составить общее представление о предполагаемом использовании данного интерфейса. Оценщику следует не только сделать заключение о том, что такое назначение существует, но и что оно точно отражает ИФБО, с учетом другой информации об интерфейсе, такой как описание действий и сообщений об ошибках.

10.4.3.3.3 Шаг оценивания ADV_FSP.3-3

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней содержится описание метода использования для каждого ИФБО.

Метод использования для ИФБО предоставляет краткую информацию по поводу того, каким образом в результате управления интерфейсом вызывают действия и получают результаты, связанные с ИФБО. Оценщику следует быть в состоянии посредством чтения материалов в функциональной спецификации вынести заключение о том, как использовать каждый интерфейс. Это не обязательно означает, что для каждого ИФБО нужен отдельный метод использования, поскольку можно, например описать в общем, как происходит системный вызов ядра, а затем идентифицировать каждый интерфейс, используя общий для всех интерфейсов стиль. Различные типы интерфейсов требуют различных спецификаций по методу их использования. У интерфейсов программирования приложений, сетевых протоколов, параметров системной конфигурации и шины аппаратных средств абсолютно разные методы использования, и это следует учитывать разработчику при разработке функциональной спецификации, так же, как и оценщику при проведении её оценки.

Для администрирующих интерфейсов, функции которых документированы как недоступные недоверенным пользователям, оценщик удостоверяется в том, что метод, благодаря которому данные функции являются недоступными таким пользователям, описан в функциональной спецификации. Следует отметить, что разработчику необходимо протестировать эту недоступность при проведении испытаний.

Оценщику следует не только сделать заключение о существовании подмножества описаний методов использования, но и о том, что описания точно охватывают каждый ИФБО.

ИСО/МЭК 15408-3 ADV_FSP.3.3C: *В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.*

10.4.3.3.4 Шаг оценивания ADV_FSP.3-4

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение, полностью ли идентифицированы в нем все параметры, связанные с каждым ИФБО.

Оценщик исследует функциональную спецификацию, чтобы сделать заключение, что в ней описаны все параметры для каждого ИФБО. Параметры — явные исходные данные или данные на выходе интерфейса, которые контролируют режим функционирования этого интерфейса. Например, параметрами являются: аргументы, поставляемые интерфейсу программирования приложений; различные поля в пакете для данного сетевого протокола; индивидуальные значения ключа в реестре Windows; сигналы, проходящие через контакты чипа и т. д.

Для заключения о том, что все данные параметры присутствуют в ИФБО, оценщику следует исследовать остальные описания интерфейса (действия, сообщения об ошибках и т. д.) и сделать заключение о том, что эффекты этих параметров перечислены в описании. Оценщику следует также проверить другие свидетельства, предоставленные для оценки (например проект ОО, описание архитектуры безопасности, руководство пользователя по эксплуатации, представление реализации) на предмет того, есть ли там описания режима функционирования интерфейса или дополнительных параметров, отсутствующие в функциональной спецификации.

10.4.3.3.5 Шаг оценивания ADV_FSP.3-5

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение, полно ли и точно ли описаны в нем все параметры, связанные с каждым ИФБО.

Как только все параметры идентифицированы, оценщику нужно удостовериться, что они описаны точно и что описание параметров проведено полно. Описание параметра некоторым значащим образом определяет, что представляет собой данный параметр. Например, интерфейс *foo (i)* может быть описан как имеющий «параметр *i*, который является целым числом»; но такое описание параметра неприемлемо. Более приемлемое описание — «параметр *i* — целое число, указывающее на число пользователей, которые в настоящий момент зарегистрированы в системе».

Для вынесения заключения о том, что описание параметра является полным, оценщику следует исследовать остальные описания интерфейса (назначение, метод использования, действия интерфейса, сообщения об ошибках и т. д.) и сделать вывод о том, что описания этих параметров перечислены в описании. Оценщику следует также проверить другие предоставленные свидетельства (например проект ОО, проект архитектуры, руководство пользователя по эксплуатации, представление реализации) на предмет того, есть ли там описания режима функционирования интерфейса или его дополнительных параметров, отсутствующие в функциональной спецификации.

ИСО/МЭК 15408-3 ADV_FSP.3.4C: *Для каждого ИФБО, осуществляющего выполнение ФТБ, функциональная спецификация должна содержать описание связанных с данным ИФБО действий, осуществляющих выполнение ФТБ.*

10.4.3.3.6 Шаг оценивания ADV_FSP.3-6

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение о том, что в нем полно и точно описаны все осуществляющие выполнение ФТБ действия, связанные с осуществляющими выполнение ФТБ интерфейсами.

Если действие, доступное через интерфейс, может быть прослежено к одному из ФТБ по ФБО, то этот интерфейс является осуществляющим выполнение ФТБ. Это относится не только к политикам управления доступом, но также и к любым функциям, определенным одним из ФТБ, содержащимся в ЗБ. Следует отметить, что у интерфейса могут быть различные действия и результаты его вызова, некоторые из которых могут быть осуществляющими ФТБ, а некоторые — нет.

От разработчика не требуется «маркировать» интерфейсы как осуществляющие выполнение ФТБ и также не требуется идентифицировать доступные через интерфейс действия как осуществляющие выполнение ФТБ. Оценщик обязан исследовать свидетельства, представленные разработчиком, и сделать заключение о том, что требуемая информация в них присутствует. В случае, если разработчик идентифицировал осуществляющие выполнение ФТБ ИФБО и доступные через эти ИФБО осуществляющие выполнение ФТБ действия, оценщик должен оценить полноту и точность данной идентификации, основываясь на информации, поставленной для оценки (например на проекте ОО, описании архитектуры безопасности, руководстве пользователя по эксплуатации) и информации, представленной для данных интерфейсов (параметры и описания этих параметров, сообщения об ошибках и т. д.).

В этом случае (когда разработчик предоставил только касающуюся осуществления выполнения ФТБ информацию для осуществляющих выполнение ФТБ интерфейсов) оценщик также удостоверяется в том, что все интерфейсы правильно категорированы путем исследования информации, предоставленной для оценки (например проекта ОО, описания архитектуры безопасности, руководства пользователя по эксплуатации), и информации по интерфейсам (параметров и описаний этих параметров например, не идентифицированным как осуществляющие выполнение ФТБ.

В случае, если разработчик предоставил информацию одинаковой степени полноты и детализации для всех интерфейсов, оценщик выполняет такой же анализ, описанный в предыдущих параграфах. Оценщику следует сделать заключение о том, какие интерфейсы являются осуществляющими выполнение ФТБ, а какие не являются, а затем удостовериться в том, что осуществляющие выполнение ФТБ аспекты осуществляющих выполнение ФТБ действий правильно описаны.

Осуществляющие выполнение ФТБ действия — это те, которые видимы в любом внешнем интерфейсе и предусматривают удовлетворение предъявляемых ФТБ. Например, если требования по аудиту включены в ЗБ, то связанные с аудитом действия являются осуществляющими выполнение ФТБ и поэтому должны быть описаны, даже если результат этого действия обычно невозможно наблюдать через вызванный интерфейс (при проведении аудита обычной является ситуация, когда пользовательское действие в одном интерфейсе производит контрольный отчет, видимый только через другой интерфейс).

Под требуемым уровнем описания понимается достаточный для того, чтобы читатель понял роль действий ИФБО по отношению к ФТБ. Оценщику следует иметь в виду, что рекомендуется, чтобы опи-

сание было детализировано в достаточной степени для поддержки создания (и оценки) тестовых ситуаций для данного интерфейса. Если описание неясно или недостаточно детализировано и поэтому значимое тестирование ИФБО не может быть проведено, то, скорее всего, описание является несоответствующим предъявляемым к нему требованиям.

ИСО/МЭК 15408-3 ADV_FSP.3.5C: *Для каждого ИФБО, осуществляющего выполнение ФТБ, функциональная спецификация должна содержать описание сообщений о непосредственных ошибках, возникающих в результате влияющих на безопасность эффектов и нештатных ситуаций, связанных с вызовом данного ИФБО.*

10.4.3.3.7 Шаг оценивания ADV_FSP.3-7

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение о том, что в нем полно и точно описаны сообщения о связанных с осуществляющими выполнение ФТБ интерфейсами ошибках, которые могут быть последствием действий, осуществляющих выполнение ФТБ.

Этот шаг оценивания следует выполнять вместе с шагом оценивания ADV_FSP.3-6 или после него, чтобы удостовериться, что набор осуществляющих выполнение ФТБ интерфейсов правильно идентифицирован. Оценщику следует иметь в виду, что требования и связанные с ними шаги оценивания предписывают необходимость описания всех сообщений о непосредственных ошибках, связанных с ИФБО и действиями, осуществляющими выполнение ФТБ. На данном уровне доверия дополнительную информацию, полученную из описаний сообщений об ошибках, следует использовать для вынесения заключения о том, все ли аспекты осуществляющих выполнение ФТБ интерфейсов ФБО были описаны правильно. Например, если в связанном с ИФБО сообщении об ошибке (например в сообщении вида «в доступе отказано») указывается, что произошло действие или принято решение, осуществляющее выполнение ФТБ, но в описании осуществляющих выполнение ФТБ действий нет упоминания этого конкретного механизма, осуществляющего выполнение ФТБ, тогда описание может быть признано неполным.

Ошибки могут принимать различные формы в зависимости от описываемого интерфейса. В случае интерфейса программирования приложений интерфейс сам может вернуть код ошибки, установить состояние глобальной ошибки или определенный параметр с кодом ошибки. В случае файла конфигурации неправильно настроенный параметр может привести к появлению в системном журнале сообщения об ошибке. В случае аппаратных средств, например шины ввода/вывода, возникновение ошибки может подать на шину сигнал или вызвать особое состояние центрального процессора.

Ошибки (и связанные с ними сообщения об ошибках) проявляются через запрос интерфейса. Обработка, которая происходит в ответ на запрос интерфейса, может столкнуться с некоторыми условиями, вызывающими ошибку и сообщение об этой ошибке (путем определенного механизма, специфического для данной реализации). В некоторых случаях это может быть возвращаемое самим интерфейсом значение; в других случаях глобальное значение может быть назначено и проверено после запроса интерфейса. Скорее всего, в ОО будет много сообщений об ошибках низкого уровня, которые являются результатом фундаментальных условий для ресурсов, например «недостаточно места на диске» или «ресурс заблокирован». Несмотря на то, что сообщения об ошибках могут быть прослежены к большому количеству ИФБО, их можно использовать для выявления тех случаев, когда некоторые детали в описании интерфейса были опущены. Например, если есть ИФБО, который выдает сообщение «недостаточно места на диске», но для которого не представлено ясное описание того, почему этому ИФБО следует позволять получение доступа к диску, оценщику может потребоваться исследовать другие свидетельства (семейств ADV_ARC «Архитектура безопасности», ADV_TDS «Проект ОО»), связанные с этим ИФБО, чтобы сделать заключение о том, является ли точным его описание.

Чтобы вынести заключение о том, что описание сообщений об ошибках ИФБО составлено точно и полно, оценщик сравнивает длину данного описания интерфейса с другими представленными для оценки свидетельствами (например с проектом ОО, описанием архитектуры безопасности, руководством пользователя по эксплуатации), а также с другими свидетельствами по данному ИФБО (описанием осуществляющих выполнение ФТБ действий, кратким изложением поддерживающих и не влияющих на выполнение ФТБ действий и результатов).

ИСО/МЭК 15408-3 ADV_FSP.3.6C: *В функциональной спецификации должны быть приведены все связанные с каждым ИФБО действия, поддерживающие или не влияющие на выполнение ФТБ.*

10.4.3.3.8 Шаг оценивания ADV_FSP.3-8

Оценщик должен исследовать представление ИФБО, чтобы вынести заключение о том, что в нем приводится краткое описание связанных с каждым ИФБО действий, поддерживающих или не влияющих на выполнение ФТБ.

Цель этого шага оценивания состоит в том, чтобы детализировать описания осуществляющих выполнение ФТБ действий (которые приводятся в шаге оценивания ADV_FSP.3-6) и кратко описать все остальные действия (то есть те, которые не являются осуществляющими выполнение ФТБ). Это охватывает все поддерживающие и не влияющие на выполнение ФТБ действия, неважно, вызваны ли они осуществляющими выполнение ФТБ интерфейсами, поддерживающими или не влияющими на выполнение ФТБ. Такая краткая информация о поддерживающих и не влияющих на выполнение ФТБ действиях помогает получить более полную картину функций, обеспеченных ФБО, и должна использоваться оценщиком при определении того, верно ли категорированы действия или ИФБО.

Предоставляемая информация более абстрактна, чем требуемая для описания действий, осуществляющих выполнение ФТБ. Этой информации следует быть детализированной в достаточной степени для того, чтобы читатель мог понять суть действия, но описание не обязательно должно быть детализировано до такой степени, чтобы обеспечить, например возможность письменного тестирования. Для оценщика главное то, что информация должна быть достаточной для вынесения положительного заключения о том, что действие является поддерживающим или не влияющим на выполнение ФТБ. Если представленной информации для этого недостаточно, то краткое описание признается недостаточно полным, и необходимо получить больший объем информации.

ИСО/МЭК 15408-3 ADV_FSP.3.7C: *В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.*

10.4.3.3.9 Шаг оценивания ADV_FSP.3-9

Оценщик должен проверить, что прослеживание соотносит ФТБ с соответствующими ИФБО.

Прослеживание предоставляется разработчиком в качестве руководства для определения того, каким образом ФТБ связаны с ИФБО. Это прослеживание может быть представлено в простом виде, например в виде таблицы; оно используется в качестве исходных данных для оценщика при использовании в последующих шагах оценивания, в которых оценщик верифицирует полноту и точность этого прослеживания.

10.4.3.4 Действие ADV_FSP.3.2E

10.4.3.4.1 Шаг оценивания ADV_FSP.3-10

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она полным отображением ФТБ.

Чтобы удостовериться, что все ФТБ охвачены функциональной спецификацией, а также анализом покрытия тестами, оценщик может основываться на прослеживании, предоставленном разработчиком (см. ADV_FSP.3-9 для прослеживания между ФТБ для ОО и ИФБО). Следует учесть, что такое прослеживание иногда необходимо представлять на уровне детализации ниже, чем уровень детализации компонента или даже элемента требований из-за операций (назначения, уточнения, выбора), выполняемых над функциональным требованием автором ЗБ.

Например, компонент FDP_ACC.1 содержит элемент с операциями назначения. Если бы в ЗБ содержалось, например десять правил в отношении назначения для данного компонента FDP_ACC.1 и эти правила были бы охвачены тремя различными ИФБО, то для оценщика некорректно было бы проследить FDP_ACC.1 к ИФБО A, B и C и утверждать о завершении шага оценивания. Вместо этого оценщик должен был бы проследить FDP_ACC.1 (правило 1) к ИФБО A; FDP_ACC.1 (правило 2) к ИФБО B и т. д. Может иметь место и случай, когда интерфейс является интерфейсом адаптера (например IOCTL), и тогда прослеживание должно быть определенным к набору параметров для данного интерфейса.

Оценщик должен осознавать, что для требований, которые незначительно проявляются или не проявляются вовсе на границах ФБО (например FDP_RIP), не ожидается, что эти требования будут прослежены к ИФБО. Анализ таких требований будет выполняться в процессе анализа проекта ОО (ADV_TDS), когда он включен в ЗБ. Важно отметить, что, так как параметры, связанные с ИФБО, должны быть полностью специфицированы, оценщику следует быть в состоянии сделать заключение о том, все ли аспекты ФТБ реализованы на интерфейсном уровне.

10.4.3.4.2 Шаг оценивания ADV_FSP.3-11

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, что она является точным отображением ФТБ.

Для каждого функционального требования в ЗБ, которое оказывает видимый эффект на границах ФБО, информация в связанном с ним ИФБО специфицирует требуемые функции, описанные в требовании. Например, если в ЗБ содержится требование наличия списков контроля доступа и единственный ИФБО, прослеживаемый к этому требованию, специфицирует функции Unix-подобных разрядов защиты, тогда функциональная спецификация не является точной в отношении требований.

Оценщик должен осознавать, что для требований, которые незначительно проявляются или не проявляются вовсе на границах ФБО (например FDP_RIP), не ожидается, что эти требования будут прослежены к ИФБО. Анализ таких требований будет выполняться в процессе анализа проекта ОО (ADV_TDS), когда он включен в ЗБ.

10.4.4 Подвид деятельности по оценке (ADV_FSP.4)

10.4.4.1 Цели

Цель данного подвида деятельности — сделать заключение, предоставил ли разработчик описание ИФБО таким образом, чтобы оценщик имел возможность сделать вывод о том, полно ли и точно ли описаны ИФБО и реализуют ли они функциональные требования безопасности ЗБ.

10.4.4.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности, требуемыми шагами оценивания, являются:

a) ЗБ;

b) функциональная спецификация;

c) проект ОО.

Свидетельствами оценки для этого подвида деятельности, которые используются в случае их включения в ЗБ по ОО, являются:

a) описание архитектуры безопасности;

b) представление реализации;

c) описание внутреннего состава ФБО;

d) руководство пользователя по эксплуатации.

10.4.4.3 Замечания по применению

Функциональная спецификация описывает интерфейсы ФБО (ИФБО) структурированным образом. Из-за зависимости от Подвида деятельности по оценке (ADV_TDS.1) ожидается, что оценщик идентифицирует ФБО до начала работы по этому подвиду деятельности. Без точного знания того, что включают в себя ФБО, невозможно оценить полноту ИФБО.

При выполнении различных шагов оценивания, включенных в оценивание этого семейства, оценщика просят оценить точность и полноту нескольких факторов (описание самих ИФБО, а также их индивидуальных компонентов — параметров, действий, сообщений об ошибках и т. д.). Ожидается, что при выполнении этого анализа оценщик будет использовать документацию, предоставленную для оценки — т. е. ЗБ, проект ОО и некоторую другую документацию — руководство пользователя по эксплуатации, описание архитектуры безопасности и представление реализации. Документацию следует исследовать итеративным способом. Оценщик может прочитать, например в проекте ОО, каким образом реализована определенная функция, но не обнаружить там способа вызова этой функции через интерфейс. Это может заставить оценщика подвергнуть сомнению полноту конкретного описания ИФБО или сделать заключение о том, что данный интерфейс был упущен из виду при составлении функциональной спецификации. Описание подобных действий по оценке в ТОО является ключевым методом в представлении обоснования того, что шаги оценивания были выполнены верным образом.

Следует учесть, что есть функциональные требования, функциональные возможности которых проявляются (полностью или частично) архитектурно, а не через определенный механизм. Пример этого — внедрение механизмов, осуществляющих требования семейства «Защита остаточной информации» (FDP_RIP). Такие механизмы, как правило, реализуются для обеспечения отсутствия того или иного режима функционирования системы, а это трудно протестировать и поэтому верификация осуществляется путем анализа. В случаях, где такие функциональные требования включены в ЗБ, ожидается, что оценщик выявит наличие ФТБ, для которых нет интерфейсов, и что это не следует считать недостатком функциональной спецификации.

10.4.4.4 Действие ADV_FSP.4.1E

ИСО/МЭК 15408-3 ADV_FSP.4.1C: *В функциональной спецификации должны быть полностью представлены ФБО.*

10.4.4.4.1 Шаг оценивания ADV_FSP.4-1

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней полностью представлены ФБО.

Идентификация ИФБО — необходимая предпосылка для всех действий данного подвида деятельности. Для идентификации ИФБО должны быть идентифицированы ФБО (в рамках шагов оценивания семейства ADV_TDS «Проект ОО»). Эта деятельность может быть проведена на высоком уровне, чтобы удостовериться, что не упущены крупные группы интерфейсов (сетевых протоколов, аппаратных средств, файлов конфигурации), или на низком уровне как часть оценки функциональной спецификации.

При проведении данного шага оценивания оценщик делает заключение о том, что все части ФБО описаны в терминах интерфейсов, перечисленных в функциональной спецификации. Для всех частей ФБО следует иметь соответствующее описание интерфейсов или, при отсутствии соответствующих интерфейсов для части ФБО, оценщик делает заключение, что такое отсутствие допустимо и приемлемо.

ИСО/МЭК 15408-3 ADV_FSP.4.2C: *В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.*

10.4.4.4.2 Шаг оценивания ADV_FSP.4-2

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней указано назначение каждого ИФБО.

Назначение ИФБО — это общее утверждение, кратко описывающее функциональные возможности, обеспеченные интерфейсом. Не подразумевается, что оно должно быть полным изложением всех действий и результатов, относящихся к интерфейсу, а, скорее, оно должно помочь читателю составить общее представление о предполагаемом использовании данного интерфейса. Оценщику следует не только сделать заключение о том, что такое назначение существует, но и что оно точно отражает ИФБО, с учетом другой информации об интерфейсе, такой как описание действий и сообщений об ошибках.

10.4.4.4.3 Шаг оценивания ADV_FSP.4-3

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней содержится описание метода использования для каждого ИФБО.

Метод использования для ИФБО предоставляет краткую информацию по поводу того, каким образом в результате управления интерфейсом вызывают действия и получают результаты, связанные с ИФБО. Оценщику следует быть в состоянии посредством чтения материалов в функциональной спецификации вынести заключение о том, как использовать каждый интерфейс. Это не обязательно означает, что для каждого ИФБО нужен отдельный метод использования, поскольку можно, например описать в общем, как происходит системный вызов ядра, а затем идентифицировать каждый интерфейс, используя общий для всех интерфейсов стиль. Различные типы интерфейсов требуют различных спецификаций по методу их использования. У интерфейсов программирования приложений, сетевых протоколов, параметров системной конфигурации и шины аппаратных средств абсолютно разные методы использования, и это следует учитывать разработчику при разработке функциональной спецификации, так же, как и оценщику при проведении её оценки.

Для администрирующих интерфейсов, функции которых документированы как недоступные недоверенным пользователям, оценщик удостоверяется в том, что метод, благодаря которому данные функции являются недоступными таким пользователям, описан в функциональной спецификации. Следует отметить, что разработчику необходимо протестировать эту недоступность при проведении испытаний.

Оценщику следует не только сделать заключение о том, что имеется подмножество описаний методов использования, но и что эти описания точно охватывают каждый ИФБО.

10.4.4.4.4 Шаг оценивания ADV_FSP.4-4

Оценщик должен исследовать функциональную спецификацию, чтобы определить полноту ИФБО.

Оценщик должен использовать проектную документацию, чтобы идентифицировать возможные типы интерфейсов. Оценщик должен осуществить поиск проектной документации и руководств для потенциальных ИФБО, не описанных в документации, предоставленной разработчиком, таким образом указав на то, что набор ИФБО, определенный разработчиком, является неполным. Оценщик должен исследовать аргументы, представленные разработчиком для свидетельства полноты описания ИФБО, и проверить все уровни представления проектной документации вплоть до проекта самого низкого уровня и представления реализации на предмет того, что не существует никаких дополнительных ИФБО.

ИСО/МЭК 15408-3 ADV_FSP.4.3C: *В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.*

10.4.4.4.5 Шаг оценивания ADV_FSP.4-5

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение, полностью ли идентифицированы в нем все параметры, связанные с каждым ИФБО.

Оценщик исследует функциональную спецификацию, чтобы удостовериться, что в ней описаны все параметры для каждого ИФБО. Параметры — явные исходные данные или данные на выходе интерфейса, которые контролируют режим функционирования этого интерфейса. Например, параметрами являются: аргументы, поставляемые интерфейсу программирования приложений; различные поля в пакете для данного сетевого протокола; индивидуальные значения ключа в реестре Windows; сигналы, проходящие через контакты чипа и т. д.

Для вынесения заключения о том, что все данные параметры присутствуют в ИФБО, оценщику следует исследовать остальные описания интерфейса (действия, сообщения об ошибках и т. д.) и сделать заключение о том, что эффекты этих параметров перечислены в описании. Оценщику следует также проверить другие свидетельства, предоставленные для оценки (например проект ОО, описание архитектуры безопасности, руководство пользователя по эксплуатации, представление реализации) на предмет того, есть ли там описания режима функционирования интерфейса или дополнительных параметров, отсутствующие в функциональной спецификации.

10.4.4.4.6 Шаг оценивания ADV_FSP.4-6

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение, полно ли и точно ли описаны в нем все параметры, связанные с каждым ИФБО.

Как только все параметры идентифицированы, оценщику нужно удостовериться, что они описаны точно и что описание параметров проведено полно. Описание параметра некоторым значащим образом определяет, что представляет собой данный параметр. Например, интерфейс *foo (i)* может быть описан как имеющий «параметр *i*, который является целым числом»; но такое описание параметра неприемлемо. Более приемлемое описание — «параметр *i* — целое число, указывающее на число пользователей, которые в настоящий момент зарегистрированы в системе».

Для вынесения заключения о том, что описание параметра является полным, оценщику следует исследовать остальные описания интерфейса (назначение, метод использования, действия интерфейса, сообщения об ошибках и т. д.) и сделать вывод о том, что описания этих параметров перечислены в описании. Оценщику следует также проверить другие предоставленные свидетельства (например проект ОО, проект архитектуры, руководство пользователя по эксплуатации, представление реализации) на предмет того, есть ли там описания режима функционирования интерфейса или его дополнительных параметров, отсутствующие в функциональной спецификации.

ИСО/МЭК 15408-3 ADV_FSP.4.4C: *В функциональной спецификации должны быть описаны все действия, связанные с каждым ИФБО.*

10.4.4.4.7 Шаг оценивания ADV_FSP.4-7

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение о том, что в нем полно и точно описаны все действия, связанные с каждым ИФБО.

Оценщик осуществляет проверку для того, чтобы удостовериться, что все действия описаны. Действия, доступные через интерфейс, описывают, что именно делает данный интерфейс (в противоположность проекту ОО, где описывается, как действия предоставляются ФБО).

Действия интерфейса описывают функциональную возможность, которая может быть вызвана через интерфейс и может быть отнесена к стандартным действиям и относящимся к ФТБ действиям. Стандартные действия — описания того, что делает интерфейс. Количество информации, предоставляемой данным описанием, зависит от сложности интерфейса. Относящиеся к ФТБ действия — те, которые являются видимыми в любом внешнем интерфейсе (например следует предоставить описание деятельности по аудиту, которая требуется при вызове интерфейса (предполагаем, что требования аудита включены в ЗБ), даже если результат этого действия вообще не наблюдается через вызываемый интерфейс). В зависимости от параметров интерфейса может быть много различных действий, которые вызываются через интерфейс (например у интерфейса программирования приложений первый параметр может быть «подкомандой», а последующие параметры могут быть специфическими для этой подкоманды. Пример подобного интерфейса — интерфейс программирования приложений IOCTL в некоторых системах Unix).

Для вынесения заключения о том, что действия ИФБО описаны полностью, оценщику следует рассмотреть остальные части описания интерфейса (описания параметров, сообщений об ошибках и т. д.) и сделать заключение, перечислены ли в них описанные действия. Оценщику следует также проанализировать другие свидетельства, предоставленные для оценки (например проект ОО, описание архитектуры безопасности, руководство пользователя по эксплуатации, представление реализации), чтобы определить, есть ли там свидетельства действий интерфейса, отсутствующие в функциональной спецификации.

ИСО/МЭК 15408-3 ADV_FSP.4.5C: *Функциональная спецификация должна содержать описание сообщений обо всех непосредственных ошибках, которые могут возникнуть при вызове каждого ИФБО.*

10.4.4.4.8 Шаг оценивания ADV_FSP.4-8

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение о том, что в нем полно и точно описаны все сообщения об ошибках, возникающих при вызове ИФБО.

Ошибки могут принимать различные формы в зависимости от описываемого интерфейса. В случае интерфейса программирования приложений интерфейс сам может вернуть код ошибки, установить

состояние глобальной ошибки или определенный параметр с кодом ошибки. В случае файла конфигурации неправильно настроенный параметр может привести к появлению в системном журнале сообщения об ошибке. В случае аппаратных средств, например шины ввода/вывода, возникновение ошибки может подать на шину сигнал или вызвать особое состояние центрального процессора.

Ошибки (и связанные с ними сообщения об ошибках) появляются через запрос интерфейса. Обработка, которая происходит в ответ на запрос интерфейса, может столкнуться с некоторыми условиями, вызывающими ошибку и сообщение об этой ошибке (путем определенного механизма, специфического для данной реализации). В некоторых случаях это может быть возвращаемое самим интерфейсом значение; в других случаях глобальное значение может быть назначено и проверено после запроса интерфейса. Скорее всего, у ОО будет много сообщений об ошибках низкого уровня, которые являются результатом фундаментальных условий для ресурсов, например «недостаточно места на диске» или «ресурс заблокирован». Несмотря на то, что эти сообщения об ошибках могут быть прослежены к большому количеству ИФБО, их можно использовать для выявления тех случаев, когда часть описания интерфейса была опущена. Например, если есть ИФБО, который выдает сообщение «недостаточно места на диске», но для которого не представлено ясное описание того, почему этому ИФБО следует позволять получение доступа к диску, оценщику может потребоваться исследовать другие свидетельства (семейств ADV_ARC «Архитектура безопасности», ADV_TDS «Проект ОО»), связанные с этим ИФБО, чтобы сделать заключение о том, является ли его описание полным и точным.

Оценщик делает заключение о том, что для каждого ИФБО определен точный набор сообщений об ошибках, которые выдаются при вызове этого интерфейса. Оценщик рассматривает свидетельства, представленные по интерфейсу, чтобы сделать заключение о том, кажется ли приведенный набор ошибок полным. Он сверяет эту информацию с другими предоставленными для оценки свидетельствами (например проект ОО, описание архитектуры безопасности, руководство пользователя по эксплуатации, представление реализации), чтобы удостовериться, что нет ошибок, возникающих при обработке вызовов упомянутых интерфейсов, описание которых отсутствует в функциональной спецификации.

10.4.4.4.9 Шаг оценивания ADV_FSP.4-9

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение о том, что в нем полно и точно описаны значения всех ошибок, связанных с вызовами каждого ИФБО.

Для определения степени точности описания оценщик должен быть в состоянии понять значение ошибки. Например, если интерфейс возвращает числовое значение 0, 1 или 2, оценщик не в состоянии понять ошибку, если в функциональной спецификации описано только следующее: «возможные ошибки, возникающие при вызове интерфейса *foo ()* — 0, 1 или 2». Вместо этого оценщик выполняет проверку, чтобы удостовериться, что ошибки описаны иначе например: «возможные ошибки, возникающие при вызове интерфейса *foo ()* — 0 (обработка успешно выполнена), 1 (файл не найден) или 2 (неверная спецификация имени файла)».

Для вынесения заключения о том, что ошибки, возникающие в результате вызовов ИФБО, описаны полностью, оценщик исследует остальную часть описания интерфейса (описания параметров, действий и т. д.) и делает заключение, перечислены ли в ней возможные условия возникновения ошибок, которые могут возникнуть вследствие использования данного интерфейса. Оценщик также проверяет другие свидетельства, предоставленные для оценки (например проект ОО, описание архитектуры безопасности, руководство пользователя по эксплуатации, представление реализации), чтобы определить, что нет ошибок, возникающих при обработке вызовов упомянутых интерфейсов, описание которых отсутствует в функциональной спецификации.

ИСО/МЭК 15408-3 ADV_FSP.4.6C: *В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.*

10.4.4.4.10 Шаг оценивания ADV_FSP.4-10

Оценщик должен проверить, что прослеживание соотносит ФТБ с соответствующими ИФБО.

Прослеживание предоставляется разработчиком в качестве руководства для определения того, каким образом ФТБ связаны с ИФБО. Это прослеживание может быть представлено в простом виде, например в виде таблицы; оно используется в качестве исходных данных для оценщика при использовании в последующих шагах оценивания, в которых оценщик верифицирует полноту и точность этого прослеживания.

10.4.4.5 Действие ADV_FSP.4.2E

10.4.4.5.1 Шаг оценивания ADV_FSP.4-11

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она полным отображением ФТБ.

Чтобы удостовериться, что все функциональные ФТБ охвачены функциональной спецификацией, а также анализом покрытия тестами, оценщик может основываться на прослеживании, предоставленном разработчиком (см. ADV_FSP.4-10 для прослеживания между ФТБ для ОО и ИФБО). Следует учесть, что такое прослеживание иногда необходимо представлять на уровне детализации ниже, чем уровень детализации компонента или даже элемента требований из-за операций (назначения, уточнения, выбора), выполняемых над функциональным требованием автором ЗБ.

Например, компонент FDP_ACC.1 содержит элемент с операциями назначения. Если бы в ЗБ содержалось, например десять правил в отношении назначения для данного компонента FDP_ACC.1, и эти правила были бы охвачены тремя различными ИФБО, то для оценщика некорректно было бы проследить FDP_ACC.1 к ИФБО A, B и C и утверждать о завершении шага оценивания. Вместо этого оценщик должен был бы проследить FDP_ACC.1 (правило 1) к ИФБО A; FDP_ACC.1 (правило 2) к ИФБО B и т.д. Может иметь место и случай, когда интерфейс является интерфейсом адаптера (например IOCTL), и тогда прослеживание должно быть определенным к набору параметров для данного интерфейса.

Оценщик должен осознавать, что для требований, которые незначительно проявляются или не проявляются вовсе на границах ФБО (например FDP_RIP), не ожидается, что эти требования будут прослежены к ИФБО. Анализ таких требований будет выполняться в процессе анализа проекта ОО (ADV_TDS), когда он включен в ЗБ. Важно отметить, что так как параметры, связанные с ИФБО, должны быть полностью специфицированы, оценщику следует быть в состоянии сделать заключение о том, все ли аспекты ФТБ реализованы на интерфейсном уровне.

10.4.4.5.2 Шаг оценивания ADV_FSP.4-12

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, что она является точным отображением ФТБ.

Для каждого функционального требования в ЗБ, которое оказывает видимый эффект на границах ФБО, информация в связанном с ним ИФБО специфицирует требуемые функции описанные в требовании. Например, если в ЗБ содержится требование наличия списков контроля доступа и единственный ИФБО, прослеживаемый к этому требованию, специфицирует функции Unix-подобных разрядов защиты, тогда функциональная спецификация не является точной в отношении требований.

Оценщик должен осознавать, что для требований, которые незначительно проявляются или не проявляются вовсе на границах ФБО (например FDP_RIP), не ожидается, что эти требования будут прослежены к ИФБО. Анализ таких требований будет выполняться в процессе анализа проекта ОО (ADV_TDS), когда он включен в ЗБ.

10.4.5 Подвид деятельности по оценке (ADV_FSP.5)

10.4.5.1 Цели

Цель данного подвида деятельности — сделать заключение, предоставил ли разработчик описание ИФБО таким образом, чтобы оценщик имел возможность сделать вывод о том, полно ли и точно ли описаны ИФБО и реализуют ли они функциональные требования безопасности ЗБ. Полнота описания интерфейсов оценивается на основании представления реализации.

10.4.5.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности, требуемыми шагами оценивания, являются:

a) ЗБ;

b) функциональная спецификация;

c) проект ОО;

d) представление реализации.

Свидетельствами оценки для этого подвида деятельности, которые используются в случае их включения в ЗБ по ОО, являются:

a) описание архитектуры безопасности;

b) описание внутреннего состава ФБО;

c) модель формальной политики безопасности;

d) руководство пользователя по эксплуатации.

10.4.5.3 Действие ADV_FSP.5.1E

ИСО/МЭК 15408-3 ADV_FSP.5.1C: *В функциональной спецификации должны быть полностью представлены ФБО.*

10.4.5.3.1 Шаг оценивания ADV_FSP.5-1

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней полностью представлены ФБО.

Идентификация ИФБО — необходимая предпосылка для всех действий данного подвида деятельности. Для идентификации же ИФБО должны быть идентифицированы ФБО (в рамках шагов оценивания семейства ADV_TDS «Проект ОО»). Эта деятельность может быть проведена на высоком уровне, чтобы удостовериться, что не упущены крупные группы интерфейсов (сетевых протоколов, аппаратных средств, файлов конфигурации), или на низком уровне — как часть оценки функциональной спецификации.

При проведении данного шага оценивания оценщик делает заключение о том, что все части ФБО описаны в терминах интерфейсов, перечисленных в функциональной спецификации. Для всех частей ФБО следует иметь соответствующее описание интерфейсов или, при отсутствии соответствующих интерфейсов для части ФБО, оценщик делает заключение, что такое отсутствие допустимо и приемлемо.

ИСО/МЭК 15408-3 ADV_FSP.5.2C: *Функциональная спецификация должна содержать полуформальное описание ИФБО.*

10.4.5.3.2 Шаг оценивания ADV_FSP.5-2

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что она представлена в полуформальном стиле описания.

Полуформальное описание характеризуется стандартизированным форматом с четким синтаксисом, уменьшающим двусмысленность, которая может возникнуть в неформальных описаниях. Так как цель полуформального описания состоит в том, чтобы повысить способность читателя понять данное описание, целесообразно, хотя и не обязательно, использовать определенные структурированные методы представления (псевдокод, блок-схемы, графики).

В целях этой деятельности оценщику следует удостовериться, что описания интерфейсов отформатированы в структурированной, последовательной манере и используют общую терминологию. Полуформальное описание интерфейсов также подразумевает, что уровень детализации представления для интерфейсов в основном согласован для всех ИФБО. Для функциональной спецификации приемлемо ссылаться на внешние спецификации для некоторых частей интерфейса, если эти внешние спецификации также представлены в полуформальном стиле описания.

ИСО/МЭК 15408-3 ADV_FSP.5.3C: *В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.*

10.4.5.3.3 Шаг оценивания ADV_FSP.5-3

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней указано назначение каждого ИФБО.

Назначение ИФБО — это общее утверждение, кратко описывающее функциональные возможности, обеспеченные интерфейсом. Не подразумевается, что оно не должно быть полным изложением всех действий и результатов, относящихся к интерфейсу, а, скорее, оно должно помочь читателю составить общее представление о предполагаемом использовании данного интерфейса. Оценщику следует не только сделать заключение о том, что такое назначение существует, но и что оно точно отражает ИФБО, с учетом другой информации об интерфейсе, такой как описание действий и сообщений об ошибках.

10.4.5.3.4 Шаг оценивания ADV_FSP.5-4

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней содержится описание метода использования для каждого ИФБО.

Метод использования для ИФБО предоставляет краткую информацию по поводу того, каким образом в результате управления интерфейсом вызывают действия и получают результаты, связанные с ИФБО. Оценщику следует посредством чтения материалов в функциональной спецификации вынести заключение о том, как использовать каждый интерфейс. Это не обязательно означает, что для каждого ИФБО нужен отдельный метод использования, поскольку можно описать в общем, как происходит системный вызов ядра, а затем идентифицировать каждый интерфейс, используя общий для всех интерфейсов стиль. Различные типы интерфейсов требуют различных спецификаций по методу использования. У интерфейсов программирования приложений, сетевых протоколов, параметров системной конфигурации и шины аппаратных средств абсолютно разные методы использования, и это следует учитывать разработчику при разработке функциональной спецификации, так же, как и оценщику при проведении её оценки.

Для администрирующих интерфейсов, функции которых документированы как недоступные недоверенным пользователям, оценщик удостоверяется в том, что метод, благодаря которому данные функции являются недоступными таким пользователям, описан в функциональной спецификации. Следует отметить, что разработчику необходимо протестировать эту недоступность при проведении испытаний.

Оценщику следует не только сделать заключение о том, что имеется подмножество описаний методов использования, но и что эти описания точно охватывают каждый ИФБО.

10.4.5.3.5 Шаг оценивания ADV_FSP.5-5

Оценщик должен исследовать функциональную спецификацию, чтобы определить полноту ИФБО.

Оценщик должен использовать проектную документацию, чтобы идентифицировать возможные типы интерфейсов. Оценщик должен осуществить поиск проектной документации и руководств для потенциальных ИФБО, не описанных в документации, предоставленной разработчиком, таким образом указав на то, что набор ИФБО, определенный разработчиком, является неполным. Оценщик должен исследовать аргументы, представленные разработчиком для доказательства полноты описания ИФБО, и проверить все уровни представления проектной документации вплоть до проекта самого низкого уровня и представления реализации на предмет того, что не существует никаких расширенных ИФБО.

ИСО/МЭК 15408-3 ADV_FSP.5.4C: *В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.*

10.4.5.3.6 Шаг оценивания ADV_FSP.5-6

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение, полностью ли идентифицированы в нем все параметры, связанные с каждым ИФБО.

Оценщик исследует функциональную спецификацию, чтобы удостовериться, что в ней описаны все параметры для каждого ИФБО. Параметры — явные исходные данные или данные на выходе интерфейса, которые контролируют режим функционирования этого интерфейса. Например, параметрами являются: аргументы, поставляемые интерфейсу программирования приложений; различные поля в пакете для данного сетевого протокола; индивидуальные значения ключа в Реестре Windows; сигналы, проходящие через контакты чипа и т.д.

Для вынесения заключения о том, что все данные параметры присутствуют в ИФБО, оценщику следует исследовать остальные описания интерфейса (действия, сообщения об ошибках и т.д.) и сделать заключение о том, что эффекты этих параметров перечислены в описании. Оценщику следует также проверить другие свидетельства, предоставленные для оценки (например проект ОО, описание архитектуры безопасности, руководство пользователя по эксплуатации, представление реализации) на предмет того, есть ли там описания режима функционирования интерфейса или дополнительных параметров, отсутствующие в функциональной спецификации.

10.4.5.3.7 Шаг оценивания ADV_FSP.5-7

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение, полно ли и точно ли описаны в нем все параметры, связанные с каждым ИФБО.

Как только все параметры были идентифицированы, оценщику нужно удостовериться, что они описаны точно и описание параметров проведено полно. Описание параметра некоторым значащим образом определяет, что представляет собой данный параметр. Например, интерфейс *foo (i)* может быть описан как имеющий «параметр *i*, который является целым числом»; но такое описание параметра не приемлемо. Более приемлемое описание — «параметр *i* — целое число, указывающее на число пользователей, которые в настоящий момент зарегистрированы в системе».

Для вынесения заключения о том, что описание параметра является полным, оценщику следует исследовать остальные описания интерфейса (назначение, метод использования, действия интерфейса, сообщения об ошибках и т.д.) и сделать вывод о том, что описания этих параметров перечислены в описании. Оценщику следует также проверить другие предоставленные свидетельства (например проект ОО, проект архитектуры, руководство пользователя по эксплуатации, представление реализации) на предмет того, есть ли там описания режима функционирования интерфейса или его дополнительных параметров, отсутствующие в функциональной спецификации.

ИСО/МЭК 15408-3 ADV_FSP.5.5C: *В функциональной спецификации должны быть описаны все действия, связанные с каждым ИФБО.*

10.4.5.3.8 Шаг оценивания ADV_FSP.5-8

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение о том, что в нем полно и точно описаны все действия, связанные с каждым ИФБО.

Оценщик осуществляет проверку для того, чтобы удостовериться, что все действия описаны. Действия, доступные через интерфейс, описывают, что именно делает данный интерфейс (в противоположность проекту ОО, где описывается, как действия предоставляются ФБО).

Действия интерфейса описывают функциональную возможность, которая может быть вызвана через интерфейс и может быть отнесена к стандартным действиям и относящимся к ФТБ действиям. Стандартные действия — описания того, что делает интерфейс. Количество информации, предостав-

ляемой данным описанием, зависит от сложности интерфейса. Относящиеся к ФТБ действия — те, которые являются видимыми в любом внешнем интерфейсе (например следует предоставить описание деятельности по аудиту, которая требуется при вызове интерфейса (предполагаем, что требования аудита включены в ЗБ), даже если результат этого действия вообще не наблюдается через вызываемый интерфейс). В зависимости от параметров интерфейса может быть много различных действий, которые вызываются через интерфейс (например у интерфейса программирования приложений первый параметр может быть «подкомандой», а последующие параметры могут быть специфическими для этой подкоманды. Пример подобного интерфейса — интерфейс программирования приложений IOCTL в некоторых системах Unix).

Для вынесения заключения о том, что действия ИФБО описаны полностью, оценщику следует рассмотреть остальные части описания интерфейса (описания параметров, сообщений об ошибках и т. д.) и сделать заключение, перечислены ли в них описанные действия. Оценщику следует также проанализировать другие свидетельства, предоставленные для оценки (например проект ОО, описание архитектуры безопасности, руководство пользователя по эксплуатации, представление реализации), чтобы определить, есть ли там свидетельства действий интерфейса, отсутствующие в функциональной спецификации.

ИСО/МЭК 15408-3 ADV_FSP.5.6C: *Функциональная спецификация должна содержать описание сообщений обо всех непосредственных ошибках, которые могут возникнуть при вызове каждого ИФБО.*

10.4.5.3.9 Шаг оценивания ADV_FSP.5-9

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение о том, что в нем полно и точно описаны все сообщения об ошибках, возникающих при вызове ИФБО.

Ошибки могут принимать различные формы в зависимости от описываемого интерфейса. В случае интерфейса программирования приложений интерфейс сам может вернуть код ошибки, установить состояние глобальной ошибки или определенный параметр с кодом ошибки. В случае файла конфигурации неправильно настроенный параметр может привести к появлению в системном журнале сообщения об ошибке. В случае аппаратных средств, например шины ввода/вывода, возникновение ошибки может подать на шину сигнал или вызвать особое состояние центрального процессора.

Ошибки (и связанные с ними сообщения об ошибках) появляются через запрос интерфейса. Обработка, которая происходит в ответ на запрос интерфейса, может столкнуться с некоторыми условиями, вызывающими ошибку и сообщение об этой ошибке (путем определенного механизма, специфического для данной реализации). В некоторых случаях это может быть возвращаемое самим интерфейсом значение; в других случаях глобальное значение может быть назначено и проверено после запроса интерфейса. Скорее всего, у ОО будет много сообщений об ошибках низкого уровня, которые являются результатом фундаментальных условий для ресурсов, например «недостаточно места на диске» или «ресурс заблокирован». Несмотря на то, что эти сообщения об ошибках могут быть прослежены к большому количеству ИФБО, их можно использовать для выявления тех случаев, когда часть описания интерфейса была опущена. Например, если есть ИФБО, который выдает сообщение «недостаточно места на диске», но для которого не представлено ясное описание того, почему этому ИФБО следует позволять получение доступа к диску, оценщику может потребоваться исследовать другие свидетельства (семейств ADV_ARC «Архитектура безопасности», ADV_TDS «Проект ОО»), связанные с этим ИФБО, чтобы сделать заключение о том, является ли его описание полным и точным.

Оценщик делает заключение о том, что для каждого ИФБО определен точный набор сообщений об ошибках, которые выдаются при вызове этого интерфейса. Оценщик рассматривает свидетельства, представленные по интерфейсу, чтобы сделать заключение о том, кажется ли приведенный набор ошибок полным. Он сверяет эту информацию с другими предоставленными для оценки свидетельствами (например проект ОО, описание архитектуры безопасности, руководство пользователя по эксплуатации, представление реализации), чтобы удостовериться, что нет ошибок, возникающих при обработке вызовов упомянутых интерфейсов, описание которых отсутствует в функциональной спецификации.

10.4.5.3.10 Шаг оценивания ADV_FSP.5-10

Оценщик должен исследовать представление ИФБО, чтобы сделать заключение о том, что в нем полно и точно описаны значения всех ошибок, связанных с вызовами каждого ИФБО.

Для определения степени точности описания оценщик должен быть в состоянии понять значение ошибки. Например, если интерфейс возвращает числовое значение 0, 1 или 2, оценщик не в состоянии понять ошибку, если в функциональной спецификации описано только следующее: «возможные ошибки, возникающие при вызове интерфейса *foo ()* — 0, 1 или 2». Вместо этого оценщик выполняет проверку, чтобы удостовериться, что ошибки описаны иначе, например: «возможные ошибки, возникающие

при вызове интерфейса *foo ()* — 0 (обработка успешно выполнена), 1 (файл не найден) или 2 (неверная спецификация имени файла)».

Для вынесения заключения о том, что ошибки, возникающие в результате вызовов ИФБО, описаны полностью, оценщик исследует остальную часть описания интерфейса (описания параметров, действий и т.д.) и делает заключение, перечислены ли в ней возможные условия возникновения ошибок, которые могут возникнуть вследствие использования данного интерфейса. Оценщик также проверяет другие свидетельства, предоставленные для оценки (например проект ОО, описание архитектуры безопасности, руководство пользователя по эксплуатации, представление реализации), чтобы определить, что нет ошибок, возникающих при обработке вызовов упомянутых интерфейсов, описание которых отсутствует в функциональной спецификации.

ИСО/МЭК 15408-3 ADV_FSP.5.7C: *Функциональная спецификация должна содержать описание всех сообщений об ошибках, возникающих не в результате вызова ИФБО.*

10.4.5.3.11 Шаг оценивания ADV_FSP.5-11

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что она полностью и точно описывает все сообщения об ошибках, возникающих не в результате вызова ИФБО.

Этот шаг оценивания дополняет шаг оценивания ADV_FSP.5-9, в котором описываются те сообщения об ошибках, которые возникают в результате вызова ИФБО. Вместе эти шаги оценивания охватывают все сообщения об ошибках, которые могли быть вызваны ФБО.

Оценщик оценивает полноту и точность функциональной спецификации, сравнивая ее содержание с примерами создания сообщений об ошибке в представлении реализации. Большинство этих сообщений об ошибках будет уже охвачено в шаге оценивания ADV_FSP.5-9.

Сообщения об ошибках, связанные с этим шагом оценивания, как правило, являются такими, которые будут выданы с малой степенью вероятности, но всё же запрограммированы в целях соблюдения лучших практик. Например, оператор выбора, определяющий действия, происходящие в случае выбора конкретного пункта, может заканчиваться условным оператором *else* для возможности применения в ситуациях, которые не ожидаются; эта практика обеспечивает невозможность перехода ФБО в неопределенное состояние. Однако не ожидается, что при исполнении программы когда-нибудь дойдет до этого условного оператора; таким образом, никогда не будет создано сообщение об ошибке, связанной с выполнением этого оператора. Но даже если эта ошибка не возникает, она должна быть включена в функциональную спецификацию.

ИСО/МЭК 15408-3 ADV_FSP.5.8C: *Функциональная спецификация должна содержать обоснование каждого сообщения об ошибке, содержащегося в реализации ФБО, но не являющегося результатом вызова ИФБО.*

10.4.5.3.12 Шаг оценивания ADV_FSP.5-12

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о том, что в ней представлено обоснование для каждого сообщения об ошибке, содержащегося в реализации ФБО, но не являющегося результатом вызова ИФБО.

Оценщик удостоверяется, что каждое сообщение об ошибке, обнаруженное в процессе выполнения шага оценки ADV_FSP.5-11, содержит обоснование, описывающее, почему это сообщение об ошибке не является результатом вызова ИФБО.

Как описано в предыдущем шаге оценивания, это обоснование может быть настолько же целенаправленным, как и факт, что рассматриваемое сообщение об ошибке предоставлено для полноты логики выполнения программы и что оно, как ожидается, никогда не будет выдано. Оценщик убеждается, что обоснование каждого такого сообщения об ошибке является логичным.

ИСО/МЭК 15408-3 ADV_FSP.5.9C: *В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.*

10.4.5.3.13 Шаг оценивания ADV_FSP.5-13

Оценщик должен проверить, что прослеживание соотносит ФТБ с соответствующими ИФБО.

Прослеживание предоставляется разработчиком в качестве руководства для определения того, каким образом ФТБ связаны с ИФБО. Это прослеживание может быть представлено в простом виде, например в виде таблицы; оно используется в качестве исходных данных для оценщика для использования в последующих шагах оценивания, в которых оценщик верифицирует полноту и точность этого прослеживания.

10.4.5.4 Действие ADV_FSP.5.2E

10.4.5.4.1 Шаг оценивания ADV_FSP.5-14

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она полным отображением ФТБ.

Чтобы удостовериться, что все ФТБ охвачены функциональной спецификацией, а также анализом покрытия тестами, оценщик может основываться на прослеживании, предоставленном разработчиком (см. ADV_FSP.5-13 для прослеживания между ФТБ и ИФБО). Следует учесть, что такое прослеживание иногда необходимо представлять на уровне детализации ниже, чем уровень детализации компонента или даже элемента требований из-за операций (назначения, уточнения, выбора), выполняемых над функциональным требованием автором ЗБ.

Например, компонент FDP_ACC.1 содержит элемент с операциями назначения. Если бы в ЗБ содержалось, например десять правил в отношении назначения для данного компонента FDP_ACC.1, и эти правила были бы охвачены тремя различными ИФБО, то для оценщика некорректно было бы проследить FDP_ACC.1 к ИФБО A, B и C и утверждать о завершении шага оценивания. Вместо этого оценщик должен был бы проследить FDP_ACC.1 (правило 1) к ИФБО A; FDP_ACC.1 (правило 2) к ИФБО B и т.д. Может иметь место и случай, когда интерфейс является интерфейсом адаптера (например IOCTL), и тогда прослеживание должно быть определенным к набору параметров для данного интерфейса.

Оценщик должен осознавать, что для требований, которые незначительно проявляются или не проявляются вовсе на границах ФБО (например FDP_RIP), не ожидается, что эти требования будут прослежены к ИФБО. Анализ таких требований будет выполняться в процессе анализа проекта ОО (ADV_TDS), когда он включен в ЗБ. Важно отметить, что так как параметры, связанные с ИФБО, должны быть полностью специфицированы, оценщику следует быть в состоянии сделать заключение о том, все ли аспекты ФТБ реализованы на уровне интерфейсов.

10.4.5.4.2 Шаг оценивания ADV_FSP.5-15

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, что она является точным отображением ФТБ.

Для каждого функционального требования в ЗБ, которое оказывает видимый эффект на границах ФБО, информация в связанном с ним ИФБО специфицирует требуемые функции в требовании. Например, если в ЗБ содержится требование наличия списков контроля доступа и единственный ИФБО, прослеживаемый к этому требованию, специфицирует функции Unix-подобных разрядов защиты, тогда функциональная спецификация не является точной в отношении требований.

Оценщик должен осознавать, что для требований, которые незначительно проявляются или не проявляются вовсе на границах ФБО (например FDP_RIP), не ожидается, что эти требования будут прослежены к ИФБО. Анализ таких требований будет выполняться в процессе анализа проекта ОО (ADV_TDS), когда он включен в ЗБ.

10.4.6 Подвид деятельности по оценке (ADV_FSP.6)

Общее руководство отсутствует; за консультациями по выполнению данного подвида деятельности следует обращаться в конкретную систему оценки.

10.5 Представление реализации (ADV_IMP)

10.5.1 Подвид деятельности по оценке (ADV_IMP.1)

10.5.1.1 Цели

Цель данного подвида деятельности — сделать заключение, является ли полученное от разработчика представление реализации пригодным для использования в других видах деятельности по оценке; эта пригодность оценивается по степени соответствия требованиям данного компонента.

10.5.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) представление реализации;

b) документация по инструментам разработки, как следует из ALC_TAT;

c) описание проекта ОО.

10.5.1.3 Замечания по применению

Представление реализации предоставляется для того, чтобы удостовериться, что действия по анализу не были сокращены из-за нехватки информации. Это, однако, не подразумевает, что при выполнении действий оценщика исследуется все представление. Практически всегда это представляется непрактичным, особенно с учетом того факта, что, скорее всего, исследование представления целиком не будет приводить к более высокому уровню доверия ОО по сравнению с предполагаемым по представлению реализации. Для данного подвида деятельности это еще более справедливо. Для оценщика не представляется целесообразным проводить большое количество времени, проверяя требования для одной части представления реализации, а затем использовать различные части представления

реализации при выполнении анализа в других шагах оценивания. Поэтому поощряется выполнение выборки представления реализации ОО из областей ОО, которые будут представлять наибольший интерес во время проведения анализа, выполняемого в рамках шагов оценивания других семейств (например ATE_IND, AVA_VAN и ADV_INT).

10.5.1.4 Действие ADV_IMP.1.1E

ИСО/МЭК 15408-3 ADV_IMP.1.1C: *Представление реализации должно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дополнительных проектных решений.*

10.5.1.4.1 Шаг оценивания ADV_IMP.1-1

Оценщик должен проверить представление реализации, чтобы сделать заключение, определены ли однозначно в нем ФБО на таком уровне детализации, что ФБО могут быть сгенерированы без каких бы то ни было дальнейших проектных решений.

Исходный код или диаграммы аппаратных средств и/или программный код модели интегральных схем или размещения данных, которые используются для построения фактических аппаратных средств, являются примерами частей представления реализации. Оценщик оценивает выборку представления реализации, чтобы приобрести уверенность в том, что этот уровень является приемлемым, а не, например псевдокодовым представлением, которое требует дополнительных проектных решений. Поощряется выполнение быстрой проверки, сначала проанализировав представление реализации, чтобы удостовериться, что разработчик находится на верном пути. Однако поощряется также выполнение большей части этой проверки при работе на других шагах оценивания, на которых необходимо исследовать представление реализации; это поможет удостовериться в том, что выборка, исследованная во время этого шага оценивания, является релевантной.

ИСО/МЭК 15408-3 ADV_IMP.1.2C: *Представление реализации должно быть изложено в том виде, какой используется персоналом, занимающимся разработкой.*

10.5.1.4.2 Шаг оценивания ADV_IMP.1-2

Оценщик должен проверить, что представление реализации изложено в виде, используемом персоналом разработки.

Представление реализации выполняется разработчиком таким образом, чтобы потом была возможность превращения этого представления в фактическую реализацию. Например, разработчик может работать с файлами, содержащими исходный текст программ, который потом будет скомпилирован и станет частью ФБО. Разработчик делает доступным представление реализации в той форме, в какой он его использует, благодаря чему оценщик может применять методы автоматизированного анализа. Это также увеличивает уверенность в том, что оцениваемое представление реализации является именно тем, которое используется при производстве ФБО (в отличие от того случая, когда оно сопровождается альтернативным форматом представления, например документом текстового процессора). Следует отметить, что разработчик может использовать различные формы представления реализации; они также должны прилагаться. Основная цель — снабдить оценщика такой информацией, которая позволила бы максимизировать эффективность его усилий по анализу.

Оценщик исследует выборку представления реализации, чтобы приобрести уверенность в том, что оцениваемая версия является приемлемой для использования разработчиком. Выборка должна быть такой, чтобы у оценщика имелось доверие к тому, что все области представления реализации удовлетворяют требованию; однако не требуется проводить полное исследование всего представления реализации.

Соглашения в некоторых формах представления реализации могут затруднить или сделать невозможным только по представлению реализации сделать заключение о том, каким будет фактический результат компиляции или интерпретации при запуске. Например, директивы компилятора на языке Си приведут к тому, что компилятор исключит или включит целые части программного кода.

Для некоторых форм представления реализации требуется дополнительная информация, поскольку их довольно сложно понять и проанализировать. В качестве примера можно привести «скрытый» или каким-либо образом запутанный фрагмент исходного текста программы, который сложно понять и/или проанализировать. Подобные формы представления реализации чаще всего возникают, когда разработчик ОО применяет к некоторой версии представления реализации некие программы по сокрытию или запутыванию кода. Хотя представление со скрытыми участками кода является именно тем, что будет в дальнейшем подвергнуто компиляции, а потому может быть даже ближе к реализации (по структуре), чем оригинальная версия, но предоставление оценщику запутанного программного кода может привести к тому, что анализ рисков, связанных с данным представлением реализации, потребует значительно больше времени. При создании подобных форм представления в компонентах данного

семейства должны быть детализированы примененные средства/алгоритмы сокрытия, что позволит снабдить оценщика представлением до применения сокрытия участков кода, а дополнительная информация может быть использована для приобретения уверенности в том, что процесс сокрытия участков кода не нарушил выполнение каких-либо функций безопасности.

Оценщик рассматривает выборку представления реализации для того, чтобы была получена вся информация, которая необходима для интерпретации представления реализации. Следует отметить, что на инструментальные средства этого ссылаются компоненты семейства «Инструментальные средства и методы» (ALC_TAT). Поощряется выполнение быстрой проверки, сначала проанализировав представление реализации, чтобы удостовериться, что разработчик находится на верном пути. Однако также поощряется выполнить большую часть этой проверки при работе на других шагах оценивания, на которых необходимо исследовать представление реализации; это поможет удостовериться в том, что выборка, исследованная во время этого шага оценивания, является релевантной.

ИСО/МЭК 15408-3 ADV_IMP.1.3C: *В прослеживании между выборкой представления реализации и описанием проекта ОО должно быть продемонстрировано их соответствие.*

10.5.1.4.3 Шаг оценивания ADV_IMP.1-3

Оценщик должен исследовать прослеживание между описанием проекта ОО и образцом представления реализации, чтобы сделать заключение о том, что оно является точным.

Оценщик усиливает заключение о существовании (описанное в шаге оценивания ADV_IMP.1-1), проверяя точность части представления реализации и описания проекта ОО. Для тех частей ОО, которые представляют особый интерес, оценщик проверяет, что представление реализации точно отражает описание, представленное в проекте ОО.

Например, в описании проекта ОО может быть идентифицирован модуль логина, который используется для идентификации и подтверждения подлинности пользователей. Если аутентификация пользователя достаточно значима, оценщик верифицирует, что соответствующий код фактически осуществляет тот сервис, который описан в описании проекта ОО. Возможно, необходимо также верифицировать, что код принимает те параметры, которые описаны в функциональной спецификации.

Стоит указать, что разработчик должен выбрать, выполнить ли прослеживание для всего представления реализации, таким образом обеспечивая охват выборки прослеживанием, или перед выполнением прослеживания подождать выборки. В первом случае возможен больший объем работы, но она может быть закончена еще до начала самой оценки. Во втором случае объем работы меньше, но на время производства необходимых свидетельств придется приостановить деятельность по оценке.

10.5.2 Подвид деятельности по оценке (ADV_IMP.2)

Общее руководство отсутствует; за консультациями по выполнению данного подвида деятельности следует обращаться в конкретную систему оценки.

10.6 Внутренняя структура ФБО (ADV_INT)

10.6.1 Подвид деятельности по оценке (ADV_INT.1)

10.6.1.1 Цели

Цель данного подвида деятельности — сделать заключение, является ли определенное подмножество ФБО спроектированным и структурированным таким образом, что снижается вероятность уязвимостей и что обслуживание ФБО может быть выполнено без введения уязвимостей.

10.6.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) описание проекта ОО;

c) представление реализации (если ADV_IMP является частью требуемого доверия);

d) описание архитектуры безопасности;

e) документация по стандартам кодирования, как следует из ALC_TAT.

10.6.1.3 Замечания по применению

Роль описания внутренней структуры ФБО заключается в том, чтобы представить свидетельства структуры проекта и реализации ФБО.

У структуры проекта есть два аспекта: составные части ФБО и процедуры, использованные при проектировании ФБО. В случае, если ФБО разработаны в манере, совместимой с проектом, представленном в проекте ОО (см. ADV_TDS), оценка проекта ФБО проводится очевидным образом. В случае выполнения процедур проектирования (см. ALC_TAT) оценка методики проектирования ФБО также очевидна.

В случае, когда ФБО реализуются, используя основанное на выполнении процедур программное обеспечение, структура оценивается на основе ее модульности; модули, идентифицированные в описании внутренней структуры, совпадают с теми модулями, которые идентифицированы в проекте ОО (семейство ADV_TDS «Проект ОО»). Модуль состоит из одного или более файлов исходного кода, которые являются наименьшими структурными единицами.

Использование операции назначения в этом компоненте налагает более строгие ограничения на подмножество ФБО, явно идентифицированное в назначении ADV_INT.1.1D, чем на остальную часть ФБО. Несмотря на то, что все ФБО должны быть разработаны с использованием хороших технических принципов и практик и в результате представлять собой хорошо структурированные ФБО, только указанное подмножество анализируется на предмет соответствия этой характеристике. Оценщик делает заключение о том, что применение разработчиком стандартов кодирования приводит к понятным ФБО.

Основная цель этого компонента состоит в том, чтобы удостовериться, что представление реализации подмножества ФБО достаточно понятно для облегчения обслуживания и анализа этого подмножества (как для разработчика, так и для оценщика).

10.6.1.4 Действие ADV_INT.1.1E

ИСО/МЭК 15408-3 ADV_INT.1.1C: *В логическом обосновании должно приводиться объяснение того, на основании каких характеристик оценивается «полнота определения» внутренней структуры.*

10.6.1.4.1 Шаг оценивания ADV_INT.1-1

Оценщик должен исследовать логическое обоснование, чтобы сделать заключение о том, что в нём идентифицирована основа для вынесения заключения о том, полно ли определена внутренняя структура ФБО.

Оценщик проверяет, что критерии для определения полноты и правильности определения внутренней структуры ФБО ясно определены в логическом обосновании. Приемлемые критерии, как правило, представлены в промышленных стандартах для технологической дисциплины. Например, процедурное программное обеспечение, которое выполняется линейно, традиционно считается в полной мере структурированным, если оно было написано в соответствии с лучшими техническими практиками программирования, такими, например как определенные в Стандарте IEEE (Стандарт. IEEE 610.12—1990). Это определяет критерии для процедурных частей программного обеспечения подмножества ФБО:

a) процесс, используемый для модульной декомпозиции

b) стандарты кодирования, используемые при разработке реализации

c) описание максимального допустимого уровня связности между модулями, представленными в подмножестве ФБО, и

d) описание минимального допустимого уровня связности между модулями, представленными в подмножестве ФБО.

Для других типов технологий, используемых в ОО, таких как непроцедурное программное обеспечение (например объектно-ориентированного программирования), широко распространенные в качестве товаров аппаратные средства (например микропроцессоры персональных компьютеров) и аппаратные средства специального назначения (например процессоры смарт-карт), оценщику следует получить руководство от органа оценки для того, чтобы определить по заданным критериям полноту определения внутренней структуры.

ИСО/МЭК 15408-3 ADV_INT.1.2C: *В описании внутренней структуры ФБО должно быть продемонстрировано, что внутренняя структура заданного подмножества ФБО является полностью определенной.*

10.6.1.4.2 Шаг оценивания ADV_INT.1-2

Оценщик должен проверить описание внутренней структуры ФБО, чтобы сделать заключение о том, что в ней идентифицировано означенное подмножество ФБО.

Это подмножество может быть идентифицировано в терминах внутренней структуры ФБО на любом уровне абстракции. Например, в терминах структурных элементов ФБО, идентифицированных в проекте ОО (например подсистема аудита), или в терминах реализации (например файлы encrypt.c и decrypt.c или чип 6227 интегральной схемы).

Недостаточно просто идентифицировать это подмножество в терминах требуемых ФТБ (например части ФБО, которые обеспечивают анонимность, как определено в FPR_ANO.2), поскольку при этом не определено, на чем следует сосредоточить деятельность по анализу.

10.6.1.4.3 Шаг оценивания ADV_INT.1-3

Оценщик должен исследовать описание внутренней структуры ФБО, чтобы сделать заключение о том, что оно демонстрирует, что внутренняя структура означенного подмножества ФБО является полностью определенной.

Оценщик исследует описание внутренней структуры, чтобы удостовериться, что оно предоставляет полное объяснение того, каким образом подмножество ФБО соответствует критериям ADV_INT.1-1.

Например, это объясняет, каким образом процедурные части программного обеспечения подмножества ФБО удовлетворяют следующим требованиям по наличию:

a) непосредственного соответствия модулей, идентифицированных в подмножестве ФБО и модулей, описанных в проекте ОО (ADV_TDS),

b) описания того, как в проекте ФБО отражен процесс модульной декомпозиции,

c) логического обоснования всех случаев, где стандарты кодирования не используются или им нет соответствия, и

d) логического обоснования любой связности вне приемлемых границ.

10.6.1.5 Действие ADV_INT.1.2E

10.6.1.5.1 Шаг оценивания ADV_INT.1-4

Оценщик должен сделать заключение о том, что проект ОО для означенного подмножества ФБО имеет полностью определенную внутреннюю структуру.

Оценщик исследует образец проекта ОО, чтобы верифицировать точность логического обоснования. Например, образец проекта ОО анализируется в целях определения его соответствия нормам проектирования и т.д. Как и во всех областях, где оценщик выполняет действия над подмножеством, оценщик предоставляет логическое обоснование объема выборки и области оценивания.

Описание декомпозиции ОО на подсистемы и модули приведет к доводу о том, что полнота определения внутренней структуры ФБО является очевидной. Верификация того, что процедуры структурирования ФБО (как исследуется в ALC_TAT) выполняются, сделает очевидным полноту определения внутренней структуры ФБО.

10.6.1.5.2 Шаг оценивания ADV_INT.1-5

Оценщик должен сделать заключение о том, что означенное подмножество ФБО имеет полностью определенную внутреннюю структуру.

Если ADV_IMP не является частью требуемого доверия, то этот шаг оценивания не применим и поэтому считается удовлетворенным.

Оценщик исследует образец подмножества ФБО, чтобы верифицировать точность описания внутренней структуры. Например, образец процедурных частей программного обеспечения подмножества ФБО анализируется в целях определения его связности и приверженности стандартам кодирования т.д. Как и во всех областях, где оценщик выполняет действия над подмножеством, оценщик предоставляет логическое обоснование объема выборки и области оценивания.

10.6.2 Подвид деятельности по оценке (ADV_INT.2)

10.6.2.1 Цели

Цель данного подвида деятельности — сделать заключение, является ли определенное подмножество ФБО спроектированным и структурированным таким образом, что снижается вероятность уязвимостей и обслуживание ФБО может выполняться без введения уязвимостей.

10.6.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) описание модульного проекта;

b) представление реализации (если ADV_IMP является частью требуемого доверия);

c) описание внутренней структуры ФБО;

d) документация по стандартам кодирования, как следует из ALC_TAT.

10.6.2.3 Замечания по применению

Роль описания внутренней структуры ФБО — представить свидетельства структуры проекта и реализации ФБО.

У структуры проекта есть два аспекта: составные части ФБО и процедуры, использованные при проектировании ФБО. В случае, если ФБО разработаны в манере, совместимой с проектом, представленном в проекте ОО (см. ADV_TDS), оценка проекта ФБО проводится очевидным образом. В случае выполнения процедур проектирования (см. ALC_TAT), оценка методики проектирования ФБО также очевидна.

В случае, когда ФБО реализуются, используя основанное на выполнении процедур программное обеспечение, структура оценивается на основе ее модульности; модули, идентифицированные в описании внутренней структуры, совпадают с теми модулями, которые идентифицированы в проекте ОО (семейство ADV_TDS «Проект ОО»). Модуль состоит из одного или более файлов исходного кода, которые являются наименьшими структурными единицами.

Основная цель этого компонента состоит в том, чтобы удостовериться, что представление реализации подмножества ФБО достаточно понятно для облегчения обслуживания и анализа этого подмножества (как для разработчика, так и для оценщика).

10.6.2.4 Действие ADV_INT.2.1E

ИСО/МЭК 15408-3 ADV_INT.2.1C: *В логическом обосновании должно приводиться объяснение того, на основании каких характеристик оценивается «полнота определения» внутренней структуры.*

10.6.2.4.1 Шаг оценивания ADV_INT.2-1

Оценщик должен исследовать логическое обоснование, чтобы сделать заключение, что в нём идентифицирована основа для вынесения заключения о том, полно ли определена внутренняя структура ФБО.

Оценщик проверяет, что критерии для определения полноты и правильности определения внутренней структуры ФБО ясно определены в логическом обосновании. Приемлемые критерии, как правило, представлены в промышленных стандартах для технологической дисциплины. Например, процедурное программное обеспечение, которое выполняется линейно, традиционно считается в полной мере структурированным, если оно было написано в соответствии с лучшими техническими практиками программирования, такими, например как определенные в Стандарте IEEE (Стандарт. IEEE 610.12—1990). Это определяет критерии для процедурных частей программного обеспечения подмножества ФБО:

a) процесс, используемый для модульной декомпозиции,

b) стандарты кодирования, используемые при разработке реализации,

c) описание максимального допустимого уровня связности между модулями, представленными в подмножестве ФБО, и

d) описание минимального допустимого уровня связности между модулями, представленными в подмножестве ФБО.

Для других типов технологий, используемых в ОО, таких как непроцедурное программное обеспечение (например объектно-ориентированного программирования), широко распространенные в качестве товаров аппаратные средства (например микропроцессоры персональных компьютеров) и аппаратные средства специального назначения (например процессоры смарт-карт), оценщик должен получить руководство от органа оценки для того, чтобы определить по заданным критериям полноту определения внутренней структуры.

ИСО/МЭК 15408-3 ADV_INT.2.2C: *В описании внутренней структуры ФБО должно быть продемонстрировано, что внутренняя структура означенного подмножества ФБО является полностью определенной.*

10.6.2.4.2 Шаг оценивания ADV_INT.2-2

Оценщик должен исследовать описание внутренней структуры ФБО, чтобы сделать заключение о том, что оно демонстрирует, что внутренняя структура означенного подмножества ФБО является полностью определенной.

Оценщик исследует описание внутренней структуры, чтобы удостовериться, что оно предоставляет полное объяснение того, каким образом подмножество ФБО соответствует критериям ADV_INT.1-1.

Например, это объясняет, каким образом процедурные части программного обеспечения подмножества ФБО удовлетворяют следующим требованиям по наличию:

a) непосредственного соответствия модулей, идентифицированных в подмножестве ФБО и модулей, описанных в проекте ОО (ADV_TDS),

b) описания того, как в проекте ФБО отражен процесс модульной декомпозиции,

c) логического обоснования всех случаев, где стандарты кодирования не используются или им нет соответствия, и

d) логического обоснования любой связности вне приемлемых границ.

10.6.2.5 Действие ADV_INT.2.2E

10.6.2.5.1 Шаг оценивания ADV_INT.2-3

Оценщик должен сделать заключение о том, что проект ОО имеет полностью определенную внутреннюю структуру.

Оценщик исследует образец проекта ОО, чтобы верифицировать точность логического обоснования. Например, образец проекта ОО анализируется в целях определения его соответствия нормам проектирования и т.д. Как и во всех областях, где оценщик выполняет действия над подмножеством, оценщик предоставляет логическое обоснование объема выборки и области оценивания.

Описание декомпозиции ОО на подсистемы и модули приведет к выводу о том, что полнота определения внутренней структуры ФБО является очевидной. Верификация того, что процедуры структу-

рирования ФБО (как исследуется в ALC_TAT) выполняются, сделает очевидным полноту определения внутренней структуры ФБО.

10.6.2.5.2 Шаг оценивания ADV_INT.2-4

Оценщик должен сделать заключение о том, что означенное подмножество ФБО имеет полностью определенную внутреннюю структуру.

Если ADV_IMP не является частью требуемого доверия, то этот шаг оценивания не применим и поэтому считается удовлетворенным.

Оценщик исследует образец подмножества ФБО, чтобы верифицировать точность описания внутренней структуры. Например, образец процедурных частей программного обеспечения подмножества ФБО анализируется в целях определения его связности и приверженности стандартам кодирования. Как и во всех областях, где оценщик выполняет действия над подмножеством, оценщик предоставляет логическое обоснование объема выборки и области оценивания.

10.6.3 Подвид деятельности по оценке (ADV_INT.3)

Общее руководство отсутствует; за консультациями по выполнению данного подвида деятельности следует обращаться в конкретную систему оценки.

10.7 Моделирование политики безопасности (ADV_SMP)

10.7.1 Подвид деятельности по оценке (ADV_SPM.1)

Общее руководство отсутствует; за консультациями по выполнению данного подвида деятельности следует обращаться в конкретную систему оценки.

10.8 Проект ОО (ADV_TDS)

10.8.1 Подвид деятельности по оценке (ADV_TDS.1)

10.8.1.1 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) описание архитектуры безопасности;

d) проект ОО.

10.8.1.2 Действие ADV_TDS.1.1E

ИСО/МЭК 15408-3 ADV_TDS.1.1C: *В проекте должно приводиться описание структуры ОО на уровне подсистем.*

10.8.1.2.1 Шаг оценивания ADV_TDS.1-1

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что структура всего ОО описана в терминах подсистем.

Оценщик удостоверяется, что все подсистемы ОО идентифицированы. Это «Описание ОО» будет использоваться в качестве исходных данных для шага оценивания ADV_TDS.1-2, где идентифицированы части ОО, которые составляют ФБО. Таким образом, это требование относится ко всему ОО, а не только к ФБО.

ОО (и ФБО) может быть описан на нескольких уровнях детализации (то есть подсистем и модулей). В зависимости от сложности ОО, его проект может быть описан в терминах подсистем и модулей, как описано в ИСО/МЭК 15408-3, Приложение А.4 ADV_TDS: «Подсистемы и модули». На этом уровне доверия декомпозиция требуется только на уровне подсистем.

При выполнении этой деятельности оценщик исследует другие свидетельства, представленные ОО (например ЗБ, пользовательское руководство оператора), чтобы сделать заключение о том, что «Описание ОО» в таких свидетельствах совместимо с описанием, содержавшимся в проекте ОО.

ИСО/МЭК 15408-3 ADV_TDS.1.2C: *В проекте должны быть идентифицированы все подсистемы ФБО.*

10.8.1.2.2 Шаг оценивания ADV_TDS.1-2

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что все подсистемы ФБО идентифицированы.

В шаге оценивания ADV_TDS.1-1 были идентифицированы все подсистемы ОО и вынесено заключение о том, что подсистемы, не относящиеся к ФБО, правильно охарактеризованы. Основываясь на этом, подсистемы, которые не характеризовались как не относящиеся к ФБО, следует точно идентифицировать. Оценщик делает заключение о том, что для аппаратного и программного обеспечения, установленного и настроенного согласно руководству в семействе AGD_PRE «Подготовительные процедуры», каждая подсистема идентифицирована или как являющаяся частью ФБО или как не являющаяся.

ИСО/МЭК 15408-3 ADV_TDS.1.3C: *В проекте должно приводиться описание режима функционирования для каждой подсистемы, поддерживающей выполнение ФТБ или не влияющей на их выполнение, с предоставлением детальной информации, достаточной для того, чтобы установить, что подсистема не является осуществляющей выполнение ФТБ.*

10.8.1.2.3 Шаг оценивания ADV_TDS.1-3

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что каждая подсистема ФБО, являющаяся поддерживающей выполнение ФТБ или не влияющей на выполнение ФТБ, описана таким образом, что оценщик может сделать вывод о том, что подсистема является поддерживающей выполнение ФТБ или не влияющей на выполнение ФТБ.

Поддерживающие и не влияющие на выполнение ФТБ подсистемы не нужно описывать подробно относительно того, как они функционируют в системе. Однако оценщик на основании свидетельств, предоставленных разработчиком, делает заключение, что подсистемами, у которых нет описаний верхнего уровня, являются поддерживающие выполнение ФТБ или не влияющие на выполнение ФТБ. Следует отметить, что если разработчик предоставляет однородный уровень детализации при предоставлении документации, тогда этот шаг оценивания будет в основном выполнен, так как смысл категоризации подсистем в том, чтобы позволить разработчику предоставлять меньше информации относительно поддерживающих и не влияющих на выполнение ФТБ подсистем, чем для подсистем, осуществляющих выполнение ФТБ.

Поддерживающая выполнение ФТБ подсистема — та, которая зависит от осуществляющей выполнение ФТБ в удовлетворении ФТБ, но не играет в этом роль напрямую в отличие от осуществляющей выполнение ФТБ подсистемы. Подсистема, не влияющая на выполнение ФТБ, это та подсистема, которая не является поддерживающей или помогающей в выполнении ФТБ, от неё в плане выполнения ФТБ другие подсистемы не зависят.

ИСО/МЭК 15408-3 ADV_TDS.1.4C: *В проекте должна приводиться аннотация осуществляющих выполнение ФТБ режимов безопасности тех подсистем, которые являются осуществляющими выполнение ФТБ.*

10.8.1.2.4 Шаг оценивания ADV_TDS.1-4

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что он предоставляет полное и точное описание верхнего уровня для обеспечивающего выполнение ФТБ режима функционирования подсистем, обеспечивающих выполнение ФТБ.

Разработчик может определять подсистемы как обеспечивающие выполнение ФТБ, поддерживающие выполнение ФТБ или не влияющие на выполнение ФТБ, но эти «категории» используются только для того, чтобы описать количество и тип информации, которую должен предоставить разработчик, и может использоваться для ограничения количества информации, которую должен предоставить разработчик в том случае, если сам процесс разработки не производит требуемую документацию. Были подсистемы категоризированы разработчиком или нет, в обязанности оценщика входит задача вынести заключение о том, что в подсистемы включена соответствующая их роли в ОО (обеспечивающие выполнение ФТБ и т.д.) информация и получить соответствующую информацию от разработчика в случае, если разработчик не в состоянии предоставить необходимую информацию для конкретной подсистемы.

Обеспечивающий выполнение ФТБ режим функционирования ссылается на то, каким образом подсистемой выполняются функции, которые обеспечивают выполнение ФТБ. Описание верхнего уровня не должно относиться к определенным структурам данных (хотя такой случай возможен), но описывает в общем потоки данных, потоки сообщений и взаимоотношения контроля в пределах подсистемы. Цель этих описаний состоит в том, чтобы предоставить оценщику достаточно информации для понимания того, каким образом достигается обеспечивающий выполнение ФТБ режим функционирования. Следует отметить, что для данного шага оценивания оценщику следует считать недопустимым заявления об обеспечении выполнения ФТБ в документации проекта ОО. Также следует отметить, что заключение оценщика, с точки зрения описания верхнего уровня, выносится для конкретного ОО, и оценщик для вынесения правильного вердикта по данному шагу оценивания должен получить достаточно информации от разработчика.

Чтобы определить полноту и точность, оценщик исследует другую доступную информацию (например функциональную спецификацию, описание архитектуры безопасности, представление реализации). Описаниям функций в этих документах следует быть совместимыми с тем, что предоставлено в свидетельствах данного шага оценивания.

ИСО/МЭК 15408-3 ADV_TDS.1.5C: *В проекте должно приводиться описание взаимодействий между осуществляющими выполнение ФТБ подсистемами ФБО, а также между ними и другими подсистемами ФБО.*

10.8.1.2.5 Шаг оценивания ADV_TDS.1-5

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что в нем приведены описания взаимодействий между подсистемами ФБО.

Цель описания взаимодействий между осуществляющими выполнение ФТБ подсистемами и другими подсистемами состоит в том, чтобы предоставить читателю лучшее понимание того, каким образом ФБО выполняют свои функции. Эти взаимодействия не должны быть характеризованы на уровне реализации (например параметры из процедуры в одной подсистеме переходят к процедуре другой подсистемы; глобальные переменные; сигналы аппаратных средств (например прерывания) от подсистемы аппаратных средств до системы обработки прерываний), но элементы данных, идентифицированных для конкретной подсистемы, которые будут использоваться другой подсистемой, должны быть охвачены этим рассмотрением. Любые отношения контроля между подсистемами (например имеется подсистема, ответственная за формирование базовых правил для межсетевого экрана и подсистема, которая фактически реализует эти правила) также следует включать в описание.

Оценщику нужно использовать свое собственное суждение при оценивании полноты описания. Если причина взаимодействия подсистем неясна или если есть относящиеся к выполнению ФТБ взаимодействия (выявленные, например в ходе анализа описания режимов функционирования подсистемы), которые недостаточно ясно описаны, оценщику следует удостовериться, что эта информация предоставлена разработчиком. Однако, если оценщик может сделать заключение о том, что взаимодействия между конкретным набором подсистем, хотя и не полностью описаны разработчиком, не помогут ни в понимании общих функций, ни в понимании функций безопасности, обеспечиваемых ФБО, тогда оценщик может считать описание достаточным; полнота описания ради самой полноты не преследуется.

ИСО/МЭК 15408-3 ADV_TDS.1.6C: *В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.*

10.8.1.2.6 Шаг оценивания ADV_TDS.1-6

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что он содержит полное и точное прослеживание от ИФБО, описанных в функциональной спецификации, к подсистемам ФБО, описанным в проекте ОО.

В описании подсистем в проекте ОО предоставляется описание того, каким образом ФБО реализуются, достаточно детально для обеспечивающих выполнение ФТБ частей ФБО и на более высоком уровне представления для других частей ФБО. ИФБО обеспечивают описание того, каким образом осуществлена реализация. Свидетельства от разработчика идентифицируют подсистему, которая вовлечена в процесс запроса операции от ИФБО, и идентифицируют различные подсистемы, которые прежде всего ответственны за реализацию функций. Следует отметить, что для данного шага оценивания не требуется предоставление полного «дерева вызовов» для каждого ИФБО.

Оценщик оценивает полноту прослеживания, удостоверяясь, что каждый ИФБО прослежен по крайней мере к одной подсистеме. Проверка точности сложнее.

Первый аспект точности заключается в том, что каждый ИФБО прослеживается к подсистеме, находящейся в пределах ФБО. Такое заключение может быть сделано при рассмотрении описания подсистем и их взаимодействия и определении места подсистемы в архитектуре безопасности на основании данной информации. Следующий аспект точности — то, что прослеживание имеет смысл. Например, прослеживание ИФБО, обеспечивающего контроль доступа, к подсистеме, которая проверяет пароли, не будет являться точным. Оценщику и в этом случае при вынесении заключения следует использовать свое суждение. Цель состоит в том, что эта информация поможет оценщику в понимании системы, реализации выполнения ФТБ и способов, которыми сущности в пределах ФБО могут взаимодействовать с ФБО. Большая часть оценки того, точно ли описаны ФТБ подсистемами, выполняется при проведении других шагов оценивания.

10.8.1.3 Действие ADV_TDS.1.2E

10.8.1.3.1 Шаг оценивания ADV_TDS.1-7

Оценщик должен исследовать ФТБ ОО и проект ОО, чтобы сделать заключение о том, что все ФТБ в ЗБ охвачены в проекте ОО.

Оценщик может провести прослеживание между ФТБ для ОО и проектом ОО. Это прослеживание, вероятно, будет проводиться от функционального требования до ряда подсистем и будет по уровню детализации ниже, чем для компонента или даже для элемента требований, из-за операций (назначения, уточнения, выбора), которые выполняются над функциональным требованием автором ЗБ.

Например, компонент FDP_ACC.1 «Ограниченное управление доступом» содержит элемент с операцией назначения. Если бы в ЗБ содержалось, например десять правил в назначении для данного компонента FDP_ACC.1, и эти правила применялись бы в определенных местах в пределах пятнадцати модулей, то для оценщика некорректно было бы проследить компонент FDP_ACC.1 к одной подсистеме и утверждать о завершении шага оценивания. Вместо этого оценщик должен проследить первое правило компонента FDP_ACC.1 к подсистеме A и режимам функционирования x, y и z; второе правило компонента FDP_ACC.1 к подсистеме A и режимам функционирования x, p и q; и т. д.

10.8.1.3.2 Шаг оценивания ADV_TDS.1-8

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что в нем точно представлены все ФТБ.

Оценщик удостоверяется, что для каждого из ФТБ, перечисленных в подразделе ЗБ «Функциональные требования безопасности», есть соответствующее описание в проекте ОО, которое детализирует, каким образом ФБО отвечают этому требованию. Это требуется для того, чтобы оценщик идентифицировал собрание подсистем, которые отвечают за осуществление данного функционального требования, а затем исследовал эти подсистемы, чтобы понять, каким образом выполняется требование. Наконец, оценщик оценивает точность выполнения требования.

Например, если требования в ЗБ определяют основанный на ролевой модели механизм управления доступом, то оценщик сначала идентифицирует подсистемы, которые способствуют реализации этого механизма. Это может быть сделано с применением углубленного изучения или с применением понимания проекта ОО или работ, полученных в предыдущих шагах оценивания. Следует отметить, что это прослеживание необходимо только для идентификации подсистем и не является полным анализом.

Следующий шаг — понять, какой из механизмов подсистемы осуществляется. Например, если в проекте описывается реализация управления доступом, основанная на битах защиты UNIX, то проект не является точным отражением требований по управлению доступом в ЗБ для того примера, который использовался выше. Если оценщик не может сделать заключение о том, что механизм был реализован точным образом из-за недостаточной детализации предоставленной ему информации, то ему нужно будет оценить, были ли все осуществляющие выполнение ФТБ подсистемы идентифицированы и был ли предоставлен для этих подсистем достаточный уровень детализации.

10.8.2 Подвид деятельности по оценке (ADV_TDS.2)

10.8.2.1 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) описание архитектуры безопасности;

d) проект ОО.

10.8.2.2 Действие ADV_TDS.2.1E

ИСО/МЭК 15408-3 ADV_TDS.2.1C: *В проекте должно приводиться описание структуры ОО на уровне подсистем.*

10.8.2.2.1 Шаг оценивания ADV_TDS.2-1

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что структура всего ОО описана в терминах подсистем.

Оценщик удостоверяется, что все подсистемы ОО идентифицированы. Это «Описание ОО» будет использоваться в качестве исходных данных для шага оценивания ADV_TDS.2-2, где идентифицированы части ОО, которые составляют ФБО. Таким образом, это требование относится ко всему ОО, а не только к ФБО.

ОО (и ФБО) может быть описан на нескольких уровнях детализации (то есть подсистем и модулей). В зависимости от сложности ОО его проект может быть описан в терминах подсистем и модулей, как описано в ИСО/МЭК 15408-3, приложение A.4 ADV_TDS: «Подсистемы и модули». На этом уровне доверия декомпозиция требуется только на уровне подсистем.

При выполнении этой деятельности оценщик исследует другие свидетельства, представленные ОО (например ЗБ, пользовательское руководство оператора), чтобы сделать заключение о том, что «Описание ОО» в таких свидетельствах совместимо с описанием, содержавшимся в проекте ОО.

ИСО/МЭК 15408-3 ADV_TDS.2.2C: *В проекте должны быть идентифицированы все подсистемы ФБО.*

10.8.2.2.2 Шаг оценивания ADV_TDS.2-2

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что все подсистемы ФБО идентифицированы.

В шаге оценивания ADV_TDS.2-1 были идентифицированы все подсистемы ОО, и вынесено заключение о том, что подсистемы, не относящиеся к ФБО, правильно охарактеризованы. Основываясь на этом, подсистемы, которые не характеризовались как не относящиеся к ФБО, следует точно идентифицировать. Оценщик делает заключение о том, что для аппаратного и программного обеспечения, установленного и настроенного согласно руководству в семействе «Подготовительные процедуры» (AGD_PRE), каждая подсистема идентифицирована или как являющаяся частью ФБО, или как не являющаяся.

ИСО/МЭК 15408-3 ADV_TDS.2.3C: *В проекте должно приводиться описание режима функционирования для каждой подсистемы ФБО, не влияющей на выполнение ФТБ, с предоставлением детальной информации, достаточной для того, чтобы установить, что подсистема не влияет на выполнение ФТБ.*

10.8.2.2.3 Шаг оценивания ADV_TDS.2-3

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что каждая подсистема ФБО, не влияющая на выполнение ФТБ, описана таким образом, что оценщик может сделать вывод о том, что подсистема является не влияющей на выполнение ФТБ.

Не влияющие на выполнение ФТБ подсистемы не нужно описывать подробно относительно того, как они функционируют в системе. Однако оценщик на основании свидетельств, предоставленных разработчиком, выносит заключение, что подсистемами, у которых нет описаний верхнего уровня, являются не влияющие на выполнение ФТБ. Следует отметить, что если разработчик предоставляет однородный уровень детализации при предоставлении документации, тогда этот шаг оценивания будет в основном выполнен, так как смысл категоризации подсистем в том, чтобы позволить разработчику предоставлять меньше информации относительно не влияющих на выполнение ФТБ подсистем, чем для подсистем, осуществляющих выполнение ФТБ и поддерживающих выполнение ФТБ.

Не влияющая на выполнение ФТБ подсистема та, от которой не зависят осуществляющие и поддерживающие выполнение ФТБ; она не играет роли в осуществлении функций выполнения ФТБ.

ИСО/МЭК 15408-3 ADV_TDS.2.4C: *В проекте должно приводиться описание осуществляющих выполнение ФТБ режимов безопасности тех подсистем, которые являются осуществляющими выполнение ФТБ.*

10.8.2.2.4 Шаг оценивания ADV_TDS.2-4

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что он предоставляет полное, точное и детальное описание для обеспечивающего выполнение ФТБ режима функционирования подсистем, обеспечивающих выполнение ФТБ.

Разработчик может определять подсистемы как обеспечивающие выполнение ФТБ, поддерживающие выполнение ФТБ или не влияющие на выполнение ФТБ, но эти «категории» используются только для того, чтобы описать количество и тип информации, которую должен предоставить разработчик, и может использоваться для ограничения количества информации, которую должен предоставить разработчик в том случае, если сам процесс разработки не производит требуемую документацию. Были подсистемы категорированы разработчиком или нет, в обязанности оценщика входит задача вынести заключение о том, что в подсистемы включена соответствующая их роли в ОО (обеспечивающие выполнение ФТБ и т.д.) информация и получить соответствующую информацию от разработчика в случае, если разработчик не предоставил необходимую информацию для конкретной подсистемы.

Обеспечивающий выполнение ФТБ режим функционирования ссылается на то, каким образом подсистемой выполняются функции, которые обеспечивают выполнение ФТБ. Детализированное описание режима функционирования, хотя и не приводится на уровне алгоритмического описания, описывает то, каким образом предоставляется функциональная возможность, в терминах того, что представляют собой данные ключа и структуры данных, какие взаимоотношения контроля существуют внутри подсистемы и каким образом данные элементы функционируют вместе для предоставления обеспечивающего выполнение ФТБ режима функционирования. Такое описание также ссылается на поддерживающий выполнение ФТБ режим функционирования, который следует рассматривать оценщику при выполнении последующих шагов оценивания.

Чтобы определить полноту и точность, оценщик исследует другую доступную информацию (например функциональную спецификацию, описание архитектуры безопасности, представление реализации). Описаниям функций в этих документах следует быть совместимыми с тем, что предоставляется в свидетельствах данного шага оценивания.

ИСО/МЭК 15408-3 ADV_TDS.2.5C: *В проекте должна приводиться аннотация поддерживающих и не влияющих на выполнение ФТБ режимов безопасности тех подсистем, которые являются осуществляющими выполнение ФТБ.*

10.8.2.2.5 Шаг оценивания ADV_TDS.2-5

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что он предоставляет полное и точное описание верхнего уровня для поддерживающих и не влияющих на выполнение ФТБ режимов функционирования подсистем, обеспечивающих выполнение ФТБ.

Разработчик может определять подсистемы как обеспечивающие выполнение ФТБ, поддерживающие выполнение ФТБ или не влияющие на выполнение ФТБ, но эти «категории» используются только для того, чтобы описать количество и тип информации, которую должен предоставить разработчик, и может использоваться для ограничения количества информации, которую должен предоставить разработчик в том случае, если сам процесс разработки не производит требуемую документацию. Были подсистемы категорированы разработчиком или нет, в обязанности оценщика входит задача вынести заключение о том, что в подсистемы включена соответствующая их роли в ОО (обеспечивающие выполнение ФТБ и т.д.) информация и получить соответствующую информацию от разработчика в случае, если разработчик не предоставил необходимую информацию для конкретной подсистемы.

В отличие от предыдущего шага оценивания, на этом шаге оценивания требуется, чтобы оценщик оценил поддерживающую и не влияющую на выполнение ФТБ информацию, предоставленную для осуществляющих выполнение ФТБ подсистем. У этой оценки двойная цель. Во-первых, следует, чтобы оценивание предоставило оценщику лучшее понимание способа функционирования для каждой подсистемы. Во-вторых, оценщик делает заключение о том, что описаны все осуществляющие выполнение ФТБ режимы функционирования, имеющиеся в подсистеме. В отличие от предыдущего шага оценивания, информация, предусмотренная для описания поддерживающих или не влияющих на выполнение ФТБ режимов функционирования, не должна быть настолько детализированной, как информация по осуществляющему выполнение ФТБ режиму функционирования. Например, для структуры данных или элементов данных, которые не относятся к осуществляющим выполнение ФТБ функциям, не должно быть приведено подробных описаний (а также описания могут быть вовсе не нужны). Решение относительно того, что «высокий уровень» описания значит для конкретного ОО, возлагается на оценщика, и оценщик должен получить достаточно информации от разработчика (даже если она окажется эквивалентной информации, предусмотренной для подсистем, которые являются осуществляющими выполнение ФТБ) для вынесения положительного вердикта по данному шагу оценивания.

Оценщику следует помнить, однако, что целью данного шага оценивания не является приобретение «совершенного» доверия, поэтому суждение оценщика должно применяться при внесении заключения о количестве и составе свидетельств, требуемых для вынесения вердикта для данного шага оценивания.

Чтобы определить полноту и точность, оценщик исследует другую доступную информацию (например функциональную спецификацию, описание архитектуры безопасности, представление реализации). Описаниям функций в этих документах следует быть совместимыми с тем, что обеспечено свидетельствами данного шага оценивания. В частности, следует использовать функциональную спецификацию для вынесения заключение о том, что режим функционирования, необходимый для осуществления интерфейсов ФБО, описанных в функциональной спецификации, полностью описан подсистемой, так как режим функционирования будет или осуществляющим, или поддерживающим, или не влияющим на выполнение ФТБ.

ИСО/МЭК 15408-3 ADV_TDS.2.6C: *В проекте должна приводиться аннотация режимов безопасности тех подсистем, которые являются осуществляющими выполнение ФТБ.*

10.8.2.2.6 Шаг оценивания ADV_TDS.2-6

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что он предоставляет полное и точное описание верхнего уровня для режимов функционирования подсистем, поддерживающих выполнение ФТБ.

Разработчик может определять подсистемы как обеспечивающие выполнение ФТБ, поддерживающие выполнение ФТБ или не влияющие на выполнение ФТБ, но эти «категории» используются только для того, чтобы описать количество и тип информации, которую должен предоставить разработчик, и может использоваться для ограничения количества информации, которую должен предоставить разработчик в том случае, если сам процесс разработки не производит требуемую документацию. Были подсистемы категорированы разработчиком или нет, в обязанности оценщика входит задача вынести заключение о том, что в подсистемы включена соответствующая их роли в ОО (обеспечивающие выполнение ФТБ и т.д.) информация и получить соответствующую информацию от разработчика в случае, если разработчик не предоставил необходимую информацию для конкретной подсистемы.

В отличие от предыдущих двух шагов оценивания, на этом шаге оценивания требуется, чтобы разработчик предоставил, а оценщик оценил информацию по поводу поддерживающих выполнение ФТБ подсистем. На такие подсистемы следует ссылаться в описаниях осуществляющих выполнение ФТБ подсистем, так же, как и в описаниях взаимодействий для шага оценивания ADV_TDS.2-7. У этой оценки, как и на предыдущем шаге оценивания, двойная цель. Во-первых, следует, чтобы оценивание предоставляло оценщику лучшее понимание способа функционирования для каждой поддерживающей выполнение ФТБ подсистемы. Во-вторых, оценщик делает заключение о том, что все режимы функционирования, имеющиеся в подсистеме, описаны в должной степени детализации для ясного определения способа поддержания подсистемой режима функционирования и того, что сам режим при этом не является осуществляющим выполнение ФТБ. Информация, предусмотренная для описания режимов функционирования подсистем, поддерживающих выполнение ФТБ, не должна быть такой же детализированной, как информация по осуществляющему выполнение ФТБ режиму функционирования. Например, для структуры данных или элементов данных, которые не относятся к осуществляющим выполнение ФТБ функциям, не должно быть приведено подробных описаний (а также описания могут быть вовсе не нужны). Решение относительно того, что «высокий уровень» описания значит для конкретного ОО, возлагается на оценщика, и оценщик должен получить достаточно информации от разработчика (даже если она окажется эквивалентной информации, предусмотренной для подсистем, которые являются осуществляющими выполнение ФТБ) для вынесения вердикта по данному шагу оценивания.

Оценщику следует помнить, однако, что целью данного шага оценивания не является приобретение «совершенного» доверия, поэтому суждение оценщика должно применяться при внесении заключения о количестве и составе свидетельств, требуемых для вынесения вердикта для данного шага оценивания.

Чтобы определить полноту и точность, оценщик исследует другую доступную информацию (например функциональную спецификацию, описание архитектуры безопасности, представление реализации). Описаниям функций в этих документах следует быть совместимыми с тем, что предоставлено в свидетельствах данного шага оценивания. В частности, следует использовать функциональную спецификацию для вынесения заключения о том, что режим функционирования, необходимый для осуществления интерфейсов ФБО, описанных в функциональной спецификации, полностью описан подсистемой, так как режим функционирования будет или осуществляющим, или поддерживающим, или не влияющим на выполнение ФТБ.

ИСО/МЭК 15408-3 ADV_TDS.2.7C: *В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.*

10.8.2.2.7 Шаг оценивания ADV_TDS.2-7

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что в нем приведены описания взаимодействия между подсистемами ФБО.

Цель описания взаимодействий между осуществляющими выполнение ФТБ подсистемами и другими подсистемами состоит в том, чтобы предоставить читателю лучшее понимание того, каким образом ФБО выполняют свои функции. Эти взаимодействия не должны быть характеризованы на уровне реализации (например параметры из одной процедуры в одной подсистеме переходят к процедуре другой подсистемы; глобальные переменные; сигналы аппаратных средств (например прерывания) от подсистемы аппаратных средств до системы обработки прерываний), но элементы данных, идентифицированных для конкретной подсистемы, которые будут использоваться другой подсистемой, должны быть охвачены этим рассмотрением. Любые отношения контроля между подсистемами (например имеется подсистема, ответственная за формирование базовых правил для межсетевого экрана и подсистемы, которая фактически реализует эти правила) также следует включать в описание.

Следует отметить, что хотя разработчику следует характеризовать все взаимодействия между подсистемами, оценщику нужно использовать свое собственное суждение при оценивании полноты описания. Если причина взаимодействия подсистем не ясна или если есть относящиеся к выполнению ФТБ взаимодействия (выявленные, например в ходе анализа описания режимов функционирования подсистемы), которые недостаточно ясно описаны, оценщику следует удостовериться, что эта информация предоставлена разработчиком. Однако, если оценщик может сделать заключение о том, что взаимодействия между конкретным набором подсистем, хотя и не полностью описаны разработчиком, не помогут ни в понимании общих функций, ни в понимании функций безопасности, обеспечиваемых ФБО, тогда оценщик может считать описание достаточным; полнота описания ради самой полноты не преследуется.

ИСО/МЭК 15408-3 ADV_TDS.2.8C: *В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.*

10.8.2.2.8 Шаг оценивания ADV_TDS.2-8

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что он содержит полное и точное прослеживание от ИФБО, описанных в функциональной спецификации, к подсистемам ФБО, описанным в проекте ОО.

Описание подсистем в проекте ОО представляет описание того, каким образом ФБО реализуются, достаточно детально для обеспечивающих выполнение ФТБ частей ФБО, и на более высоком уровне представления для других частей ФБО. ИФБО обеспечивают описание того, каким образом осуществлена реализация. Свидетельства от разработчика идентифицируют подсистему, которая вовлечена в процесс запроса операции от ИФБО, и идентифицируют различные подсистемы, которые прежде всего ответственны за реализацию функций. Следует отметить, что для данного шага оценивания не требуется предоставления полного «дерева вызовов» для каждого ИФБО.

Оценщик оценивает полноту прослеживания, удостоверяясь, что каждый ИФБО прослежен по крайней мере к одной подсистеме. Проверка точности более сложна.

Первый аспект точности заключается в том, что каждый ИФБО прослеживается к подсистеме, находящейся в пределах ФБО. Такое заключение может быть сделано при рассмотрении описания подсистем, их взаимодействия и при определении места подсистемы в архитектуре безопасности на основании данной информации. Следующий аспект точности — то, что прослеживание имеет смысл. Например, прослеживание ИФБО, обеспечивающего контроль доступа, к подсистеме, которая проверяет пароли, не будет являться точным. Оценщику и в этом случае следует при вынесении заключения использовать свое суждение. Цель состоит в том, что эта информация поможет оценщику в понимании системы, реализации выполнения ФТБ и способов, которыми сущности в пределах ФБО могут взаимодействовать с ФБО. Большая часть оценки того, точно ли описаны ФТБ подсистемами, выполняется при проведении других шагов оценивания.

10.8.2.3 Действие ADV_TDS.2.2E

10.8.2.3.1 Шаг оценивания ADV_TDS.2-9

Оценщик должен исследовать ФТБ ОО и проект ОО, чтобы сделать заключение о том, что все ФТБ в ЗБ охвачены в проекте ОО.

Оценщик может провести прослеживание между ФТБ для ОО и проектом ОО. Это прослеживание, вероятно, будет проводиться от функционального требования до ряда подсистем. Следует отметить, что это прослеживание, вероятно, будет по уровню детализации ниже, чем для компонента или даже для элемента требований, из-за операций (назначения, уточнения, выбора), которые выполняются над функциональным требованием автором ЗБ.

Например, компонент FDP_ACC.1 «Ограниченное управление доступом» содержит элемент с операцией назначения. Если бы в ЗБ содержалось, например десять правил в назначении для данного компонента FDP_ACC.1, и эти правила применялись бы в определенных местах в пределах пятнадцати модулей, то для оценщика некорректно было бы проследить компонент FDP_ACC.1 к одной подсистеме и утверждать о завершении шага оценивания. Вместо этого оценщик должен проследить первое правило компонента FDP_ACC.1 к подсистеме A и режимам функционирования x, y и z; второе правило компонента FDP_ACC.1 к подсистеме A и режимам функционирования x, p и q; и т.д.

10.8.2.3.2 Шаг оценивания ADV_TDS.2-10

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что в нем точно представлены все ФТБ.

Оценщик удостоверяется, что для каждого из ФТБ, перечисленных в подразделе ЗБ «Функциональные требования безопасности», есть соответствующее описание в проекте ОО, которое детализирует, каким образом ФБО отвечают этому требованию. Это требуется для того, чтобы оценщик идентифицировал собрание подсистем, которые отвечают за осуществление данного функционального требования, а затем исследовал эти подсистемы, чтобы понять, каким образом выполняется требование. Наконец, оценщик оценивает точность выполнения требования.

Например, если требования в ЗБ определяют основанный на ролевой модели механизм управления доступом, оценщик сначала идентифицирует подсистемы, которые способствуют реализации этого механизма. Это может быть сделано с применением углубленного изучения или с применением понимания проекта ОО или работ, полученных в предыдущих шагах оценивания. Следует отметить, что это прослеживание необходимо только для идентификации подсистем и не является полным анализом.

Следующий шаг — понять, какой из механизмов подсистемы осуществляется. Например, если в проекте описывается реализация управления доступом, основанная на битах защиты UNIX, то проект не является точным отражением требований по управлению доступом в ЗБ для того примера, который

использовался выше. Если оценщик не может сделать заключение о том, что механизм был реализован точным образом из-за недостаточной детализации предоставленной ему информации, то ему нужно будет оценить, были ли все осуществляющие выполнение ФТБ подсистемы идентифицированы и был ли предоставлен для этих подсистем достаточный уровень детализации.

10.8.3 Подвид деятельности по оценке (ADV_TDS.3)

10.8.3.1 Цели

Цель этого подвида деятельности состоит в том, чтобы определить, обеспечено ли в проекте ОО «Описание ОО» в терминах подсистем, достаточное для определения границ ФБО, и обеспечено ли описание внутренней структуры ФБО в терминах модулей (и, опционально, представлений верхнего уровня). Оценщику предоставляется подробное описание осуществляющих выполнение ФТБ модулей и достаточный объем информации о поддерживающих и не влияющих на выполнение ФТБ модулей, чтобы сделать заключение о том, что ФТБ полностью и точно осуществлены; как таковой, проект ОО предоставляет объяснение представления реализации.

10.8.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) описание архитектуры безопасности;

d) проект ОО.

10.8.3.3 Замечания по применению

Есть три типа деятельности, которую оценщик должен предпринять относительно проекта ОО. Во-первых, оценщик делает заключение о том, что границы ФБО описана достаточным образом. Во-вторых, оценщик делает заключение о том, что разработчик предоставил документацию, которая соответствует содержанию и требованиям представления для этой подсистемы, и эта документация совместима с другой документацией, предусмотренной для ОО. Наконец, оценщик должен проанализировать информацию о проекте, включая описание осуществляющих выполнение ФТБ модулей (подробно) и поддерживающих и не влияющих на выполнение ФТБ (менее подробно) для того, чтобы понять, каким образом реализована система, и с этим пониманием удостовериться, что ИФБО в функциональной спецификации описаны достаточным образом, и что тестовая информация в достаточной мере тестирует ФБО (проводится в шагах оценивания класса ATE: Тестирование).

Важно отметить, что, в то время как разработчик обязан обеспечить полное описание ФБО (хотя и в меньшей степени детализации для поддерживающих и не влияющих на выполнение ФТБ модулей, чем для осуществляющих выполнение ФТБ), предполагается, что оценщик будет использовать собственное суждение при выполнении анализа ФБО. Хотя и ожидается, что оценщик будет исследовать каждый модуль, степень детализации при таком рассмотрении может быть различной. Оценщик анализирует каждый модуль, чтобы определить степень влияния функций модуля на безопасность системы; глубина анализа может изменяться в зависимости от роли модуля в системе. Важный аспект этого анализа — то, что оценщику следует использовать другую предоставленную ему документацию (краткую и функциональную спецификацию ОО, описание архитектуры безопасности, документацию по внутренней структуре ФБО), чтобы сделать заключение о том, что описанные функции правильны, и что неявное обозначение поддерживающих или не влияющих на выполнение ФТБ модулей (см. ниже) поддерживается их ролью в системной архитектуре.

Разработчик может определять модули как обеспечивающие выполнение ФТБ, поддерживающие выполнение ФТБ или не влияющие на выполнение ФТБ, но эти «категории» используются только для того, чтобы описать количество и тип информации, которую должен предоставить разработчик, и может использоваться для ограничения количества информации, которую должен предоставить разработчик в том случае, если сам процесс разработки не производит требуемую документацию. Были модули категорированы разработчиком или нет, в обязанности оценщика входит задача вынести заключение о том, что в модули включена соответствующая их роли в ОО (обеспечивающие выполнение ФТБ и т.д.) информация и получить соответствующую информацию от разработчика в случае, если разработчик не предоставил необходимую информацию для конкретного модуля.

10.8.3.4 Действие ADV_TDS.3.1E

ИСО/МЭК 15408-3 ADV_TDS.3.1C: *В проекте должно приводиться описание структуры ОО на уровне подсистем.*

10.8.3.4.1 Шаг оценивания ADV_TDS.3-1

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что структура всего ОО описана в терминах подсистем.

Оценщик удостоверяется, что все подсистемы ОО идентифицированы. Это «Описание ОО» будет использоваться в качестве исходных данных для шага оценивания ADV_TDS.3-2, где идентифицированы части ОО, которые составляют ФБО. Таким образом, это требование относится ко всему ОО, а не только к ФБО.

ОО (и ФБО) может быть описан на нескольких уровнях детализации (то есть подсистем и модулей). В зависимости от сложности ОО его проект может быть описан в терминах подсистем и модулей, как описано в ИСО/МЭК 15408-3, приложение А.4 ADV_TDS: «Подсистемы и модули». Для очень простого ОО, который может быть описан исключительно на уровне «модуля» (см. ADV_TDS.3-2), этот шаг оценивания не применим, и поэтому считается удовлетворенным.

При выполнении этой деятельности оценщик исследует другие свидетельства, представленные по ОО (например ЗБ, пользовательское руководство оператора), чтобы сделать заключение о том, что «Описание ОО» в таких свидетельствах совместимо с описанием, содержавшимся в проекте ОО.

ИСО/МЭК 15408-3 ADV_TDS.3.2C: *Проект должен содержать описание ФБО на уровне модулей.*

10.8.3.4.2 Шаг оценивания ADV_TDS.3-2

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что все ФБО описаны в терминах модулей.

Оценщик исследует модули на определенные свойства на других шагах оценивания; на этом шаге оценивания оценщик делает заключение о том, что модульное описание касается всего ФБО, а не только части ФБО. При вынесении этого заключения оценщик использует и другие свидетельства (например функциональную спецификацию, описание архитектуры безопасности). Например, если функциональная спецификация содержит интерфейсы функции, которая не описана в явном виде в описании проекта ОО, может возникнуть ситуация, что часть ФБО не была включена в описание достаточным образом. Вынесение этого заключения, вероятно, будет повторяющимся процессом, поскольку чем больший анализ проводится для других свидетельствах, тем больше доверия может быть приобретено относительно полноты документации.

В отличие от подсистем, модули описывают реализацию на уровне детализации, которая может служить руководством по рассмотрению представления реализации. Рекомендуется, чтобы описание модулей было таким, чтобы можно было реализовать модуль по описанию, и полученная реализация будет: 1) идентичной фактической реализации ФБО в терминах интерфейсов, представленных и используемых модулем, и 2) алгоритмически идентичной модулю ФБО. Например, в RFC 793 предоставлено описание верхнего уровня протокола TCP. Это описание обязательно является независимой реализацией. Хотя требуемый уровень детализации обеспечен, это описание проекта не является достаточным, потому что не является определенным для реализации. Фактическая реализация может быть добавлена к протоколу, определенному в RFC, и выбор реализации (например использование глобальных данных относительно локальных данных в различных частях реализации) может оказать влияние на выполненный анализ. В описании проекта модуля TCP должны быть перечислены интерфейсы, предоставленные в реализации (а не просто определенные в RFC 793), а также описание алгоритма обработки, связанного с модулями, осуществляющими TCP (предполагается, что это часть ФБО).

ИСО/МЭК 15408-3 ADV_TDS.3.3C: *В проекте должны быть идентифицированы все подсистемы ФБО.*

10.8.3.4.3 Шаг оценивания ADV_TDS.3-3

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что все подсистемы ФБО идентифицированы.

Если проект представлен исключительно в терминах модулей, то подсистемы в этих требованиях эквивалентны модулям, и деятельность следует выполнить на уровне модуля.

В шаге оценивания ADV_TDS.3-1 были идентифицированы все подсистемы ОО и вынесено заключение о том, что подсистемы, не относящиеся к ФБО, правильно охарактеризованы. Основываясь на этом, подсистемы, которые не характеризовались как не относящиеся к ФБО, следует точно идентифицировать. Оценщик делает заключение о том, что для аппаратного и программного обеспечения, установленного и настроенного согласно руководству в семействе «Подготовительные процедуры» (AGD_PRE), каждая подсистема идентифицирована или как являющаяся частью ФБО или как не являющаяся.

ИСО/МЭК 15408-3 ADV_TDS.3.4C: *В проекте должно приводиться описание каждой из подсистем ФБО.*

10.8.3.4.4 Шаг оценивания ADV_TDS.3-4

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что для каждой подсистемы ФБО описана роль в осуществлении ФТБ, описанных в ЗБ.

Если проект представлен исключительно в терминах модулей, то этот шаг оценивания считается удовлетворенным оценкой, сделанной на последующих шагах оценивания; в этом случае от оценщика не требуется явных действий.

Для достаточно сложных систем, где помимо модульного описания, предоставлено описание уровня подсистем ФБО, цель описания на уровне подсистем состоит в том, чтобы предоставить оценщику контекст для последующего модульного описания. Поэтому оценщик удостоверяется, что описание на уровне подсистем содержит описание того, каким образом ФТБ достигаются в проекте, но на уровне представления выше модульного описания. В этом описании следует рассмотреть механизмы, используемые на уровне, который равен уровню модульных описаний; это предоставит оценщику план действий для разумной оценки информации, содержащейся в описании модуля. Правильно составленный набор описаний подсистемы может помочь оценщику в определении модулей, которые являются самыми важными для анализа, таким образом сфокусировав деятельность оценки на частях ФБО, которые имеют наибольшее значение для осуществления ФТБ.

Оценщик удостоверяется, что описаны все подсистемы ФБО. Описание следует сосредоточить на роли, которую подсистема играет в осуществлении или поддержке реализации выполнения ФТБ и должно быть предоставлено достаточно информации для понимания функций, имеющих значение для выполнения ФТБ.

ИСО/МЭК 15408-3 ADV_TDS.3.5C: *В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.*

10.8.3.4.5 Шаг оценивания ADV_TDS.3-5

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что в нем приведены описания взаимодействий между подсистемами ФБО.

Если проект представлен только в терминах модулей, тогда этот шаг оценивания будет считаться удовлетворенным оцениванием, сделанным во время последующих шагов оценивания. В таком случае от оценщика не требуется никаких явных действий.

По системам, которые достаточно сложные, чтобы предоставлять описание ФБО на уровне подсистем в дополнение к модульному описанию, цель описания взаимодействий между подсистемами состоит в том, чтобы предоставить читателю лучшее понимание того, каким образом ФБО выполняют свои функции. Эти взаимодействия не нужно характеризовать на уровне реализации (например параметры из процедуры в одной подсистеме переходят к процедуре другой подсистемы; глобальные переменные; сигналы аппаратных средств (например прерывания) от подсистемы аппаратных средств до системы обработки прерываний), но элементы данных, идентифицированных для конкретной подсистемы, которые будут использоваться другой подсистемой, следует охватить этим рассмотрением. Любые отношения контроля между подсистемами (например имеется подсистема, ответственная за формирование базовых правил для межсетевого экрана и подсистемы, которая фактически реализует эти правила) также следует включать в описание.

Следует отметить, что, хотя разработчику следует характеризовать все взаимодействия между подсистемами, оценщику нужно использовать свое собственное суждение при оценивании полноты описания. Если причина взаимодействия подсистем не ясна, или если есть относящиеся к выполнению ФТБ взаимодействия (выявленные, например в ходе анализа описания режимов функционирования подсистемы), которые не описаны в явном виде, оценщику следует удостовериться, что эта информация предоставлена разработчиком. Однако, если оценщик может сделать заключение о том, что взаимодействия между конкретным набором подсистем, хотя и не полностью описаны разработчиком, не помогут ни в понимании общих функций, ни в понимании функций безопасности, обеспечиваемых ФБО, тогда оценщик может считать описание достаточным; полнота описания ради самой полноты не преследуется.

ИСО/МЭК 15408-3 ADV_TDS.3.6C: *В проекте должно быть осуществлено прослеживание подсистем ФБО с модулями ФБО.*

10.8.3.4.6 Шаг оценивания ADV_TDS.3-6

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что прослеживание между подсистемами ФБО и модулями ФБО осуществлено в полной мере.

Если проект представлен исключительно в терминах модулей, то этот шаг оценивания считается удовлетворенным.

Для ОО, которые достаточно сложны для описания на уровне подсистем ФБО в дополнение к модульному описанию, разработчик предоставляет простое прослеживание, показывающее, каким образом модули ФБО размещаются по подсистемам. Это предоставит оценщику руководство по вы-

полнению оценки на уровне модулей. Чтобы определить полноту, оценщик исследует каждое прослеживание и делает заключение о том, что все подсистемы прослежены, по крайней мере, к одному модулю, и что все модули прослежены хотя бы к одной подсистеме.

10.8.3.4.7 Шаг оценивания ADV_TDS.3-7

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что прослеживание между подсистемами ФБО и модулями ФБО является точным.

Если проект представлен исключительно в терминах модулей, то этот шаг оценивания считается удовлетворенным.

Для ОО, которые достаточно сложны для предоставления описания на уровне подсистем ФБО в дополнение к модульному описанию, разработчик предоставляет простое прослеживание, показывающее, каким образом модули ФБО размещаются по подсистемам. Это предоставит оценщику руководство по выполнению оценки на уровне модулей. Оценщик может проверить точность прослеживания при выполнении других шагов оценивания. «Неточное» прослеживание — такое, где модуль по ошибке связан с подсистемой, а его функции не используются в пределах подсистемы. Поскольку прослеживание предназначается в качестве руководства для поддержки более подробного анализа, оценщику следует применить соответствующее усилие к этому шагу оценивания. Не следует тратить слишком много усилий на проверку точности прослеживания.

Погрешности, которые приводят к недопониманию проекта и которые раскрываются при выполнении этого или иных шагов оценивания, следует связать с этим шагом оценивания и исправить.

ИСО/МЭК 15408-3 ADV_TDS.3.7C: *В проекте должен быть описан каждый осуществляющий выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.*

10.8.3.4.8 Шаг оценивания ADV_TDS.3-8

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что описание назначения каждого осуществляющего выполнение ФТБ модуля является полным и точным.

Разработчик может определять модули как обеспечивающие выполнение ФТБ, поддерживающие выполнение ФТБ или не влияющие на выполнение ФТБ, но эти «категории» используются только для того, чтобы описать количество и тип информации, которую должен предоставить разработчик, и может использоваться для ограничения количества информации, которую должен предоставить разработчик в том случае, если сам процесс разработки не производит требуемую документацию. Были модули категорированы разработчиком или нет, в обязанности оценщика входит задача вынести заключение о том, что в модули включена соответствующая их роли в ОО (обеспечивающие выполнение ФТБ и т.д.) информация и получить соответствующую информацию от разработчика в случае, если разработчик не предоставил необходимую информацию для конкретного модуля.

В назначении модуля приводится описание, указывающее на выполняемые модулем функции. Следует предостеречь оценщика о следующем. Этот шаг оценивания следует направить на то, чтобы предоставить оценщику понимание функционирования модуля таким образом, чтобы можно было сделать заключение о достаточности реализации выполнения ФТБ, а также для поддержания архитектурного анализа, выполняемого для компонента ADV_ARC. Пока у оценщика есть хорошее понимание функционирования модуля и его взаимодействия с другими модулями и с ОО в целом, оценщику следует считать цель шага оценивания достигнутой и не участвовать в проверке документации разработчика (требуя, например полного алгоритмического описания для очевидного представления реализации).

ИСО/МЭК 15408-3 ADV_TDS.3.8C: *В проекте должен быть описан каждый осуществляющий выполнение ФТБ модуль с точки зрения его относящихся к ФТБ интерфейсов, значений, предоставляемых этими интерфейсами в ответ на запросы, взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей.*

10.8.3.4.9 Шаг оценивания ADV_TDS.3-9

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что описание интерфейсов, представленных каждым осуществляющим выполнение ФТБ модулем, содержит точное и полное описание относящихся к ФТБ интерфейсов, значений, предоставляемых этими интерфейсами в ответ на запросы, взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей.

Относящиеся к ФТБ интерфейсы модуля — это интерфейсы, используемые другими модулями в качестве средства вызова относящихся к ФТБ операций, и для получения исходных или результирующих данных от модуля. Цель спецификации этих интерфейсов состоит в том, чтобы сделать заключение об их осуществлении во время тестирования. Межмодульные интерфейсы, которые не связаны с ФТБ, не должны определяться и описываться, так как они не рассматриваются в тестировании. Также и другие внутренние интерфейсы, которые не рассматриваются при пересечении связанных с ФТБ пу-

тей выполнения (например фиксированных внутренних путей) не должны определяться и описываться, так как они не рассматриваются в тестировании.

Относящиеся к ФТБ интерфейсы описываются в терминах того, как они вызываются, и какие значения возвращают. Это описание включает перечень связанных с ФТБ параметров и описание этих параметров. Следует отметить, что глобальные данные также считаются параметрами, если используются модулем (или как исходные, или как данные на выходе) при вызове. Если у параметра есть ряд значений (например параметр «флажок»), то определяется полный комплект значений параметра, который будет влиять на обработку модуля. Также и параметры, представляющие структуры данных, описываются таким образом, чтобы каждая область структуры данных была идентифицирована и описана. Следует отметить, что в различных языках программирования могут быть дополнительные «интерфейсы», которые были бы неявными, например оператор/функция перезагрузки в C++. Этот «неявный интерфейс» в описании класса должен быть также описан как часть проекта ОО нижнего уровня. Следует отметить, что хотя модуль может представлять только один интерфейс, чаще всего он представляет собой набор связанных интерфейсов.

В терминах оценки параметров (на входе и выходе) модуля нужно также рассмотреть любое использование глобальных данных. Модуль «использует» глобальные данные, если он читает или записывает данные. Для того, чтобы удостовериться, что описание таких параметров (если оно используется), выполнено полно, оценщик использует иную информацию, предоставленную о модуле в проекте ОО (интерфейсы, алгоритмическое описание и т. д.), а также описание особого набора глобальных данных, оцениваемого в шаге оценивания ADV_TDS.3-9. Например, оценщик может сначала сделать заключение об обработке модуля, исследуя его функцию и представленные интерфейсы (особенно параметры интерфейсов). Тогда он может проверить, «касается» ли обработка какой-либо из глобальных областей данных, идентифицированных в проекте ОО. Затем оценщик делает заключение о том, что для каждой глобальной области данных, которая «затронута», глобальная область данных описана как исходные данные или данные на выходе исследуемого оценщиком модуля.

Запрос — описание программно-справочного типа, которое можно использовать, чтобы правильно вызвать интерфейс модуля при написании программы для использования функций модуля через данный интерфейс. Это включает необходимые данные на входе и выходе, включая любую настройку глобальных переменных.

Значения, возвращаемые через интерфейс, относятся к значениям, которые передаются через параметры или сообщения; значениям, которые сам вызов функции возвращает в стиле «C» вызова функции программы; значениям, которые прошли через глобальные средства (такие как определенные ошибочные процедуры в *ix-подобных операционных системах).

Чтобы удостовериться в полноте описания, оценщик исследует другую доступную информацию (например функциональную спецификацию, описание архитектуры безопасности, представление реализации), чтобы удостовериться, что все данные, необходимые для того, чтобы выполнить функции модуля, предоставлены модулю, и что любые значения, которые необходимы другим модулям от оцениваемого модуля, идентифицированы как возвращаемые модулем. Оценщик определяет точность описания, удостоверяясь, что описание обработки соответствует информации, обозначенной как получаемой или передаваемой от интерфейса.

Поскольку модули на таком низком уровне, может быть трудно определить воздействие полноты и точности на основании анализа другой документации, такой как руководство пользователя по эксплуатации, функциональная спецификация, внутренняя структура ФБО или «Описание архитектуры безопасности». Однако оценщик использует информацию этих документов по мере возможности, чтобы удостовериться в точности и полноте описания назначения. Такому анализу может помочь анализ, выполняемый для шагов оценивания элемента ADV_TDS.3.10C, при котором прослеживаются ИФБО в функциональной спецификации к модулям ФБО.

ИСО/МЭК 15408-3 ADV_TDS.3.9C: *В проекте должен быть описан каждый поддерживающий и не влияющий на выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.*

10.8.3.4.10 Шаг оценивания ADV_TDS.3-10

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что поддерживающие выполнение ФТБ и не влияющие на выполнение ФТБ модули правильно категорированы.

В случаях, когда разработчик обеспечил различное количество информации для различных модулей, была сделана неявная классификация. Таким образом, модули (например) с детализацией, представленной на связанных с ФТБ интерфейсах (см. ADV_TDS.3.10C), являются модулями-кандидатами

на категорию осуществляющих выполнение ФТБ, хотя проведенный оценщиком анализ может привести к заключению, что некоторые из них — поддерживающие или не влияющие на выполнение ФТБ. Те, для которых приводится только описание назначения и взаимодействия с другими модулями, например «неявно категорируются» как поддерживающие или не влияющие на выполнение ФТБ.

В этих случаях усилия оценщика направлены на попытку сделать заключение на основе свидетельств, предусмотренных для каждого модуля, неявно категорированного как поддерживающий или не влияющий на выполнение ФТБ, и информации об оценке других модулей (в проекте ОО, функциональной спецификации, описании архитектуры безопасности и руководстве пользователя по эксплуатации), является ли модуль действительно поддерживающим или не влияющим на выполнение ФТБ. На этом уровне доверия может быть допущена некоторая ошибка; оценщик не обязан быть абсолютно уверен, что данный модуль — поддерживающий или не влияющий на выполнение ФТБ, даже если он маркирован как таковой. Однако, если предоставленные свидетельства указывают, что поддерживающие или не влияющие на выполнение ФТБ модули являются на самом деле осуществляющими выполнение ФТБ, оценщик запрашивает дополнительную информацию от разработчика, чтобы сделать заключение о явной несогласованности. Например, предположим, что в документации для Модуля А (который является осуществляющим выполнение ФТБ) указано, что он вызывает Модуль В для проверки доступа некой конструкции. Когда оценщик исследует информацию, связанную с Модулем В, он обнаруживает, что разработчик предоставил только назначение и ряд взаимодействий (таким образом неявно категорируя Модуль В как поддерживающий или не влияющий на выполнение ФТБ). При исследовании назначения и взаимодействий Модуля А оценщик не находит упоминания о Модуле В, выполняющем проверку доступа, а Модуль А не отмечен как модуль, с которым взаимодействует Модуль В. В этом пункте оценщику следует обратиться к разработчику, чтобы сделать заключение о несоответствии между информацией, предоставленной в Модуле А и в Модуле В.

Другой пример, когда оценщик исследует прослеживание ИФБО к модулям в соответствии с ADV_ TDS.3.2D. Этот анализ показывает, что Модуль С связан с требуемой по ФТБ идентификацией пользователя. Опять же, когда оценщик исследует информацию, связанную с Модулем С, он обнаруживает, что разработчик предоставил только назначение и ряд взаимодействий (таким образом неявно категорируя Модуль С как поддерживающий или не влияющий на выполнение ФТБ). Исследуя назначение и ряд Модуля С, оценщик не способен определить, почему Модуль С, перечисленный в прослеживании к ИФБО, касающемуся пользовательской идентификации, не классифицирован как осуществляющий выполнение требований ФТБ. И в этом случае оценщику следует обратиться к разработчику для того, чтобы сделать заключение о том, что это несоответствие.

Последний пример касается обратного случая. Допустим, разработчик предоставил информацию, связанную с Модулем D, по назначению и ряду взаимодействий (таким образом неявно категорируя Модуль В как поддерживающий или не влияющий на выполнение ФТБ). Оценщик исследует все свидетельства, включая назначение и взаимодействия для Модуля D. В назначении дается значимое описание функции Модуля D в ОО; взаимодействия совместимы с этим описанием, и нет ничего, указывающего на возможную принадлежность Модуля D к осуществляющим выполнение ФТБ. В этом случае оценщику не следует требовать дополнительную информацию о Модуле D «просто для уверенности», что он правильно категорирован. Разработчик выполнил свои обязательства, и приобретенного оценщиком доверия от неявной классификации Модуля D (по определению) достаточно для этого уровня доверия.

10.8.3.4.11 Шаг оценивания ADV_TDS.3-11

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что описание назначения каждого поддерживающего или не влияющего на выполнение ФТБ модуля выполнено полно и точно.

Описание назначения модуля указывает на то, какие функции выполняет модуль. Из описания оценщику следует быть в состоянии получить общее представление о роли модуля. Чтобы удостовериться, что описание достаточно полно, оценщик использует информацию, предоставленную о взаимодействиях модуля с другими модулями для оценки совместимости причин вызовов модуля с назначением модуля. Если описание взаимодействия содержит функции, которые не очевидны из назначения модуля или являются конфликтующими с ним, оценщик должен сделать заключение, является ли это несоответствие проблемой точности или полноты описания. Оценщику следует с подозрением относиться к слишком коротким описаниям назначения, так как значимый анализ, основанный на назначении только с одним предложением, вероятно, будет провести невозможно.

В этих случаях усилия оценщика направлены на попытку сделать заключение на основе свидетельств, предусмотренных для каждого модуля, неявно категорированного как поддерживающий

или не влияющий на выполнение ФТБ, и информации об оценке других модулей (в проекте ОО, функциональной спецификации, описании архитектуры безопасности и руководстве пользователя по эксплуатации), является ли модуль действительно поддерживающим или не влияющим на выполнение ФТБ. На этом уровне доверия может быть допущена некоторая ошибка; оценщик не обязан быть абсолютно уверен, что данный модуль — поддерживающий или не влияющий на выполнение ФТБ, даже если он маркирован как таковой. Однако, если предоставленные свидетельства указывают, что поддерживающие или не влияющие на выполнение ФТБ модули являются на самом деле осуществляющими выполнение ФТБ, оценщик запрашивает дополнительную информацию от разработчика, чтобы сделать заключение о явной несогласованности. Например, предположим, что в документации для Модуля А (который является осуществляющим выполнение ФТБ) указано, что он вызывает Модуль В для проверки доступа некой конструкции. Когда оценщик исследует информацию, связанную с Модулем В, он обнаруживает, что разработчик предоставил только назначение и ряд взаимодействий (таким образом неявно категорируя Модуль В как поддерживающий или не влияющий на выполнение ФТБ). При исследовании назначения и взаимодействий Модуля А оценщик не находит упоминания о Модуле В, выполняющем проверку доступа, а Модуль А не отмечен как модуль, с которым взаимодействует Модуль В. Оценщику следует обратиться к разработчику, чтобы сделать заключение о несоответствии между информацией, предоставленной в Модуле А и Модуле В.

10.8.3.4.12 Шаг оценивания ADV_TDS.3-12

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что описание взаимодействия каждого поддерживающего или не влияющего на выполнение ФТБ модуля с другими модулями является полным и точным.

Важно отметить, что в терминах требований ИСО/МЭК 15408-3 и этого шага оценивания термин *взаимодействие* является менее строгим, чем *интерфейс*. Взаимодействие не обязательно должно быть характеризовано на уровне реализации (например параметры из одной процедуры в одной подсистеме переходят к процедуре другой подсистемы; глобальные переменные; сигналы аппаратных средств (например прерывания) от подсистемы аппаратных средств до системы обработки прерываний), но элементы данных, идентифицированных для конкретного модуля, которые будут использоваться другим модулем, следует охватить этим рассмотрением. Любые отношения контроля между подсистемами (например имеется подсистема, ответственная за формирование базовых правил для межсетевого экрана и подсистемы, которая фактически реализует эти правила) также следует включать в описание.

Поскольку модули на таком низком уровне, может быть трудно определить воздействие полноты и точности на основании анализа другой документации, такой как руководство пользователя по эксплуатации, функциональная спецификация, внутренняя структура ФБО или «Описание архитектуры безопасности». Однако оценщик использует информацию этих документов по мере возможности, чтобы удостовериться в точности и полноте описания функций. Такому анализу может помочь анализ, выполняемый для шагов оценивания элемента ADV_TDS.3.10C, при котором прослеживаются ИФБО в функциональной спецификации к модулям ФБО.

Взаимодействие модуля с другими модулями рассматривается вне документа, где зафиксировано дерево вызовов. Взаимодействие описывается с функциональной точки зрения и касается того, почему данный модуль взаимодействует с другими модулями. В назначении модуля описывается, какие функции модуль предоставляет другим модулям; во взаимодействиях следует описать, от каких модулей зависит данный модуль для выполнения своих функций.

Поскольку модули на таком низком уровне, может быть трудно определить воздействие полноты и точности на основании анализа другой документации, такой как руководство пользователя по эксплуатации, функциональная спецификация, внутренняя структура ФБО или «Описание архитектуры безопасности». Однако оценщик использует информацию этих документов по мере возможности, чтобы удостовериться в точности и полноте описания взаимодействий.

ИСО/МЭК 15408-3 ADV_TDS.3.10C: *В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.*

10.8.3.4.13 Шаг оценивания ADV_TDS.3-13

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что он содержит полное и точное прослеживание от ИФБО, описанных в функциональной спецификации, к модулям ФБО, описанным в проекте ОО.

Описание модулей в проекте ОО предоставляет описание того, каким образом ФБО реализуются. ИФБО обеспечивает описание того, каким образом осуществляется реализация. Свидетельства от разработчика идентифицируют модуль, который вовлечен в процесс запроса операции от ИФБО,

и идентифицируют цепочку модулей, которые прежде всего отвечают за реализацию функций. Однако для данного шага оценивания не требуется предоставить полное «дерево вызовов» для каждого ИФБО. Случаи, в которых требуется идентифицировать больше одного модуля, это модули «точки входа» или модули адаптера интерфейса, единственные функции которых — приведение исходных данных к требуемым условиям и демультиплексирование исходных данных. Прослеживание к этим модулям не дало бы оценщику никакой полезной информации.

Оценщик оценивает полноту прослеживания, удостоверяясь, что каждый ИФБО прослежен по крайней мере к одной подсистеме. Проверка точности более сложна.

Поскольку модули на таком низком уровне, может быть трудно определить воздействие полноты и точности на основании анализа другой документации, такой как руководство пользователя по эксплуатации, функциональная спецификация, внутренняя структура ФБО или «Описание архитектуры безопасности». Однако оценщик использует информацию этих документов по мере возможности, чтобы удостовериться в точности и полноте описания взаимодействий.

10.8.3.5 Действие ADV_TDS.3.2E

10.8.3.5.1 Шаг оценивания ADV_TDS.3-14

Оценщик должен исследовать ФТБ ОО и проект ОО, чтобы сделать заключение о том, что все ФТБ в ЗБ охвачены в проекте ОО.

Оценщик может провести прослеживание между ФТБ для ОО и проектом ОО. Это прослеживание, вероятно, будет проводиться от функционального требования до ряда подсистем и далее до модулей. Следует отметить, что это прослеживание, вероятно, будет по уровню детализации ниже, чем для компонента или даже для элемента требований, из-за операций (назначения, уточнения, выбора), которые выполняются над функциональным требованием автором ЗБ.

Например, компонент FDP_ACC.1 «Ограниченное управление доступом» содержит элемент с операцией назначения. Если бы в ЗБ содержалось, например десять правил в назначении для данного компонента FDP_ACC.1, и эти правила применялись бы в определенных местах в пределах пятнадцати модулей, то для оценщика некорректно было бы проследить компонент FDP_ACC.1 к одной подсистеме и утверждать о завершении шага оценивания. Вместо этого оценщик должен проследить первое правило компонента FDP_ACC.1 к подсистеме A и режимам функционирования x, y и z; второе правило компонента FDP_ACC.1 к подсистеме A и режимам функционирования x, p и q; и т. д.

10.8.3.5.2 Шаг оценивания ADV_TDS.3-15

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что в нем точно представлены все ФТБ.

Оценщик может провести прослеживание между ФТБ для ОО и проектом ОО. Это прослеживание, вероятно, будет проводиться от функционального требования до ряда подсистем. Следует отметить, что это прослеживание, вероятно, будет по уровню детализации ниже, чем для компонента или даже для элемента требований, из-за операций (назначения, уточнения, выбора), которые выполняются над функциональным требованием автором ЗБ.

Например, если требования в ЗБ определяют основанный на ролевой модели механизм управления доступом, оценщик сначала идентифицирует подсистемы, которые способствуют реализации этого механизма. Это может быть сделано с применением углубленного изучения или с применением понимания проекта ОО или работ, полученного в предыдущих шагах оценивания. Следует отметить, что это прослеживание необходимо только для идентификации подсистем и не является полным анализом.

Следующий шаг — понять, какой из механизмов подсистем и модулей осуществляется. Например, если в проекте описывается реализация управления доступом, основанная на битах защиты UNIX, то проект не является точным отражением требований по управлению доступом в ЗБ для того примера, который использовался выше. Если оценщик не может сделать заключение о том, что механизм был реализован точным образом из-за недостаточной детализации предоставленной ему информации, то ему нужно будет оценить, были ли все осуществляющие выполнение ФТБ подсистемы идентифицированы и был ли предоставлен для этих подсистем достаточный уровень детализации.

10.8.4 Подвид деятельности по оценке (ADV_TDS.4)

10.8.4.1 Цели

Цель этого подвида деятельности состоит в том, чтобы определить, обеспечено ли в проекте ОО описание ОО в терминах подсистем, достаточное для определения границ ФБО, и обеспечено ли описание внутренней структуры ФБО в терминах модулей (и, опционально, представлений верхнего уровня). Оценщику предоставляется подробное описание осуществляющих и поддерживающих выпол-

нение ФТБ модулей и достаточный объем информации о не влияющих на выполнение ФТБ модулей, чтобы сделать заключение о том, что ФТБ полно и точно осуществлены; как таковой, проект ОО предоставляет объяснение представления реализации.

10.8.4.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) описание архитектуры безопасности;

d) проект ОО.

10.8.4.3 Замечания по применению

Есть три типа деятельности, которую оценщик должен предпринять относительно проекта ОО. Во-первых, оценщик делает заключение о том, что границы ФБО описаны достаточным образом. Во-вторых, оценщик делает заключение о том, что разработчик предоставил документацию, которая соответствует содержанию и требованиям представления для этой подсистемы, и эта документация совместима с другой документацией, предусмотренной для ОО. Наконец, оценщик должен проанализировать информацию о проекте, включая описания осуществляющих выполнение ФТБ модулей (подробно) и поддерживающих и не влияющих на выполнение ФТБ (менее подробно) для того, чтобы понять, каким образом реализована система, и с этим пониманием удостовериться, что ИФБО в функциональной спецификации описан достаточным образом и что тестовая информация в достаточной мере тестирует ФБО (проводится в шагах оценивания класса ATE).

10.8.4.4 Действие ADV_TDS.4.1E

ИСО/МЭК 15408-3 ADV_TDS.4.1C: *В проекте должно приводиться описание структуры ОО на уровне подсистем.*

10.8.4.4.1 Шаг оценивания ADV_TDS.4-1

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что структура всего ОО описана в терминах подсистем.

Оценщик удостоверяется, что все подсистемы ОО идентифицированы. Это «Описание ОО» будет использоваться в качестве исходных данных для шага оценивания ADV_TDS.4-5, где идентифицированы части ОО, которые составляют ФБО. Таким образом, это требование относится ко всему ОО, а не только к ФБО.

ОО (и ФБО) может быть описан на нескольких уровнях детализации (то есть подсистем и модулей). В зависимости от сложности ОО его проект может быть описан в терминах подсистем и модулей, как описано в ИСО/МЭК 15408-3, приложение А.4 ADV_TDS: «Подсистемы и модули». Для очень простого ОО, который может быть описан исключительно на уровне «модуля» (см. ADV_TDS.4-3), этот шаг оценивания не применим и поэтому считается удовлетворенным.

При выполнении этой деятельности оценщик исследует другие свидетельства, представленные ОО (например ЗБ, пользовательское руководство оператора), чтобы сделать заключение о том, что «Описание ОО» в таких свидетельствах совместимо с описанием, содержавшимся в проекте ОО.

10.8.4.4.2 Шаг оценивания ADV_TDS.4-2

Оценщик должен исследовать проектную документацию, чтобы сделать заключение о том, что полуформальную запись, используемую для описания подсистем, модулей и их интерфейсов, определяют или на нее ссылаются.

Полуформальная запись может быть определена или спонсором, или ссылкой на соответствующий стандарт. Оценщику следует предоставить прослеживание функций безопасности и их интерфейсов, уделяя особое внимание тому, какая часть документации функции или интерфейса полуформально описана и какая запись для этого используется. Оценщик исследует все использованные полуформальные записи, чтобы удостовериться, что они написаны в полуформальном стиле, а также чтобы обосновать уместность способа, которым полуформальные записи используются для ОО.

Оценщику следует помнить, что полуформальное изложение характеризуется стандартизированным форматом с четким синтаксисом, который уменьшает степень двусмысленности, возможной при неформальном изложении. Синтаксис всех полуформальных записей, используемых в функциональной спецификации, должен быть определен или должен сопровождаться ссылкой на соответствующий стандарт. Оценщик проверяет, что полуформальные записи, используемые для отражения функциональной спецификации, способны отражать особенности, относящиеся к безопасности. Чтобы определить это, оценщик может обратиться к ФТБ и сравнить заявленные в ЗБ механизмы безопасности ФБО и описанные в функциональной спецификации с использованием полуформальных записей.

ИСО/МЭК 15408-3 ADV_TDS.4.2C: *В проекте должно приводиться описание структуры ОО на уровне модулей, с присвоением каждому модулю категории либо осуществляющего выполнение ФТБ, либо поддерживающего, либо не влияющего на выполнение ФТБ.*

10.8.4.4.3 Шаг оценивания ADV_TDS.4-3

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что весь ФБО описан в терминах модулей.

Оценщик исследует модули на определенные свойства на других шагах оценивания; на этом шаге оценивания оценщик делает заключение о том, что модульное описание касается всего ФБО, а не только части ФБО. При вынесении этого заключения оценщик использует и другие свидетельства (например функциональную спецификацию, описание архитектуры безопасности). Например, если функциональная спецификация содержит интерфейсы функции, которая не описана в явном виде в описании проекта ОО, может возникнуть ситуация, что часть ФБО не была включена в описание достаточным образом. Внесение этого заключения, вероятно, будет повторяющимся процессом, поскольку чем больше анализа проводится на других свидетельствах, тем больше доверия может быть приобретено относительно полноты документации.

В отличие от подсистем, модули описывают реализацию на уровне детализации, которая может служить руководством по рассмотрению представления реализации. Рекомендуется, чтобы описание модулей было таким, чтобы можно было реализовать модуль по описанию, и полученная реализация будет: 1) идентичной фактической реализации ФБО в терминах интерфейсов, представленных и используемых модулем, и 2) алгоритмически идентичной модулю ФБО. Например, в RFC 793 предоставлено описание верхнего уровня протокола TCP. Это обязательно независимая реализация. В то время как обеспечен уровень детализации, это описание проекта не является достаточным, потому что не является определенным для реализации. Фактическая реализация может быть добавлена к протоколу, определенному в RFC, и выбор реализации (например использование глобальных данных относительно локальных данных в различных частях реализации) может оказать влияние на выполненный анализ. В описании проекта модуля TCP должны быть перечислены интерфейсы, предоставленные в реализации (а не просто определенные в RFC 793), а также описание алгоритма обработки, связанного с модулями, осуществляющими TCP (предполагается, что это часть ФБО).

10.8.4.4.4 Шаг оценивания ADV_TDS.4-4

Оценщик должен проверить проект ОО, чтобы сделать заключение о том, что модули ФБО идентифицированы или как осуществляющие выполнение ФТБ, или как не влияющие на выполнение ФТБ.

Цель определения каждого модуля (согласно роли, которую каждый конкретный модуль играет в осуществлении ФТБ) состоит в том, чтобы позволить разработчикам предоставлять меньше информации о тех частях ФБО, которые играют незначительную роль в обеспечении безопасности. Разработчик всегда может предоставить больше информации или с большей степенью детализации, чем требуется. Чаще всего это может произойти, когда информация была собрана вне контекста оценки. В таких случаях разработчик должен все равно определять модули или как осуществляющие выполнение ФТБ, или как не влияющие на выполнение ФТБ.

Точность этих обозначений постоянно рассматривается на протяжении оценивания. Проблемный вопрос — неправильное обозначение модулей как менее важных (и следовательно, предоставление меньшего объема информации), чем они являются в действительности. В то время как явные неправильные обозначения могут быть очевидными (например определение модуля аутентификации не как осуществляющего выполнение ФТБ, притом что «Идентификация пользователей» (FIA_UID) включена в состав ФТБ), другие неправильные обозначения не могут быть обнаружены, пока не получено лучшее понимание ФБО. Оценщик поэтому должен учитывать, что эти обозначения — начальное максимальное усилие разработчика, которое в дальнейшем может подвергаться изменениям. Дальнейшее руководство предоставлено в шаге оценивания ADV_TDS.4-16, в котором исследуется точность этих обозначений.

ИСО/МЭК 15408-3 ADV_TDS.4.3C: *В проекте должны быть идентифицированы все подсистемы ФБО.*

10.8.4.4.5 Шаг оценивания ADV_TDS.4-5

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что все подсистемы ФБО идентифицированы.

Если проект представлен исключительно в терминах модулей, то подсистемы в этих требованиях эквивалентны модулям, и деятельность следует выполнить на уровне модуля.

В шаге оценивания ADV_TDS.4-1 были идентифицированы все подсистемы ОО, и вынесено заключение о том, что подсистемы, не относящиеся к ФБО, правильно охарактеризованы. Основываясь

на этом, подсистемы, которые не характеризовались как не относящиеся к ФБО, следует точно идентифицировать. Оценщик делает заключение о том, что для аппаратного и программного обеспечения, установленного и настроенного согласно руководству в семействе «Подготовительные процедуры» (AGD_PRE), каждая подсистема идентифицирована или как являющаяся частью ФБО или как не являющаяся.

ИСО/МЭК 15408-3 ADV_TDS.4.4C: *В проекте должно приводиться полуформальное описание каждой из подсистем ФБО, сопровождающееся вспомогательным пояснительным неформальным текстом, если это представляется целесообразным.*

10.8.4.4.6 Шаг оценивания ADV_TDS.4-6

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что для каждой подсистемы ФБО описана роль в осуществлении ФТБ, описанных в ЗБ.

Если проект представлен исключительно в терминах модулей, то этот шаг оценивания считается удовлетворенным оценкой, сделанной на последующих шагах оценивания; в этом случае от оценщика не требуется явных действий.

Для достаточно сложных систем, где помимо модульного описания, предоставлено описание уровня подсистем ФБО, цель описания на уровне подсистем состоит в том, чтобы предоставить оценщику контекст для последующего модульного описания. Поэтому оценщик удостоверяется, что описание на уровне подсистем содержит описание того, каким образом ФТБ достигаются в проекте, но на уровне представления выше модульного описания. В этом описании следует рассмотреть механизмы, используемые на уровне, который равен уровню модульных описаний; это предоставит оценщику план действий для разумной оценки информации, содержащейся в описании модуля. Хорошо составленный набор описаний подсистемы может помочь оценщику в определении модулей, которые являются самыми важными для анализа, таким образом сфокусировав деятельность оценки на частях ФБО, которые имеют наибольшее значение для осуществления ФТБ.

Оценщик удостоверяется, что описаны все подсистемы ФБО. Хотя описание следует сосредоточить на роли, которую подсистема играет в осуществлении или поддержке реализации выполнения ФТБ, должно быть предоставлено достаточно информации для понимания функций, имеющих значение для выполнения ФТБ.

ИСО/МЭК 15408-3 ADV_TDS.4.5C: *В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.*

10.8.4.4.7 Шаг оценивания ADV_TDS.4-7

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что в нем приведены описания взаимодействия между подсистемами ФБО.

Если проект представлен исключительно в терминах модулей, то этот шаг оценивания считается удовлетворенным оценкой, сделанной на последующих шагах оценивания; в этом случае от оценщика не требуется явных действий.

Для достаточно сложных систем, где помимо модульного описания, предоставлено описание уровня подсистем ФБО, цель описания взаимодействий между осуществляющими выполнение ФТБ подсистемами и другими подсистемами состоит в том, чтобы предоставить читателю лучшее понимание того, каким образом ФБО выполняют свои функции. Эти взаимодействия не должны быть характеризованы на уровне реализации (например параметры из одной процедуры в одной подсистеме переходят к процедуре другой подсистемы; глобальные переменные; сигналы аппаратных средств (например прерывания) от подсистемы аппаратных средств до системы обработки прерываний), но элементы данных, идентифицированных для конкретной подсистемы, которые будут использоваться другой подсистемой, должны быть охвачены этим рассмотрением. Любые отношения контроля между подсистемами (например имеется подсистема, ответственная за формирование базовых правил для межсетевого экрана и подсистемы, которая фактически реализует эти правила) также следует включать в описание.

Следует отметить, что, хотя разработчику следует охарактеризовать все взаимодействия между подсистемами, оценщик должен использовать свое собственное суждение при оценивании полноты описания. Если причина взаимодействия подсистем неясна или если есть относящиеся к выполнению ФТБ взаимодействия (выявленные, например в ходе анализа описания режимов функционирования подсистемы), которые не описаны в явном виде, оценщику следует удостовериться, что эта информация предоставлена разработчиком. Однако, если оценщик может сделать заключение о том, что взаимодействия между конкретным набором подсистем хотя и не полностью описаны разработчиком, не помогут ни в понимании общих функций, ни в понимании функций безопасности, обеспеченных ФБО, тогда оценщик может считать описание достаточным; полнота описания ради самой полноты не преследуется.

ИСО/МЭК 15408-3 ADV_TDS.4.6C: *В проекте должно быть осуществлено прослеживание подсистем ФБО с модулями ФБО.*

10.8.4.4.8 Шаг оценивания ADV_TDS.4-8

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что прослеживание между подсистемами ФБО и модулями ФБО осуществлено в полной мере.

Если проект представлен исключительно в терминах модулей, то этот шаг оценивания считается удовлетворенным.

Для ОО, которые достаточно сложны для предоставления описания на уровне подсистем ФБО в дополнение к модульному описанию, разработчик предоставляет простое прослеживание, показывающее, каким образом модули ФБО размещаются по подсистемам. Это предоставит оценщику руководство по выполнению оценки на уровне модулей. Чтобы сделать заключение о полноте, оценщик исследует каждое прослеживание и делает заключение о том, что все подсистемы прослежены по крайней мере к одному модулю, и что все модули прослежены хотя бы к одной подсистеме.

10.8.4.4.9 Шаг оценивания ADV_TDS.4-9

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что прослеживание между подсистемами ФБО и модулями ФБО является точным.

Если проект представлен исключительно в терминах модулей, то этот шаг оценивания считается удовлетворенным.

Для ОО, которые достаточно сложны для предоставления описания на уровне подсистем ФБО в дополнение к модульному описанию, разработчик предоставляет простое прослеживание, показывающее, каким образом модули ФБО размещаются по подсистемам. Это предоставит оценщику руководство по выполнению оценки на уровне модулей. Оценщик может проверить точность прослеживания при выполнении других шагов оценивания. «Неточное» прослеживание — такое, где модуль по ошибке связан с подсистемой, а его функции не используются в пределах подсистемы. Поскольку прослеживание предназначается в качестве руководства для поддержки более подробного анализа, оценщику следует применить соответствующее усилие к этому шагу оценивания. Не следует тратить слишком много усилий на проверку точности прослеживания. Погрешности, которые приводят к недопониманию по проекту, которые раскрываются при выполнении этого или иных шагов оценивания, следует связать с этим шагом оценивания и исправить.

ИСО/МЭК 15408-3 ADV_TDS.4.7C: *В проекте должен быть описан каждый осуществляющий и поддерживающий выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.*

10.8.4.4.10 Шаг оценивания ADV_TDS.4-10

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что описание назначения каждого осуществляющего и поддерживающего выполнение ФТБ модуля является полным и точным.

Разработчик может определять модули как обеспечивающие выполнение ФТБ, поддерживающие выполнение ФТБ или не влияющие на выполнение ФТБ, но эти «категории» используются только для того, чтобы описать количество и тип информации, которую должен предоставить разработчик, и может использоваться для ограничения количества информации, которую должен предоставить разработчик в том случае, если сам процесс разработки не производит требуемую документацию. Были модули категорированы разработчиком или нет, в обязанности оценщика входит вынести заключение о том, что в модули включена соответствующая их роли в ОО (обеспечивающие выполнение ФТБ и т. д.) информация и получить соответствующую информацию от разработчика в случае, если разработчик не предоставил необходимую информацию для конкретного модуля.

В назначении модуля приводится описание, указывающее на выполняемые модулем функции. Следует предостеречь оценщика о следующем. Этот шаг оценивания следует направить на то, чтобы предоставить оценщику понимание функционирования модуля таким образом, чтобы можно было сделать заключение о достаточности реализации выполнения ФТБ, а также для поддержания архитектурного анализа, выполняемого для компонента ADV_ARC. Пока у оценщика есть хорошее понимание функционирования модуля и его взаимодействия с другими модулями и с ОО в целом, оценщику следует считать цель шага оценивания достигнутой и не участвовать в проверке документации разработчика (требуя, например полного алгоритмического описания для очевидного представления реализации).

ИСО/МЭК 15408-3 ADV_TDS.4.8C: *В проекте должен быть описан каждый осуществляющий и поддерживающий выполнение ФТБ модуль с точки зрения относящихся к ФТБ интерфейсов, значений, предоставляемых этими интерфейсами в ответ на запросы, взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей.*

10.8.4.4.11 Шаг оценивания ADV_TDS.4-11

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что описание интерфейсов, представленных каждым осуществляющим и поддерживающим выполнение ФТБ модулем, содержит точное и полное описание относящихся к ФТБ интерфейсов, значений, предоставляемых этими интерфейсами в ответ на запросы, взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей.

Относящиеся к ФТБ интерфейсы модуля — это интерфейсы, используемые другими модулями в качестве средства вызова относящихся к ФТБ операций, и для получения исходных или результирующих данных от модуля. Цель спецификации этих интерфейсов состоит в том, чтобы сделать заключение об их осуществлении во время тестирования. Межмодульные интерфейсы, которые не связаны с ФТБ, не должны определяться и описываться, так как они не рассматриваются в тестировании. Также и другие внутренние интерфейсы, которые не рассматриваются при пересечении связанных с ФТБ путей выполнения (например фиксированных внутренних путей), не должны определяться и описываться, так как они не рассматриваются в тестировании.

Относящиеся к ФТБ интерфейсы описываются в терминах того, как они вызываются и какие значения возвращают. Это описание включает перечень связанных с ФТБ параметров и описание этих параметров. Следует отметить, что глобальные данные также считаются параметрами, если используются модулем (или как исходные или как данные на выходе) при вызове. Если у параметра есть ряд значений (например параметр «флажок»), то определяется полный комплект значений параметра, который будет влиять на обработку модуля. Также и параметры, представляющие структуры данных, описываются таким образом, чтобы каждая область структуры данных была идентифицирована и описана. Следует отметить, что в различных языках программирования могут быть дополнительные «интерфейсы», которые были бы неявными; например оператор/функция перезагрузки в C++. Этот «неявный интерфейс» в описании класса должен быть также описан как часть проекта ОО нижнего уровня. Следует отметить, что, хотя модуль может представлять только один интерфейс, чаще всего он представляет собой набор связанных интерфейсов.

В терминах оценки параметров (на входе и выходе) модуля нужно также рассмотреть любое использование глобальных данных. Модуль «использует» глобальные данные, если он читает или записывает данные. Чтобы удостовериться, что описание таких параметров (если оно используется) выполнено полно, оценщик использует иную информацию, предоставленную о модуле в проекте ОО (интерфейсы, алгоритмическое описание, и т. д.), а также описание особого набора глобальных данных, оцениваемого в шаге оценивания ADV_TDS.4-10. Например, оценщик может сначала сделать заключение об обработке модуля, исследуя его функцию и представленные интерфейсы (особенно параметры интерфейсов). Тогда он может проверить, «касается» ли обработка какой-либо из глобальных областей данных, идентифицированных в проекте ОО. Затем оценщик делает заключение о том, что для каждой глобальной области данных, которая «затронута», глобальная область данных описана как исходные данные или данные на выходе исследуемого оценщиком модуля.

Запросы — описание программно-справочного типа, которое можно использовать, чтобы правильно вызвать интерфейс модуля при написании программы для использования функций модуля через данный интерфейс. Это включает необходимые данные на входе и выходе, включая любую настройку глобальных переменных.

Значения, возвращаемые через интерфейс, относятся к значениям, которые передаются через параметры или сообщения; значениям, которые сам вызов функции возвращает в стиле «С» вызова функции программы; значениям, которые прошли через глобальные средства (такие как определенные ошибочные процедуры в *ix-подобных операционных системах).

Чтобы удостовериться в полноте описания, оценщик исследует другую доступную информацию (например функциональную спецификацию, описание архитектуры безопасности, представление реализации), чтобы удостовериться, что все данные, необходимые для того, чтобы выполнить функции модуля, предоставлены модулю, и что любые значения, которые необходимы другим модулям от оцениваемого модуля, идентифицированы как возвращаемые модулем. Оценщик определяет точность описания, удостоверяясь, что описание обработки соответствует информации, обозначенной как получаемая или передаваемая от интерфейса.

Поскольку модули на таком низком уровне, то может быть трудно сделать заключение о воздействии на полноту и точность на основании анализа другой документации, такой как руководство пользователя по эксплуатации, функциональная спецификация, внутренняя структура ФБО или «Описание архитектуры безопасности». Однако оценщик использует информацию этих документов по мере воз-

можности, чтобы удостовериться в точности и полноте описания назначения. Такому анализу может помочь анализ, выполняемый для шагов оценивания элемента ADV_TDS.4.10C, при котором прослеживаются ИФБО в функциональной спецификации к модулям ФБО.

ИСО/МЭК 15408-3 ADV_TDS.4.9C: *В проекте должен быть описан каждый не влияющий на выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.*

10.8.4.4.12 Шаг оценивания ADV_TDS.4-12

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что не влияющие на выполнение ФТБ модули правильно категорированы.

Как упоминалось в шаге оценивания ADV_TDS.4-3, меньше информации запрашивается о модулях, которые не влияют на выполнение ФТБ. В этих случаях усилия оценщика направлены на попытку сделать заключение на основе свидетельств, предусмотренных для каждого модуля, неявно категорированного как не влияющего на выполнение ФТБ, и информации об оценке других модулей (в проекте ОО, функциональной спецификации, описании архитектуры безопасности и руководстве пользователя по эксплуатации), является ли модуль действительно не влияющим на выполнение ФТБ. На этом уровне доверия может быть допущена некоторая ошибка; оценщик не обязан быть абсолютно уверен, что данный модуль — не влияющий на выполнение ФТБ, даже если он маркирован как таковой. Однако если предоставленные свидетельства указывают, что не влияющие на выполнение ФТБ модули являются на самом деле осуществляющими или поддерживающими выполнение ФТБ, оценщик запрашивает дополнительную информацию от разработчика, чтобы сделать заключение о явной несогласованности. Например, предположим, что в документации для Модуля A (который является осуществляющим выполнение ФТБ) указано, что он вызывает Модуль B для проверки доступа некой конструкции. Когда оценщик исследует информацию, связанную с Модулем B, он обнаруживает, что разработчик предоставил только назначение и ряд взаимодействий (таким образом неявно категорируя Модуль B как поддерживающий или не влияющий на выполнение ФТБ). При исследовании назначения и взаимодействий Модуля A, оценщик не находит упоминания о Модуле B, выполняющем проверку доступа, а Модуль A не отмечен как модуль, с которым взаимодействует Модуль B. В этом пункте оценщику следует обратиться к разработчику, чтобы сделать заключение о несоответствии между информацией, предоставленной в Модуле A и Модуле B.

В случаях, когда разработчик обеспечил различное количество информации для различных модулей, была сделана неявная классификация. Таким образом, модули, например с детализацией, представленной на связанных с ФТБ интерфейсах (см. ADV_TDS.3.10C), являются модулями-кандидатами на категорию осуществляющих выполнение ФТБ, хотя проведенный оценщиком анализ может привести к заключению, что некоторые из них поддерживающие или не влияющие на выполнение ФТБ. Те, для которых приводится только описание назначения и взаимодействия с другими модулями, например «неявно категорируются» как поддерживающие или не влияющие на выполнение ФТБ.

Другой пример — когда оценщик исследует прослеживание ИФБО к модулям в соответствии с ADV_TDS.4.2D. Этот анализ показывает, что Модуль C связан с требуемой по ТФБ идентификацией пользователя. Опять же, когда оценщик исследует информацию, связанную с Модулем C, он обнаруживает, что разработчик предоставил только назначение и ряд взаимодействий (таким образом неявно категорируя Модуль C как поддерживающий или не влияющий на выполнение ФТБ). Исследуя назначение и ряд Модуля C, оценщик не способен сделать заключение, почему Модуль C, перечисленный в прослеживании к ИФБО, касающемуся пользовательской идентификации, не классифицирован как осуществляющий выполнение требований ФТБ. И в этом случае оценщику следует обратиться к разработчику для того, чтобы сделать заключение о том, что это несоответствие.

Последний пример касается обратного случая. Допустим, разработчик предоставил информацию, связанную с Модулем D, по назначению и ряду взаимодействий (таким образом неявно категорируя Модуль B как поддерживающий или не влияющий на выполнение ФТБ). Оценщик исследует все свидетельства, включая назначение и взаимодействия для Модуля D. В назначении дается значимое описание функции Модуля D в ОО, взаимодействия совместимы с этим описанием, и нет ничего, указывающего на возможную принадлежность Модуля D к осуществляющим выполнение ФТБ. В этом случае оценщику не следует требовать дополнительную информацию о Модуле D «просто для уверенности», что он правильно категорирован. Разработчик выполнил свои обязательства и приобретенного оценщиком доверия от неявной классификации Модуля D (по определению) достаточно для этого уровня доверия.

10.8.4.4.13 Шаг оценивания ADV_TDS.4-13

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что описание назначения каждого не влияющего на выполнение ФТБ модуля выполнено полно и точно.

Описание назначения модуля указывает на то, какие функции выполняет модуль. Из описания оценщику следует быть в состоянии получить общее представление о роли модуля. Чтобы удостовериться, что описание достаточно полно, оценщик использует информацию, предоставленную о взаимодействиях модуля с другими модулями для оценки совместимости причин вызовов модуля с назначением модуля. Если описание взаимодействия содержит функции, которые не очевидны из назначения модуля или являются конфликтующими с ним, оценщик должен сделать заключение, является ли это несоответствие проблемой точности или полноты описания. Оценщику следует с подозрением относиться к слишком коротким описаниям назначения, так как значимый анализ, основанный на назначении только с одним предложением, вероятно, будет невозможно провести.

Поскольку модули на таком низком уровне, может быть трудно сделать заключение о воздействии на полноту и точность на основании анализа другой документации, такой как руководство пользователя по эксплуатации, функциональная спецификация, внутренняя структура ФБО или «Описание архитектуры безопасности». Однако оценщик использует информацию этих документов по мере возможности, чтобы удостовериться в точности и полноте описания назначения. Такому анализу может помочь анализ, выполняемый для шагов оценивания элемента ADV_TDS.4.10C, при котором прослеживаются ИФБО в функциональной спецификации к модулям ФБО.

10.8.4.4.14 Шаг оценивания ADV_TDS.4-14

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что описание взаимодействия каждого не влияющего на выполнение ФТБ модуля с другими модулями является полным и точным.

Важно отметить, что в терминах требований ИСО/МЭК 15408-3 и этого шага оценивания, термин *взаимодействие* является менее строгим, чем *интерфейс*. Взаимодействие не обязательно должно быть характеризовано на уровне реализации (например параметры из одной процедуры в одной подсистеме переходят к процедуре другой подсистемы; глобальные переменные; сигналы аппаратных средств (например прерывания) от подсистемы аппаратных средств до системы обработки прерываний), но элементы данных, идентифицированных для конкретного модуля, которые будут использоваться другим модулем, следует охватить этим рассмотрением. Любые отношения контроля между подсистемами (например имеется подсистема, ответственная за формирование базовых правил для межсетевого экрана и подсистемы, которая фактически реализует эти правила) также следует включать в описание.

Поскольку модули на таком низком уровне, то может быть трудно сделать заключение о воздействии на полноту и точность на основании анализа другой документации, такой как руководство пользователя по эксплуатации, функциональная спецификация, внутренняя структура ФБО или «Описание архитектуры безопасности». Однако оценщик использует информацию этих документов по мере возможности, чтобы удостовериться в точности и полноте описания функций. Такому анализу может помочь анализ, выполняемый для шагов оценивания элемента ADV_TDS.3.10C, при котором прослеживаются ИФБО в функциональной спецификации к модулям ФБО.

Взаимодействие модуля с другими модулями может быть отражено различными способами. Цель для проекта ОО состоит в том, чтобы предоставить оценщику понимание (частично посредством анализа взаимодействий модуля) роли поддерживающих и не влияющих на выполнение ФТБ модулей в общем проекте ОО. Понимание этой роли поможет оценщику на последующем шаге оценивания ADV_TDS.4-7.

Взаимодействие модуля с другими модулями рассматривается вне документа, где зафиксировано дерево вызовов. Взаимодействие описывается с функциональной точки зрения и касается того, почему данный модуль взаимодействует с другими модулями. В назначении модуля описывается, какие функции модуль предоставляет другим модулям; во взаимодействиях следует описать, от каких модулей зависит данный модуль для выполнения своих функций.

Поскольку модули на таком низком уровне, то может быть трудно сделать заключение о воздействии на полноту и точность на основании анализа другой документации, такой как руководство пользователя по эксплуатации, функциональная спецификация, внутренняя структура ФБО или «Описание архитектуры безопасности». Однако оценщик использует информацию этих документов по мере возможности, чтобы удостовериться в точности и полноте описания взаимодействий.

ИСО/МЭК 15408-3 ADV_TDS.4.10C: *В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.*

10.8.4.4.15 Шаг оценивания ADV_TDS.4-15

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что он содержит полное и точное прослеживание от ИФБО, описанных в функциональной спецификации, к модулям ФБО, описанным в проекте ОО.

Описание модулей в проекте ОО предоставляют описание того, каким образом ФБО реализуются. ИФБО обеспечивают описание того, каким образом осуществляется реализация. Свидетельства от разработчика идентифицируют модуль, который вовлечен в процесс запроса операции от ИФБО, и идентифицируют цепочку модулей, которые прежде всего отвечают за реализацию функций. Однако для данного шага оценивания не требуется предоставить полное «дерево вызовов» для каждого ИФБО. Случаи, в которых требуется идентифицировать больше одного модуля — это модули «точки входа» или модули адаптера интерфейса, единственные функции которых — приведение исходных данных к требуемым условиям и демультиплексирование исходных данных. Прослеживание к этим модулям не дало бы оценщику никакой полезной информации.

Оценщик оценивает полноту прослеживания, удостоверяясь, что каждый ИФБО прослежен по крайней мере к одной подсистеме. Проверка точности более сложна.

Первый аспект точности заключается в том, что каждый ИФБО прослеживается к подсистеме, находящейся в пределах ФБО. Такое заключение может быть сделано при рассмотрении описания подсистем и их взаимодействия и определении места подсистемы в архитектуре безопасности на основании данной информации. Следующий аспект точности — то, что прослеживание имеет смысл. Например, прослеживание ИФБО, обеспечивающего контроль доступа, к подсистеме, которая проверяет пароли, не будет являться точным. Оценщику и в этом случае при вынесении заключения следует использовать свое суждение. Цель состоит в том, что эта информация поможет оценщику в понимании системы, реализации выполнения ФТБ и способов, которыми сущности в пределах ФБО могут взаимодействовать с ФБО. Большая часть оценки того, точно ли описаны ФТБ подсистемами, выполняется при проведении других шагов оценивания.

10.8.4.5 Действие ADV_TDS.4.2E

10.8.4.5.1 Шаг оценивания ADV_TDS.4-16

Оценщик должен исследовать ФТБ ОО и проект ОО, чтобы сделать заключение о том, что все ФТБ в ЗБ охвачены в проекте ОО.

Оценщик может провести прослеживание между ФТБ для ОО и проектом ОО. Это прослеживание, вероятно, будет проводиться от функционального требования до ряда подсистем и далее до модулей. Следует отметить, что это прослеживание, вероятно, будет по уровню детализации ниже, чем для компонента или даже для элемента требований из-за операций (назначения, уточнения, выбора), которые выполняются над функциональным требованием автором ЗБ.

Например, компонент FDP_ACC.1 «Ограниченное управление доступом» содержит элемент с операцией назначения. Если бы в ЗБ содержалось, например десять правил в назначении для данного компонента FDP_ACC.1, и эти правила применялись бы в определенных местах в пределах пятнадцати модулей, то для оценщика некорректно было бы проследить компонент FDP_ACC.1 к одной подсистеме и утверждать о завершении шага оценивания. Вместо этого оценщик должен проследить первое правило компонента FDP_ACC.1 к подсистеме A и режимам функционирования x, y и z; второе правило компонента FDP_ACC.1 к подсистеме A и режимам функционирования x, p и q; и т. д.

10.8.4.5.2 Шаг оценивания ADV_TDS.4-17

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что в нем точно представлены все ФТБ.

Оценщик может провести прослеживание между ФТБ для ОО и проектом ОО. Это прослеживание, вероятно, будет проводиться от функционального требования до ряда подсистем. Следует отметить, что это прослеживание, вероятно, будет по уровню детализации ниже, чем для компонента или даже для элемента требований из-за операций (назначения, уточнения, выбора), которые выполняются над функциональным требованием автором ЗБ.

Например, если требования в ЗБ определяют основанный на ролевой модели механизм управления доступом, оценщик сначала идентифицирует подсистемы, которые способствуют реализации этого механизма. Это может быть сделано с применением углубленного изучения или с применением понимания проекта ОО или работ, полученного в предыдущих шагах оценивания. Следует отметить, что это прослеживание необходимо только для идентификации подсистем и не является полным анализом.

Следующий шаг — понять, какой из механизмов подсистем и модулей осуществляется. Например, если в проекте описывается реализация управления доступом, основанная на битах защиты UNIX, то проект не является точным отражением требований по управлению доступом в ЗБ для того примера, который использовался выше. Если оценщик не может сделать заключение о том, что механизм был реализован точным образом из-за недостаточной детализации предоставленной ему информации, то ему нужно будет оценить, были ли все осуществляющие выполнение ФТБ подсистемы и модули

идентифицированы, или был ли предоставлен для этих подсистем и модулей достаточный уровень детализации.

10.8.5 Подвид деятельности по оценке (ADV_TDS.5)

Общее руководство отсутствует; за консультациями по выполнению данного подвида деятельности следует обращаться в конкретную систему оценки.

10.8.6 Подвид деятельности по оценке (ADV_TDS.6)

Общее руководство отсутствует; за консультациями по выполнению данного подвида деятельности следует обращаться в конкретную систему оценки.

11 Класс AGD: Руководства

11.1 Введение

Вид деятельности «Руководства» предназначен для определения достаточности документации, регламентирующей, как пользователь может работать с ОО безопасным образом. В такой документации следует учитывать различные типы пользователей (например тех, кто принимает, устанавливает, администрирует и осуществляет эксплуатацию ОО), чьи неправильные действия могли бы отрицательно повлиять на безопасность ОО или их собственных данных.

Класс «Руководства» разделен на два семейства, которые касаются, во-первых, руководства пользователя по подготовительным процедурам (о том, что должно делаться для перевода поставленного ОО в его оцененную конфигурацию для среды функционирования согласно описанию в ЗБ, то есть руководство по приемке и установке ОО), а во-вторых — руководства пользователя по эксплуатации (о том, что должно делаться во время функционирования ОО в его оцененной конфигурации, то есть функционирование и администрирование).

11.2 Замечания по применению

Вид деятельности «Руководства» применяется к тем функциям и интерфейсам, которые связаны с безопасностью ОО. Безопасная конфигурация ОО описывается в ЗБ.

11.3 Руководство пользователя по эксплуатации (AGD_OPE)

11.3.1 Подвид деятельности по оценке (AGD_OPE.1)

11.3.1.1 Цели

Цели данного подвида деятельности состоят в том, чтобы сделать заключение, описаны ли в руководстве пользователя для каждой пользовательской роли функции безопасности и интерфейсы, предоставляемые ФБО; предоставлены ли инструкции и указания по безопасному использованию ОО; адресуются ли процедуры безопасности ко всем возможным режимам функционирования; способствует ли руководство упрощению предотвращения и обнаружения потенциально опасных состояний ОО и не является ли руководство необоснованным и вводящим в заблуждение.

11.3.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект ОО, если он применим;

d) руководство пользователя.

11.3.1.3 Действие AGD_OPE.1.1E

ИСО/МЭК 15408-3 AGD_OPE.1.1C: *В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть представлено описание доступных пользователям функций, возможных прав и обязанностей, которыми следует управлять в защищенной среде функционирования, а также уместных предупреждений.*

11.3.1.3.1 Шаг оценивания AGD_OPE.1-1

Оценщик должен исследовать руководство пользователя, чтобы сделать заключение, описаны ли в нем для каждой пользовательской роли доступные пользователю функции и привилегии, которыми следует управлять в среде функционирования, а также соответствующие предостережения.

В зависимости от конфигурации ОО различные пользовательские роли могут иметь различные привилегии при использовании некоторых функций ОО. Это означает, что некоторым пользователям разрешено выполнять определенные функции, в то время как другим пользователям это не разрешается. Эти функции и привилегии следует описать в руководстве пользователя для каждой пользовательской роли.

Для каждой пользовательской роли в руководстве идентифицируются функции и привилегии, которыми нужно управлять, типы команд, требуемых для них, а также причины таких команд. Рекомендуется, чтобы руководство пользователя содержало предупреждения относительно использования этих функций и привилегий. В предупреждениях следует описывать ожидаемые последствия, возможные побочные эффекты и возможные взаимодействия с другими функциями и привилегиями.

ИСО/МЭК 15408-3 AGD_OPE.1.2C: *В руководстве пользователя по эксплуатации в рамках каждой пользовательской роли должно быть представлено описание принципов безопасной работы с предоставленными в ОО интерфейсами.*

11.3.1.3.2 Шаг оценивания AGD_OPE.1-2

Оценщик должен исследовать руководство пользователя по эксплуатации, чтобы сделать заключение, описаны ли в нем для каждой пользовательской роли принципы безопасной работы с предоставляемыми ОО интерфейсами.

В руководстве пользователя следует представить рекомендации относительно эффективного использования ФБО (например практика пересмотра и смены пароля, предполагаемая частота создания резервных копий файлов пользователей, обсуждение влияния изменения пользовательских привилегий на доступ).

ИСО/МЭК 15408-3 AGD_OPE.1.3C: *В руководстве пользователя по эксплуатации должно быть представлено описание доступных для каждой пользовательской роли функций и интерфейсов, в особенности всех параметров безопасности под управлением пользователя, с указанием безопасных значений, если это уместно.*

11.3.1.3.3 Шаг оценивания AGD_OPE.1-3

Оценщик должен исследовать руководство пользователя по эксплуатации, чтобы сделать заключение о том, что оно описывает для каждой пользовательской роли доступные функции безопасности и интерфейсы, в особенности все параметры безопасности под управлением пользователя, с указанием для них безопасных значений.

В руководство пользователя следует включать краткий обзор функциональных возможностей безопасности, видимых через пользовательские интерфейсы.

В руководстве пользователя следует идентифицировать и описать назначение, режимы функционирования, а также взаимосвязи интерфейсов и функций безопасности.

Для каждого интерфейса и каждой функции безопасности в руководстве пользователя следует описать:

a) метод (методы) вызова интерфейса (например с использованием командной строки, системных вызовов языка программирования, меню, командной клавиши);

b) параметры, которые устанавливаются пользователем, их назначение, допустимые значения и значения по умолчанию, а также безопасное и небезопасное использование данных параметров как по отдельности, так и в некой комбинации;

c) реакцию, сообщения или возвращаемый код непосредственно от ФБО.

Оценщику следует рассмотреть функциональную спецификацию и ЗБ в целях вынесения заключения о том, что описанные в этих документах ФБО согласованы с руководством пользователя по эксплуатации. Оценщик должен удостовериться, что руководство пользователя по эксплуатации достаточно полно для того, чтобы позволить всем типам пользователей безопасное использование ФБО через доступные ИФБО. В рамках оказания содействия оценщик может подготовить неформальное прослеживание между руководством и этими документами. Любые упущения в этом прослеживании могут указывать на неполноту руководства.

ИСО/МЭК 15408-3 AGD_OPE.1.4C: *В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть четкое представление каждого типа имеющих значение для безопасности событий, связанных с доступными пользователю обязательными для выполнения функциями, включая изменение характеристик безопасности сущностей, находящихся под управлением ФБО.*

11.3.1.3.4 Шаг оценивания AGD_OPE.1-4

Оценщик должен исследовать руководство пользователя по эксплуатации, чтобы сделать заключение о том, что оно содержит для каждой пользовательской роли описание каждого типа относящихся к безопасности событий, связанных с доступными пользователю обязательными для выполнения функциями, включая изменение характеристик безопасности сущностей, находящихся под управлением ФБО, и операции, предпринимаемые после сбоя или ошибки эксплуатации.

Все типы событий, имеющих значение для безопасности, детализируются для каждой пользовательской роли таким образом, что каждый пользователь знает, какие события могут произойти и какие меры (если таковые возможны) ему, скорее всего, придется применить для поддержания безопасности.

События, имеющие значение для безопасности, которые могут произойти во время функционирования ОО (переполнение журнала аудита, падение системы, обновления записей пользователей, например удаление учетной записи пользователя при его увольнении из организации), определены в руководстве соответствующим образом для того, чтобы позволить пользователю вмешаться в функционирование ОО в целях поддержания безопасного функционирования.

ИСО/МЭК 15408-3 AGD_OPE.1.5C: *В руководстве пользователя по эксплуатации должны быть идентифицированы все возможные режимы работы ОО (включая операции после сбоев или ошибок эксплуатации), их последствия и участие в обеспечении безопасного функционирования.*

11.3.1.3.5 Шаг оценивания AGD_OPE.1-5

Оценщик должен исследовать руководство пользователя по эксплуатации и другие свидетельства оценки, чтобы сделать заключение о том, что в руководстве идентифицированы все возможные режимы работы ОО (включая, если возможно, операции восстановления после сбоев или ошибок эксплуатации), их последствия и участие в обеспечении безопасного функционирования.

Другие свидетельства оценки, в особенности функциональная спецификация, являются источниками информации, которые оценщику следует использовать, чтобы сделать заключение о том, что руководство содержит достаточную информацию.

Если тестовая документация включена в пакет доверия, то информация, предоставленная в этих свидетельствах, может также использоваться для того, чтобы сделать заключение о том, что документация руководств достаточна. Детализация, предоставленная на этапах тестирования, может использоваться для подтверждения того, что предоставленное руководство является достаточным для использования и администрирования ОО.

Оценщику следует сосредоточить усилия на одном видимом пользователю ИФБО единовременно, сравнивая руководство по безопасному использованию ИФБО с другими свидетельствами оценки в целях вынесения заключения о том, что руководство, связанное с ИФБО, достаточно для безопасного использования этого ИФБО (то есть соответствует ФТБ). Оценщику следует также рассмотреть отношения между интерфейсами в поисках возможных конфликтов.

ИСО/МЭК 15408-3 AGD_OPE.1.6C: *В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть описание всех мер безопасности, предназначенных для выполнения целей безопасности для среды функционирования согласно описанию в ЗБ.*

11.3.1.3.6 Шаг оценивания AGD_OPE.1-6

Оценщик должен исследовать руководство пользователя по эксплуатации, чтобы сделать заключение о том, что оно описывает для каждой пользовательской роли меры безопасности, предназначенных для выполнения целей безопасности для среды функционирования согласно описанию в ЗБ.

Оценщик анализирует цели безопасности для среды функционирования в ЗБ и делает заключение о том, что для каждой пользовательской роли в руководстве пользователя описаны соответствующие меры безопасности.

Следует, чтобы меры безопасности, описанные в руководстве пользователя, включали все меры, имеющие отношение к внешним процедурам, меры физической защиты, организационные меры, связанные с персоналом, а также меры обеспечения связности.

Следует отметить, что меры, имеющие значение для безопасной установки ОО, исследуются в рамках семейства «Подготовительные процедуры» (AGD_PRE).

ИСО/МЭК 15408-3 AGD_OPE.1.7C: *руководство пользователя по эксплуатации должно быть понятным и обоснованным.*

11.3.1.3.7 Шаг оценивания AGD_OPE.1-7

Оценщик должен исследовать руководство пользователя по эксплуатации, чтобы сделать заключение о том, что оно является ясным.

Руководство считается неясным, если оно может быть неверно истолковано администратором или пользователем и использовано способом, небезопасным и потенциально вредным для ОО или для мер/средств безопасности ОО.

11.3.1.3.8 Шаг оценивания AGD_OPE.1-8

Оценщик должен исследовать руководство пользователя по эксплуатации, чтобы сделать заключение о том, что оно является обоснованным.

Руководство считается необоснованным, если его реализация требует такого использования ОО или среды его функционирования, которое не согласуется с ЗБ или слишком обременительно для поддержания безопасности.

11.4 Подготовительные процедуры (AGD_PRE)

11.4.1 Подвид деятельности по оценке (AGD_PRE.1)

11.4.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, были ли процедуры и шаги, предпринятые для безопасной подготовки ОО к использованию, документированы и привели ли они к безопасной конфигурации ОО.

11.4.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) ОО, включая связанные с ним подготовительные процедуры;

c) описание процедур поставки, используемых разработчиком (если применимо).

11.4.1.3 Замечания по применению

Подготовительные процедуры относятся ко всем процедурам приемки и установки, необходимым для перевода ОО в безопасную конфигурацию согласно описанию в ЗБ.

11.4.1.4 Действие AGD_PRE.1.1E

ИСО/МЭК 15408-3 AGD_PRE.1.1C: *В подготовительных процедурах должны описываться все шаги, необходимые для безопасной приемки поставленного ОО в соответствии с процедурами поставки разработчика.*

11.4.1.4.1 Шаг оценивания AGD_PRE.1-1

Оценщик должен исследовать представленные процедуры приемки, чтобы сделать заключение о том, что они описывают шаги, необходимые для безопасной приемки ОО в соответствии с процедурами поставки разработчика.

Если от процедур поставки разработчика не ожидается, что процедуры приемки будут применяться или могут быть применены, то этот шаг оценивания не применим и потому считается удовлетворенным.

В процедуры приемки следует включать как минимум то, что пользователь должен проверить, что все части ОО, как указано в ЗБ, были поставлены в правильной версии.

В процедурах приемки следует отразить подразумеваемые процедурами поставки разработчика шаги, которые должен предпринять пользователь для осуществления приемки поставленного ОО.

В процедурах приемки следует предоставить подробную информацию о следующем, если это применимо:

a) о проведенной проверке того, что ОО поставлен полностью и в оцененной комплектации;

b) об обнаружении модификации/подмены ОО при поставке.

ИСО/МЭК 15408-3 AGD_PRE.1.2C: *В подготовительных процедурах должны описываться все необходимые шаги для безопасной установки ОО и безопасной подготовки среды функционирования в соответствии с целями безопасности для среды функционирования, описанными в ЗБ.*

11.4.1.4.2 Шаг оценивания AGD_PRE.1-2

Оценщик должен исследовать представленные процедуры установки, чтобы сделать заключение о том, что они описывают шаги, необходимые для безопасной установки ОО и безопасной подготовки среды функционирования в соответствии с целями безопасности в ЗБ.

Если не ожидается, что процессы установки будут применяться или могут быть применены для ОО и среды его функционирования (например потому, что ОО может уже быть поставлен в рабочем состоянии и нет никаких требований к среде функционирования), то этот шаг оценивания не применим и поэтому считается удовлетворенным.

В процедурах установки следует предоставить подробную информацию о следующем, если это применимо:

a) о минимальных системных требованиях для безопасной установки;

b) о требованиях для среды функционирования в соответствии с целями безопасности, представленными в ЗБ;

c) о шагах, которые должен выполнить пользователь, чтобы используемый ОО соответствовал его оцененной конфигурации. Такое описание должно включать — для каждого шага — понятную схему для решения по поводу следующего шага в зависимости от успеха, сбоя или проблем на текущем шаге;

d) об изменении характерных для установки характеристик безопасности сущностей, управляемых ФБО (например параметров, настроек, паролей);

e) об обработке исключений и проблем.

11.4.1.5 Действие AGD_PRE.1.2E

11.4.1.5.1 Шаг оценивания AGD_PRE.1-3

Оценщик должен выполнить все пользовательские процедуры, необходимые для подготовки ОО, чтобы сделать заключение, могут ли ОО и среда его функционирования быть защищенным образом подготовлены с использованием только предоставленного руководства пользователя по подготовительным процедурам.

По подготовительным процедурам требуется, чтобы оценщик перевел ОО от состояния, в котором он находился на момент поставки, до состояния функционирования, включая приемку и установку ОО и осуществление выполнения ФТБ, совместимых с целями безопасности для ОО, определенными в ЗБ.

Оценщику можно следовать только процедурам разработчика и выполнять действия, которые ожидаются от заказчика (пользователя ОО) для приемки и установки ОО, используя только предоставленное ему руководство пользователя по подготовительным процедурам. Любые трудности, с которыми сталкивается оценщик во время осуществления этих действий, могут быть признаками неполного, неясного или необоснованного руководства.

Этот шаг оценивания может быть выполнен вместе с действиями по оценке семейства «Независимое тестирование» (ATE_IND).

Если известно, что ОО будет использоваться в качестве зависимого компонента для оценки составного ОО, то оценщику следует удостовериться, что базовый компонент составного ОО удовлетворяет требованиям к среде функционирования ОО.

12 Класс ALC: Поддержка жизненного цикла

12.1 Введение

Вид деятельности «Поддержка жизненного цикла» предназначен для определения достаточности процедур, применяемых разработчиком во время разработки и сопровождения ОО. Эти процедуры включают в себя модель жизненного цикла, применяемую разработчиком, управление конфигурацией, меры безопасности во время разработки ОО, инструментальные средства, используемые разработчиком на протяжении жизненного цикла ОО, обработка недостатков безопасности и деятельность по поставке ОО.

Плохое управление разработкой и сопровождением ОО могут привести к уязвимостям в реализации. Соответствие определенной модели жизненного цикла может помочь улучшить меры управления в этих областях. Используемая для ОО измеримая модель жизненного цикла может снизить неоднозначность при оценивании процесса разработки ОО.

Вид деятельности «Управление конфигурацией» предназначен для помощи потребителю в идентификации оцениваемого ОО, чтобы удостовериться, что элементы конфигурации уникально идентифицированы, а также что процедуры, которые используются разработчиком для выявления и управления изменениями ОО, являются достаточными и обоснованными. Сюда же относится и детальная информация о том, какие изменения отслеживаются, каким образом комбинируются потенциальные изменения, и до какой степени используется автоматизация для уменьшения диапазона ошибки.

Процедуры безопасности, применяемые разработчиком, предназначены для защиты ОО и связанной с ним проектной информации от вмешательства или раскрытия. Вмешательство в процесс разработки может позволить преднамеренно внести уязвимости в ОО. Раскрытие информации о проекте может облегчить использование уязвимостей. Адекватность рассматриваемых процедур будет зависеть от свойств ОО и процесса его разработки.

Использование полностью определенных инструментальных средств разработки помогает удостовериться в том, что уязвимости не были непреднамеренно внесены в процессе уточнения ФБО.

Деятельность по исправлению недостатков предназначена для того, чтобы выявить недостатки защиты, сделать заключение о необходимых корректирующих действиях и донести информацию о корректирующих действиях до пользователей.

Цель деятельности по поставке состоит в том, чтобы оценить достаточность документации процедур, используемых для обеспечения того, что ОО поставлен потребителю без внесения изменений.

12.2 Возможности УК (ALC_CMC)

12.2.1 Подвид деятельности по оценке (ALC_CMC.1)

12.2.1.1 Цели

Цель данного подвида деятельности — сделать заключение, четко ли разработчик идентифицировал ОО.

12.2.1.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) ЗБ;

b) ОО, пригодный для тестирования.

12.2.1.3 Действие ALC_CMC.1.1E

ИСО/МЭК 15408-3 ALC_CMC.1.1C: *ОО должен быть помечен уникальной маркировкой.*

12.2.1.3.1 Шаг оценивания ALC_CMC.1-1

Оценщик должен проверить, что ОО, представленный для оценки, имеет собственную маркировку.

Оценщику следует удостовериться, что ОО содержит уникальную маркировку, изложенную в ЗБ. Этого можно достичь, используя маркированную упаковку или носители, или же маркировку, отображаемую ОО при функционировании. Это предоставляет потребителю возможность идентификации ОО (например при приобретении или использовании).

ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, ОО, являющийся программным продуктом, может отображать свое название и номер версии при запуске программы или в ответ на запрос через командную строку. Аппаратный или программно-аппаратный ОО может быть идентифицирован путем нанесения на нем соответствующего номера штампом.

Возможен и альтернативный вариант, когда уникальная маркировка ОО представляет собой комбинацию уникальных маркировок каждого компонента, из которых состоит ОО (например в случае составного ОО).

12.2.1.3.2 Шаг оценивания ALC_CMC.1-2

Оценщик должен проверить непротиворечивость используемой маркировки ОО.

Если ОО маркирован несколько раз, то необходима согласованность маркировок. Например, следует предусмотреть возможность связать любое маркированное руководство, поставляемое в составе ОО, с оцененным функционирующим ОО. Этим обеспечивается уверенность потребителя в том, что он приобрел оцененную версию ОО, установил эту же версию и располагает надлежащей редакцией руководства, необходимой для эксплуатации данного ОО в соответствии с его ЗБ.

Оценщик также верифицирует, что маркировка ОО согласуется с ЗБ.

Если этот шаг оценивания будет применяться к составному ОО, то применимо следующее. Составной ОО ИТ не будет маркирован уникальной (составной) маркировкой, только отдельные компоненты будут соответственно маркированы. Для этого требуется маркировать дальнейшую разработку ОО ИТ, например во время запуска и/или функционирования составной маркировкой. Если составной ОО будет поставляться как часть целого, состоящего из ОО-компонентов, то ОО-компоненты не будут маркированы составной маркировкой. Однако в ЗБ составного ОО будет включена уникальная маркировка составного ОО, а также будут идентифицированы компоненты, включенные в составной ОО, благодаря чему потребители будут в состоянии сделать заключение о том, имеются ли у них соответствующие компоненты.

12.2.2 Подвид деятельности по оценке (ALC_CMC.2)

12.2.2.1 Цели

Цели этого подвида деятельности состоят в том, чтобы сделать заключение о том, использует ли разработчик систему УК, которая уникально идентифицирует все элементы конфигурации.

12.2.2.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) ЗБ;

b) ОО, пригодный для тестирования;

c) документация по управлению конфигурацией.

12.2.2.3 Замечания по применению

Этот компонент содержит неявное действие оценщика, требуемое для того, чтобы сделать заключение, используется ли система УК. Поскольку требования здесь ограничены идентификацией ОО и предоставленным списком конфигурации, это действие уже охвачено и ограничено существующими шагами оценивания. При применении «Подвида деятельности по оценке» ALC_CMC.3 требования расширяются, и требуются более явные свидетельства функционирования системы УК помимо двух, указанных выше.

12.2.2.4 Действие ALC_CMC.2.1E

ИСО/МЭК 15408-3 ALC_CMC.2.1C: *ОО должен быть помечен уникальной маркировкой.*

12.2.2.4.1 Шаг оценивания ALC_CMC.2-1

Оценщик должен проверить, что ОО, представленный для оценки, имеет собственную маркировку.

Оценщику следует удостовериться, что ОО содержит уникальную маркировку, изложенную в ЗБ. Этого можно достичь, используя маркированную упаковку или носители, или же маркировку, отображаемую ОО при функционировании. Это предоставляет потребителю возможность идентификации ОО (например при приобретении или использовании).

ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, ОО, являющийся программным продуктом, может отображать свое название и номер версии при запуске программы или в ответ на запрос через командную строку. Аппаратный или программно-аппаратный ОО может быть идентифицирован путем нанесения на нем соответствующего номера штампом.

Возможен и альтернативный вариант, когда уникальная маркировка ОО представляет собой комбинацию уникальных маркировок каждого компонента, из которых состоит ОО (например в случае составного ОО).

12.2.2.4.2 Шаг оценивания ALC_CMC.2-2

Оценщик должен проверить непротиворечивость используемой маркировки ОО.

Если ОО маркирован несколько раз, то необходима согласованность меток. Например, следует предусмотреть возможность связать любое маркированное руководство, поставляемое в составе ОО, с оцененным функционирующим ОО. Этим обеспечивается уверенность потребителя в том, что он приобрел оцененную версию ОО, установил эту же версию и располагает надлежащей редакцией руководства, необходимой для эксплуатации данного ОО в соответствии с его ЗБ.

Оценщик также верифицирует, что маркировка ОО согласуется с ЗБ.

Если этот шаг оценивания будет применяться к составному ОО, то применимо следующее. Составной ОО ИТ не будет маркирован уникальной (составной) маркировкой; только отдельные компоненты будут соответственно маркированы. Для этого требуется маркировать дальнейшую разработку ОО ИТ, например во время запуска и/или функционирования, составной маркировкой. Если составной ОО будет поставляться как часть целого, состоящего из ОО-компонентов, то компоненты ОО не будут маркированы составной маркировкой. Однако в ЗБ составного ОО будет включена уникальная маркировка составного ОО, а также будут идентифицированы компоненты, входящие в составной ОО, благодаря чему потребители будут в состоянии сделать заключение о том, имеются ли у них соответствующие компоненты.

ИСО/МЭК 15408-3 ALC_CMC.2.2C: *В документации УК должно содержаться описание метода, используемого для уникальной идентификации элементов конфигурации.*

12.2.2.4.3 Шаг оценивания ALC_CMC.2-3

Оценщик должен исследовать метод идентификации элементов конфигурации, чтобы сделать заключение о том, что в нем описано, каким образом уникально идентифицирован каждый элемент конфигурации.

В процедурах следует описать, каким образом состояние каждого элемента конфигурации может быть прослежено на любом этапе жизненного цикла ОО. Процедуры такого прослеживания могут быть детально описаны в плане УК или по всей документации УК. В эту информацию следует включать описание:

a) метода уникальной идентификации элементов, такой, что есть возможность отследить версии конкретного элемента конфигурации;

b) метода назначения уникальных идентификаторов элементам конфигурации и метода их введения в систему УК;

c) метода, который будет использоваться для идентификации новых версий элементов конфигурации, замещающих старые.

ИСО/МЭК 15408-3 ALC_CMC.2.3C: *В системе УК должны быть уникальным образом идентифицированы все элементы конфигурации.*

12.2.2.4.4 Шаг оценивания ALC_CMC.2-4

Оценщик должен исследовать элементы конфигурации, чтобы сделать заключение о том, что они идентифицированы способом, который не противоречит документации УК.

Доверие тому, что система УК уникально идентифицирует все элементы конфигурации, приобретается путем исследования идентификаторов элементов конфигурации. И для элементов конфигурации, которые включены в ОО, и для проектов элементов конфигурации, которые предоставлены разработчиком как свидетельства оценки, оценщик подтверждает, что каждый элемент конфигурации обладает уникальным идентификатором, присвоенным ему способом, совместимым с методом уникальной идентификации, описанным в документации по УК.

12.2.3 Подвид деятельности по оценке (ALC_CMC.3)

12.2.3.1 Цели

Цели этого подвида деятельности состоят в том, чтобы сделать заключение о том, использует ли разработчик систему УК, которая уникально идентифицирует все элементы конфигурации, и правильно ли управляется способность изменять эти элементы.

12.2.3.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) ЗБ;

b) ОО, пригодный для тестирования;

c) документация по управлению конфигурацией.

12.2.3.3 Действие ALC_CMC.3.1 E

ИСО/МЭК 15408-3 ALC_CMC.3.1C: *ОО должен быть помечен уникальной маркировкой.*

12.2.3.3.1 Шаг оценивания ALC_CMC.3-1

Оценщик должен проверить, что ОО, представленный для оценки, имеет собственную маркировку.

Оценщику следует удостовериться, что ОО содержит уникальную маркировку, позволяющую отличать разные версии ОО. Этого можно достичь, используя маркированную упаковку или носители, или же маркировку, отображаемую ОО при функционировании. Это предоставляет потребителю возможность идентификации ОО (например при приобретении или использовании).

ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, ОО, являющийся программным продуктом, может отображать свое название и номер версии при запуске программы или в ответ на запрос через командную строку. Аппаратный или программно-аппаратный ОО может быть идентифицирован путем нанесения на нем соответствующего номера штампом.

Возможен и альтернативный вариант, когда уникальная маркировка ОО представляет собой комбинацию уникальных маркировок каждого компонента, из которых состоит ОО (например, в случае составного ОО).

12.2.3.3.2 Шаг оценивания ALC_CMC.3-2

Оценщик должен проверить непротиворечивость используемой маркировки ОО.

Если ОО маркирован несколько раз, то необходима согласованность меток. Например, следует предусмотреть возможность связать любое маркированное руководство, поставляемое в составе ОО, с оцененным функционирующим ОО. Этим обеспечивается уверенность потребителя в том, что он приобрел оцененную версию ОО, установил эту же версию и располагает надлежащей редакцией руководства, необходимой для эксплуатации данного ОО в соответствии с его ЗБ.

Оценщик также верифицирует, что маркировка ОО согласуется с ЗБ.

Если этот шаг оценивания будет применяться к составному ОО, то применимо следующее. Составной ОО ИТ не будет маркирован уникальной (составной) маркировкой; только отдельные компоненты будут соответственно маркированы. Для этого требуется маркировать дальнейшую разработку ОО ИТ, например во время запуска и/или функционирования, составной маркировкой. Если составной ОО будет поставляться как часть целого, состоящего из ОО-компонентов, то компоненты ОО не будут маркированы составной маркировкой. Однако в ЗБ составного ОО будет включена уникальная маркировка составного ОО, а также будут идентифицированы компоненты, включенные в составной ОО, благодаря чему потребители будут в состоянии сделать заключение о том, имеются ли у них соответствующие компоненты.

ИСО/МЭК 15408-3 ALC_CMC.3.2C: *В документации УК должно содержаться описание метода, используемого для уникальной идентификации элементов конфигурации.*

12.2.3.3.3 Шаг оценивания ALC_CMC.3-3

Оценщик должен исследовать метод идентификации элементов конфигурации, чтобы сделать заключение о том, что в нем описано, каким образом уникально идентифицирован каждый элемент конфигурации.

В процедурах следует описать, каким образом состояние каждого элемента конфигурации может быть прослежено на любом этапе жизненного цикла ОО. Процедуры такого прослеживания могут быть детально описаны в плане УК или по всей документации УК. В эту информацию следует включать описание:

a) метода уникальной идентификации элементов, такой, что есть возможность отследить версии конкретного элемента конфигурации;

b) метода назначения уникальных идентификаторов элементам конфигурации и метода их введения в систему УК;

c) метода, который будет использоваться для идентификации новых версий элементов конфигурации, замещающих старые.

ИСО/МЭК 15408-3 ALC_CMC.3.3C: *В системе УК должны быть уникальным образом идентифицированы все элементы конфигурации.*

12.2.3.3.4 Шаг оценивания ALC_CMC.3-4

Оценщик должен исследовать элементы конфигурации, чтобы сделать заключение о том, что они идентифицированы способом, который не противоречит документации УК.

Доверие тому, что система УК уникально идентифицирует все элементы конфигурации, приобретается путем исследования идентификаторов элементов конфигурации. И для элементов конфигурации, которые включены в ОО, и для проектов элементов конфигурации, которые предоставлены разработчиком как свидетельства оценки, оценщик подтверждает, что каждый элемент конфигурации обладает уникальным идентификатором, присвоенным ему способом, совместимым с методом уникальной идентификации, описанным в документации по УК.

ИСО/МЭК 15408-3 ALC_CMC.3.4C: *В системе УК должны быть предусмотрены такие меры, при применении которых в элементы конфигурации могут быть внесены только санкционированные изменения.*

12.2.3.3.5 Шаг оценивания ALC_CMC.3-5

Оценщик должен исследовать меры контроля доступа в УК, описанные в плане УК, чтобы сделать заключение об их эффективности по предотвращению несанкционированного доступа к элементам конфигурации.

Оценщик может использовать несколько методов для вынесения заключения об эффективности мер контроля доступа в УК. Например, оценщик может опробовать меры контроля доступа, чтобы удостовериться, что процедуры нельзя обойти. Оценщик может использовать выходные материалы, сгенерированные процедурами системы УК и уже подвергавшиеся исследованию на шаге оценивания ALC_CMC.3.8C. Оценщику может быть также продемонстрирована система УК, чтобы он убедился, что используемые меры контроля доступа выполняются эффективно.

ИСО/МЭК 15408-3 ALC_CMC.3.5C: *Документация УК должна включать в себя план УК.*

12.2.3.3.6 Шаг оценивания ALC_CMC.3-6

Оценщик должен проверить, что представленная документация УК содержит план УК.

План УК не обязательно должен быть единым, связанным документом, но рекомендуется, чтобы имелся некий документ с описанием того, где представлены различные части плана УК. На тот случай, если план УК не является единым документом, в следующем шаге оценивания приведен список, содержащий подсказки по поводу его содержания.

ИСО/МЭК 15408-3 ALC_CMC.3.6C: *В плане УК должно быть описание того, каким образом система УК используется для разработки ОО.*

12.2.3.3.7 Шаг оценивания ALC_CMC.3-7

Оценщик должен исследовать план УК в целях вынесения заключения о том, что в нем описывается, каким образом система УК используется для разработки ОО.

Описания, содержащиеся в плане УК, могут включать:

a) все операции, выполняемые в среде разработки ОО, которые подчинены процедурам управления конфигурацией (например создание, модификация или удаление элемента конфигурации, создание резервной копии данных, архивация);

b) средства (например инструменты УК, формы), которые должны быть доступны;

c) использование инструментов УК: необходимая детальная информация для пользователя системы УК, чтобы он мог правильно управлять инструментами УК в целях поддержания целостности ОО;

d) описание того, какие еще объекты (компоненты разработки, инструменты, среда оценки и т. д.) взяты под управление системы УК;

e) роли и обязанности должностных лиц, требуемые для выполнения операций над отдельными элементами конфигурации (для различных типов элементов конфигурации (например проектная документация или исходный код) могут быть идентифицированы различные пользовательские роли);

f) описание того, каким образом введены и укомплектованы организационно-штатные единицы системы УК (например совет по управлению изменениями, рабочие группы контроля интерфейсов);

g) описание управления изменениями;

h) процедуры, которые используются для обеспечения того, чтобы только уполномоченные лица могли изменять элементы конфигурации;

i) процедуры, которые используются для исключения проблем параллелизма, возникающих в случае одновременного изменения элементов конфигурации;

j) свидетельство, которое генерируется в результате применения процедур. Например, при изменении элемента конфигурации система УК может зафиксировать описание изменения, ответственность

за изменение, идентификацию всех затронутых элементов конфигурации, статус изменения (например «не завершено» или «завершено»), а также дату и время внесения изменения. Эта информация может быть занесена в журнал аудита произведенных изменений или в протокол контроля изменений;

k) подход к контролю версий и уникальной маркировке версий ОО (охватывающий, например выпуск исправлений («патчей») для операционных систем и последующее обнаружение их применения).

ИСО/МЭК 15408-3 ALC_CMC.3.7C: *В свидетельствах должно быть продемонстрировано, что все элементы конфигурации сопровождаются системой УК.*

12.2.3.3.8 Шаг оценивания ALC_CMC.3-8

Оценщик должен проверить, что элементы конфигурации, идентифицированные в списке конфигурации, сопровождаются системой УК.

Следует, чтобы система УК, используемая разработчиком, поддерживала целостность ОО. Оценщику следует проверить, что для каждого типа элементов конфигурации (например проектная документация или модули исходного кода), содержащихся в списке элементов конфигурации, есть примеры свидетельств, которые являются результатами производимых процедур, описанных в плане УК. В этом случае подход к осуществлению выборки будет зависеть от степени детализации, используемой в системе УК для управления элементами УК. Там, где, например в списке элементов конфигурации идентифицировано 10 000 модулей исходного кода, должна быть применена иная стратегия осуществления выборки по сравнению с тем случаем, где идентифицировано только пять таких модулей или вовсе один. Деятельность в рамках данного шага оценивания следует в первую очередь направить на оценку того, правильно ли функционирует система УК, а не на обнаружение любой незначительной ошибки.

Руководство по выборке см. в приложении А.2 «Выборка».

ИСО/МЭК 15408-3 ALC_CMC.3.8C: *В свидетельствах должно быть продемонстрировано, что система УК функционирует в соответствии с планом УК.*

12.2.3.3.9 Шаг оценивания ALC_CMC.3-9

Оценщик должен проверить документацию УК, чтобы удостовериться, что она включает записи системы УК, определенные планом УК.

Следует, чтобы выходные материалы системы УК обеспечили свидетельство, необходимое оценщику для уверенности, что план УК применяется, а все элементы конфигурации поддерживаются системой УК, как это требуется в ALC_CMC.3.7C. Пример выходных материалов может включать формы контроля изменений или формы разрешения доступа к элементам конфигурации.

12.2.3.3.10 Шаг оценивания ALC_CMC.3-10

Оценщик должен исследовать свидетельство, чтобы сделать заключение, что система УК используется в соответствии с планом УК.

Оценщику следует осуществить и исследовать выборку из свидетельства, охватывающую каждый тип операций по УК, выполняемых над элементами конфигурации (например создание, модификация, удаление, возврат к более ранней версии), чтобы подтвердить, что все операции системы УК выполнялись в соответствии с документированными процедурами. Оценщик подтверждает, что свидетельство включает всю информацию, идентифицированную для этой операции в плане УК. При исследовании свидетельства может потребоваться доступ к используемым инструментальным средствам УК. Оценщику разрешается остановиться на выборочной проверке свидетельства.

Руководство по выборке см. в приложении А.2 «Выборка».

Дополнительное доверие правильному функционированию системы УК и эффективному сопровождению элементов конфигурации может быть приобретено посредством проведения интервью с выбранными для этого участниками разработки. При проведении подобных интервью оценщику следует стремиться получить более глубокое понимание практического применения системы УК, а также удостовериться, что процедуры УК применяются в соответствии с документацией УК. Отметим, что такие интервью следует проводить скорее в дополнение, а не вместо исследования документального свидетельства; при этом они могут и не потребоваться, если документальное свидетельство само по себе удовлетворяет требованиям. Тем не менее, учитывая широкую область применения плана УК, возможно, что некоторые аспекты (например роли и обязанности) могут быть непонятны из одного только плана и протоколов УК. Это один из случаев, когда для разъяснения понадобится интервью.

Предполагается, что для поддержки этих действий оценщик посетит объект разработки.

Руководство по посещению объектов см. в приложении А.4 «Посещение объектов».

12.2.4 Подвид деятельности по оценке (ALC_CMC.4)

12.2.4.1 Цели

Цели этого подвида деятельности состоят в том, чтобы сделать заключение, идентифицировал ли разработчик ОО и связанные с ним элементы конфигурации однозначно и четко, а также организовано ли управление возможностями изменения этих элементов правильно с использованием автомати-

зированных инструментов, позволяющих сделать систему УК менее восприимчивой к человеческим ошибкам и ошибкам, допущенным по небрежности.

12.2.4.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) ЗБ;

b) ОО, пригодный для тестирования;

c) документация по управлению конфигурацией.

12.2.4.3 Действие ALC_CMC.4.1E

ИСО/МЭК 15408-3 ALC_CMC.4.1C: *ОО должен быть помечен уникальной маркировкой.*

12.2.4.3.1 Шаг оценивания ALC_CMC.4-1

Оценщик должен проверить, что ОО, представленный для оценки, имеет собственную маркировку.

Оценщику следует удостовериться, что ОО содержит уникальную маркировку, позволяющую отличать разные версии ОО. Этого можно достичь, используя маркированную упаковку или носители, или же маркировку, отображаемую ОО при функционировании. Это предоставляет потребителю возможность идентификации ОО (например при приобретении или использовании).

ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, ОО, являющийся программным продуктом, может отображать свое название и номер версии при запуске программы или в ответ на запрос через командную строку. Аппаратный или программно-аппаратный ОО может быть идентифицирован путем нанесения на нем соответствующего номера штампом.

Возможен и альтернативный вариант, когда уникальная маркировка ОО представляет собой комбинацию уникальных маркировок каждого компонента, из которых состоит ОО (например в случае составного ОО).

12.2.4.3.2 Шаг оценивания ALC_CMC.4-2

Оценщик должен проверить непротиворечивость используемой маркировки ОО.

Если ОО маркирован несколько раз, то необходима согласованность меток. Например, следует предусмотреть возможность связать любое маркированное руководство, поставляемое в составе ОО, с оцененным функционирующим ОО. Этим обеспечивается уверенность потребителя в том, что он приобрел оцененную версию ОО, установил эту же версию и располагает надлежащей редакцией руководства, необходимой для эксплуатации данного ОО в соответствии с его ЗБ.

Оценщик также верифицирует, что маркировка ОО согласуется с ЗБ.

Если этот шаг оценивания будет применяться к составному ОО, то применимо следующее. Составной ОО ИТ не будет маркирован уникальной (составной) маркировкой, только отдельные компоненты будут соответственно маркированы. Для этого требуется маркировать дальнейшую разработку ОО ИТ, например во время запуска и/или функционирования составной маркировкой. Если составной ОО будет поставляться как часть целого, состоящего из ОО-компонентов, то компоненты ОО не будут маркированы составной маркировкой. Однако в ЗБ составного ОО будет включена уникальная маркировка составного ОО, а также будут идентифицированы компоненты, включенные в составной ОО, благодаря чему потребители будут в состоянии сделать заключение о том, имеются ли у них соответствующие компоненты.

ИСО/МЭК 15408-3 ALC_CMC.4.2C: *В документации УК должно содержаться описание метода, используемого для уникальной идентификации элементов конфигурации.*

12.2.4.3.3 Шаг оценивания ALC_CMC.4-3

Оценщик должен исследовать метод идентификации элементов конфигурации, чтобы сделать заключение о том, что в нем описано, каким образом уникально идентифицирован каждый элемент конфигурации.

В процедурах следует описать, каким образом состояние каждого элемента конфигурации может быть прослежено на любом этапе жизненного цикла ОО. Процедуры такого прослеживания могут быть детально описаны в плане УК или по всей документации УК. В эту информацию следует включать описание:

a) метода уникальной идентификации элементов, такой, что есть возможность отследить версии конкретного элемента конфигурации;

b) метода назначения уникальных идентификаторов элементам конфигурации и метода их введения в систему УК;

c) метода, который будет использоваться для идентификации новых версий элементов конфигурации, замещающих старые.

ИСО/МЭК 15408-3 ALC_CMC.4.3C: *В системе УК должны быть уникальным образом идентифицированы все элементы конфигурации.*

12.2.4.3.4 Шаг оценивания ALC_CMC.4-4

Оценщик должен исследовать элементы конфигурации, чтобы сделать заключение о том, что они идентифицированы способом, который не противоречит документации УК.

Доверие тому, что система УК уникально идентифицирует все элементы конфигурации, приобретается путем исследования идентификаторов для элементов конфигурации. И для элементов конфигурации, которые включены в ОО, и для проектов элементов конфигурации, которые предоставлены разработчиком как свидетельства оценки, оценщик подтверждает, что каждый элемент конфигурации обладает уникальным идентификатором, присвоенным ему способом, совместимым с методом уникальной идентификации, описанным в документации по УК.

ИСО/МЭК 15408-3 ALC_CMC.4.4C: *В системе УК должны быть предусмотрены такие автоматизированные меры, при применении которых в элементы конфигурации могут быть внесены только санкционированные изменения.*

12.2.4.3.5 Шаг оценивания ALC_CMC.4-5

Оценщик должен исследовать меры контроля доступа в УК, описанные в плане УК (см. ALC_CMC.4.6C), чтобы сделать заключение, что они автоматизированы и эффективны для предотвращения несанкционированного доступа к элементам конфигурации.

Оценщик может использовать несколько методов для вынесения заключения об эффективности мер контроля доступа в УК. Например, оценщик может опробовать меры контроля доступа, чтобы удостовериться, что процедуры нельзя обойти. Оценщик может использовать выходные материалы, сгенерированные процедурами системы УК, требуемые на шаге оценивания ALC_CMC.4-10C. Оценщику может быть также продемонстрирована система УК, чтобы он убедился, что используемые меры контроля доступа выполняются эффективно.

ИСО/МЭК 15408-3 ALC_CMC.4.5C: *Система УК должна поддерживать производство ОО автоматизированными средствами.*

12.2.4.3.6 Шаг оценивания ALC_CMC.4-6

Оценщик должен проверить план УК (см. ALC_CMC.4.6C) для оценки автоматизированных процедур, предназначенных для поддержки производства ОО.

Термин «производство» применяется по отношению к процессам, принятым разработчиком для перевода ОО от представления реализации до состояния, приемлемого для поставки конечному потребителю.

Оценщик проверяет существование автоматизированных процедур поддержки производства ОО в рамках плана УК.

Примеры автоматизированных средств поддержки производства ОО:

- инструмент «создать» (предусмотренный во многих средствах разработки программного обеспечения) для случая ОО, являющегося программным продуктом;
- инструмент, автоматически обеспечивающий (например посредством штрих-кодов) комбинирование только тех частей, которые должны быть интегрированы для случая аппаратного ОО.

12.2.4.3.7 Шаг оценивания ALC_CMC.4-7

Оценщик должен исследовать процедуры, поддерживающие производство ОО, чтобы сделать заключение о том, что они эффективны для приобретения доверия, что сгенерированный ОО отражает представление его реализации.

В процедурах поддержки производства следует описать, какие инструменты должны использоваться для производства окончательной версии ОО из представления реализации полностью определенным способом. Соглашения, директивы и другие необходимые логические конструкции описаны в семействе ALC_TAT.

Оценщик делает заключение о том, что при выполнении процедур поддержки производства для производства ОО используются корректные элементы конфигурации. Например, в случае, когда ОО является программным обеспечением, это может включать проверку того, что автоматизированные производственные процедуры обеспечивают включение в компилированный объектный код всех исходных файлов и связанных с ними библиотек. Кроме того, процедурами следует обеспечить уникальное определение опций компилятора и других сопоставимых опций. Для аппаратных ОО в этот шаг оценивания может быть включена проверка того, что автоматизированные производственные процедуры предоставляют уверенность в том, что принадлежащие ОО части собраны вместе, и нет недостающих частей.

Клиент в этом случае может быть уверен, что версия ОО, поставленного для установки, получена из представления реализации однозначным способом и осуществляет ФТБ согласно описанию в ЗБ.

Оценщику следует учитывать, что система УК не должна обязательно обладать способностью производства ОО, но ей следует поддерживать этот процесс таким образом, который поможет уменьшить вероятность человеческой ошибки.

ИСО/МЭК 15408-3 ALC_CMC.4.6C: *Документация УК должна включать в себя план УК.*

12.2.4.3.8 Шаг оценивания ALC_CMC.4-8

Оценщик должен проверить, что представленная документация УК содержит план УК.

План УК не обязательно должен быть единым, связанным документом, но рекомендуется, чтобы имелся некий документ с описанием того, где представлены различные части плана УК. На тот случай, если план УК не является единым документом, в следующем шаге оценивания приведен список, содержащий подсказки по поводу его содержания.

ИСО/МЭК 15408-3 ALC_CMC.4.7C: *В плане УК должно быть описание того, каким образом система УК используется для разработки ОО.*

12.2.4.3.9 Шаг оценивания ALC_CMC.4-9

Оценщик должен исследовать план УК в целях вынесения заключения о том, что в нем описывается, каким образом система УК используется для разработки ОО.

Описания, содержащиеся в плане УК, могут включать:

a) все операции, выполняемые в среде разработки ОО, которые подчинены процедурам управления конфигурацией (например создание, модификация или удаление элемента конфигурации, создание резервной копии данных, архивация);

b) средства (например инструменты УК, формы) которые должны быть доступны;

c) использование инструментов УК: необходимые детальная информация для пользователя системы УК, чтобы он мог правильно управлять инструментами УК в целях поддержания целостности ОО;

d) процедуры поддержки производства;

e) описание того, какие еще объекты (компоненты разработки, инструменты, среда оценки и т. д.) взяты под управление системы УК;

f) роли и обязанности должностных лиц, требуемые для выполнения операций над отдельными элементами конфигурации (для различных типов элементов конфигурации (например проектная документация или исходный код) могут быть идентифицированы различные пользовательские роли);

g) описание того, каким образом введены и укомплектованы организационно-штатные единицы системы УК (например совет по управлению изменениями, рабочие группы контроля интерфейсов);

h) описание управления изменениями;

i) процедуры, которые используются для обеспечения того, чтобы только уполномоченные лица могли изменять элементы конфигурации;

j) процедуры, которые используются для исключения проблем параллелизма, возникающих в случае одновременного изменения элементов конфигурации;

k) свидетельство, которое генерируется в результате применения процедур. Например, при изменении элемента конфигурации система УК может зафиксировать описание изменения, ответственность за изменение, идентификацию всех затронутых элементов конфигурации, статус изменения (например «не завершено» или «завершено»), а также дату и время внесения изменения. Эта информация может быть занесена в журнал аудита произведенных изменений или в протокол контроля изменений;

l) подход к контролю версий и уникальной маркировке версий ОО (охватывающий, например выпуск исправлений («патчей») для операционных систем и последующее обнаружение их применения).

ИСО/МЭК 15408-3 ALC_CMC.4.8C: *План УК должен содержать описание процедур, используемых для приемки модифицированных или вновь созданных элементов конфигурации как части ОО.*

12.2.4.3.10 Шаг оценивания ALC_CMC.4-10

Оценщик должен исследовать план УК, чтобы сделать заключение, что в нём описываются процедуры, которые необходимо применять для приемки вновь созданных или модифицированных элементов конфигурации как части ОО.

В описание процедур приемки в плане УК следует включать описание ролей разработчиков или отдельных лиц, ответственных за приемку, а также критериев приемки. Следует учитывать все возможные при приемке ситуации:

a) первичную приемку элемента в систему УК, в особенности модулей программного, аппаратного и программно-аппаратного обеспечения других производителей в ОО («интеграция»);

b) перевод элементов конфигурации на следующий этап жизненного цикла для каждой стадии «сборки» ОО (например для модулей, подсистем и систем);

c) приемку при транспортировке между различными объектами, на которых производится разработка.

Если этот шаг оценивания применяется к зависимому компоненту, который собираются интегрировать в составной ОО, в плане УК следует учитывать управление базовыми компонентами, полученными от разработчика зависимого ОО.

При получении компонентов оценщики верифицируют следующее:

a) что передача каждого базового компонента от разработчика интегратору (разработчику зависимого ОО) осуществлялась в соответствии с процедурами безопасной поставки базового компонента ОО, как приводится в отчете о сертификации базового компонента;

b) что полученный компонент имеет такие же идентификаторы, как установлено в ЗБ и Отчете о сертификации ОО-компонента;

c) что предоставлены все дополнительные материалы, требуемые разработчиком для композиции (интеграции). К этому относится и необходимый фрагмент функциональной спецификации ОО-компонента.

ИСО/МЭК 15408-3 ALC_CMC.4.9C: *В свидетельствах должно быть продемонстрировано, что все элементы конфигурации сопровождаются системой УК.*

12.2.4.3.11 Шаг оценивания ALC_CMC.4-11

Оценщик должен проверить, что элементы конфигурации, идентифицированные в списке конфигурации, сопровождаются системой УК.

Следует, чтобы система УК, используемая разработчиком, поддерживала целостность ОО. Оценщику следует проверить, что для каждого типа элементов конфигурации (например проектная документация или модули исходного кода), содержащихся в списке элементов конфигурации, есть примеры свидетельств, которые являются результатами производимых процедур, описанных в плане УК. В этом случае подход к осуществлению выборки будет зависеть от степени детализации, используемой в системе УК для управления элементами УК. Там, где, например в списке элементов конфигурации идентифицировано 10 000 модулей исходного кода, должна быть применена иная стратегия осуществления выборки по сравнению с тем случаем, где идентифицировано только пять таких модулей или вовсе один. Деятельность в рамках данного шага оценивания следует в первую очередь направить на оценку того, правильно ли функционирует система УК, а не на обнаружение любой незначительной ошибки.

Руководство по выборке см. в приложении А.2 «Выборка».

ИСО/МЭК 15408-3 ALC_CMC.4.10C: *В свидетельствах должно быть продемонстрировано, что система УК функционирует в соответствии с планом УК.*

12.2.4.3.12 Шаг оценивания ALC_CMC.4-12

Оценщик должен проверить документацию УК, чтобы удостовериться, что она включает записи системы УК, определенные планом УК.

Следует, чтобы выходные материалы системы УК обеспечили свидетельство, необходимое оценщику для уверенности, что план УК применяется, а все элементы конфигурации поддерживаются системой УК, как это требуется в ALC_CMC.4.9C. Пример выходных материалов может включать формы контроля изменений или формы разрешения доступа к элементам конфигурации.

12.2.4.3.13 Шаг оценивания ALC_CMC.4-13

Оценщик должен исследовать свидетельство, чтобы сделать заключение, что система УК используется в соответствии с планом УК.

Оценщику следует осуществить и исследовать выборку из свидетельства, охватывающую каждый тип операций по УК, выполняемых над элементами конфигурации (например создание, модификация, удаление, возврат к более ранней версии), чтобы подтвердить, что все операции системы УК выполнялись в соответствии с документированными процедурами. Оценщик подтверждает, что свидетельство включает всю информацию, идентифицированную для этой операции в плане УК. При исследовании свидетельства может потребоваться доступ к используемым инструментальным средствам УК. Оценщику разрешается остановиться на выборочной проверке свидетельства.

Руководство по выборке см. в приложении А.2 «Выборка».

Дополнительная уверенность в правильном функционировании системы УК и эффективном сопровождении элементов конфигурации может быть получена посредством проведения интервью с отобранными для этого участниками разработки. При проведении подобных интервью оценщику следует стремиться получить более глубокое понимание практического применения системы УК, а также удостовериться, что процедуры УК применяются в соответствии с документацией УК. Отметим, что такие интервью следует проводить скорее в дополнение, а не вместо исследования документального свидетельства; при этом они могут и не потребоваться, если документальное свидетельство само по себе удовлетворяет требованиям. Тем не менее, учитывая широкую область применения плана УК, воз-

можно, что некоторые аспекты (например роли и обязанности) могут быть непонятны из одного только плана и протоколов УК. Это один из случаев, когда для разъяснения понадобится интервью.

Предполагается, что для поддержки этих действий оценщик посетит объект разработки.

Руководство по посещению объектов см. в приложении А.4 «Посещение объектов».

12.2.5 Подвид деятельности по оценке (ALC_CMC.5)

12.2.5.1 Цели

Цели этого подвида деятельности состоят в том, чтобы сделать заключение, идентифицировал ли разработчик ОО и связанные с ним элементы конфигурации однозначно и четко, а также организовано ли управление возможностями изменения этих элементов правильно с использованием автоматизированных инструментов, позволяющих сделать систему УК менее восприимчивой к человеческим ошибкам и ошибкам, допущенным по небрежности.

12.2.5.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) ЗБ;

b) ОО, пригодный для тестирования;

c) документация по управлению конфигурацией.

12.2.5.3 Действие ALC_CMC.5.1E

ИСО/МЭК 15408-3 ALC_CMC.5.1C: *ОО должен быть помечен уникальной маркировкой.*

12.2.5.3.1 Шаг оценивания ALC_CMC.5-1

Оценщик должен проверить, что ОО, представленный для оценки, имеет собственную маркировку.

Оценщику следует удостовериться, что ОО содержит уникальную маркировку, позволяющую отличать разные версии ОО. Этого можно достичь, используя маркированную упаковку или носители, или же маркировку, отображаемую ОО при функционировании. Это предоставляет потребителю возможность идентификации ОО (например при приобретении или использовании).

ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, ОО, являющийся программным продуктом, может отображать свое название и номер версии при запуске программы или в ответ на запрос через командную строку. Аппаратный или программно-аппаратный ОО может быть идентифицирован путем нанесения на нем соответствующего номера штампом.

Возможен и альтернативный вариант, когда уникальная маркировка ОО представляет собой комбинацию уникальных маркировок каждого компонента, из которых состоит ОО (например в случае составного ОО).

12.2.5.3.2 Шаг оценивания ALC_CMC.5-2

Оценщик должен проверить непротиворечивость используемой маркировки ОО.

Если ОО маркирован несколько раз, то необходима согласованность меток. Например, следует предусмотреть возможность связать любое маркированное руководство, поставляемое в составе ОО, с оцененным функционирующим ОО. Этим обеспечивается уверенность потребителя в том, что он приобрел оцененную версию ОО, установил эту же версию и располагает надлежащей редакцией руководства, необходимой для эксплуатации данного ОО в соответствии с его ЗБ.

Оценщик также верифицирует, что маркировка ОО согласуется с ЗБ.

Если этот шаг оценивания будет применяться к составному ОО, то применимо следующее. Составной ОО ИТ не будет маркирован уникальной (составной) маркировкой; только отдельные его компоненты будут соответственно маркированы. Для этого требуется маркировать дальнейшую разработку ОО ИТ, например во время запуска и/или функционирования составной маркировкой. Если составной ОО будет поставляться как часть целого, состоящего из ОО-компонентов, то компоненты ОО не будут маркированы составной маркировкой. Однако в ЗБ составного ОО будет включена уникальная маркировка составного ОО, а также будут идентифицированы компоненты, включенные в составной ОО, благодаря чему потребители будут в состоянии сделать заключение о том, имеются ли у них соответствующие компоненты.

ИСО/МЭК 15408-3 ALC_CMC.5.2C: *В документации УК должно содержаться описание метода, используемого для уникальной идентификации элементов конфигурации.*

12.2.5.3.3 Шаг оценивания ALC_CMC.5-3

Оценщик должен исследовать метод идентификации элементов конфигурации, чтобы сделать заключение о том, что в нем описано, каким образом уникально идентифицирован каждый элемент конфигурации.

В процедурах следует описать, каким образом состояние каждого элемента конфигурации может быть прослежено на любом этапе жизненного цикла ОО. Процедуры такого прослеживания могут быть

детально описаны в плане УК или по всей документации УК. В эту информацию следует включать описание:

a) метода уникальной идентификации элементов, такой, что есть возможность отследить версии конкретного элемента конфигурации;

b) метода назначения уникальных идентификаторов элементам конфигурации и метода их введения в систему УК;

c) метода, который будет использоваться для идентификации новых версий элементов конфигурации, замещающих старые.

ИСО/МЭК 15408-3 ALC_CMC.5.3C: В *документации по УК должно быть обоснование того, что процедуры приемки предоставляют рациональный и приемлемый обзор изменений всех элементов конфигурации.*

12.2.5.3.4 Шаг оценивания ALC_CMC.5-4

Оценщик должен исследовать документацию УК, чтобы сделать заключение о том, что в ней есть обоснование того, что процедуры приемки *предоставляют рациональный и приемлемый обзор изменений всех элементов конфигурации.*

Документация по УК должна сделать достаточно ясным тот факт, что при выполнении процедур приемки только части соответствующего качества включаются в состав ОО.

ИСО/МЭК 15408-3 ALC_CMC.5.4C: *В системе УК должны быть уникально идентифицированы все элементы конфигурации.*

12.2.5.3.5 Шаг оценивания ALC_CMC.5-5

Оценщик должен исследовать элементы конфигурации, чтобы сделать заключение о том, что они идентифицированы способом, который не противоречит документации УК.

Доверие тому, что система УК уникально идентифицирует все элементы конфигурации, получается путем исследования идентификаторов для элементов конфигурации. И для элементов конфигурации, которые включены в ОО, и для проектов элементов конфигурации, которые предоставлены разработчиком как свидетельства оценки, оценщик подтверждает, что каждый элемент конфигурации обладает уникальным идентификатором, присвоенным ему способом, совместимым с методом уникальной идентификации, описанным в документации по УК.

ИСО/МЭК 15408-3 ALC_CMC.5.5C: *В системе УК должны быть предусмотрены такие автоматизированные меры, при применении которых в элементах конфигурации могут быть сделаны только санкционированные изменения.*

12.2.5.3.6 Шаг оценивания ALC_CMC.5-6

Оценщик должен исследовать меры контроля доступа в УК, описанные в плане УК (см. ALC_CMC.5.12C), чтобы сделать заключение, что они автоматизированы и эффективны для предотвращения несанкционированного доступа к элементам конфигурации.

Оценщик может использовать несколько методов для вынесения заключения об эффективности мер контроля доступа в УК. Например, оценщик может опробовать меры контроля доступа, чтобы удостовериться, что процедуры нельзя обойти. Оценщик может использовать выходные материалы, сгенерированные процедурами системы УК, требуемые на шаге оценивания ALC_CMC.5-16C. Оценщику может быть также продемонстрирована система УК, чтобы он убедился, что используемые меры контроля доступа выполняются эффективно.

ИСО/МЭК 15408-3 ALC_CMC.5.6C: *Система УК должна поддерживать производство ОО автоматизированными средствами.*

12.2.5.3.7 Шаг оценивания ALC_CMC.5-7

Оценщик должен проверить план УК (см. ALC_CMC.5.12C) для оценки автоматизированных процедур, предназначенных для поддержки производства ОО.

Термин «производство» применяется по отношению к процессам, принятым разработчиком для перевода ОО от представления реализации до состояния, приемлемого для поставки конечному потребителю.

Оценщик проверяет существование автоматизированных процедур поддержки производства ОО в рамках плана УК.

Примеры автоматизированных средств поддержки производства ОО:

- инструмент «создать» (предусмотренный во многих средствах разработки программного обеспечения) для случая ОО, являющегося программным продуктом;

- инструмент, автоматически обеспечивающий (например посредством штрих-кодов) комбинирование только тех частей, которые должны быть интегрированы для случая аппаратного ОО.

12.2.5.3.8 Шаг оценивания ALC_CMC.5-8

Оценщик должен исследовать процедуры, поддерживающие производство ОО, чтобы сделать заключение о том, что они эффективны для приобретения доверия, что сгенерированный ОО отражает представление его реализации.

В процедурах поддержки производства следует описать, какие инструменты должны использоваться для производства заключительной версии ОО из представления реализации полностью определенным способом. Соглашения, директивы и другие необходимые логические конструкции описаны в семействе ALC_TAT.

Оценщик делает заключение о том, что при выполнении процедур поддержки производства ОО используются корректные элементы конфигурации. Например, в случае, когда ОО является программным обеспечением, это может включать проверку того, что автоматизированные производственные процедуры обеспечивают включение в компилированный объектный код всех исходных файлов и связанных с ними библиотек. Кроме того, процедурами следует обеспечивать уникальное определение опций компилятора и других сопоставимых опций. Для аппаратных ОО в этот шаг оценивания может быть включена проверка того, что автоматизированные производственные процедуры предоставляют уверенность в том, что принадлежащие ОО части собраны вместе, и нет недостающих частей.

Клиент может в этом случае быть уверен, что версия ОО, поставленного для установки, получена из представления реализации однозначным способом и осуществляет ФТБ согласно описанию в ЗБ.

Оценщику следует учитывать, что система УК не должна обязательно обладать способностью производства ОО, но ей следует поддерживать этот процесс таким образом, который поможет уменьшить вероятность человеческой ошибки.

ИСО/МЭК 15408-3 ALC_CMC.5.7C: *Система УК должна обеспечивать, что лицо, ответственное за приемку элемента конфигурации в УК, не является разработчиком этого элемента.*

12.2.5.3.9 Шаг оценивания ALC_CMC.5-9

Оценщик должен исследовать систему УК, чтобы сделать заключение о том, что она обеспечивает, что лицо, ответственное за приемку элемента конфигурации в УК, не является разработчиком этого элемента.

Процедуры приемки описывают, кто ответственен за приемку в систему элемента конфигурации. На основании этих описаний оценщику следует быть в состоянии сделать заключение о том, что лицо, которое приняло данный элемент конфигурации, ни в коем случае не является его разработчиком.

ИСО/МЭК 15408-3 ALC_CMC.5.8C: *В системе УК должны быть идентифицированы элементы конфигурации, которые составляют ФБО.*

12.2.5.3.10 Шаг оценивания ALC_CMC.5-10

Оценщик должен исследовать систему УК, чтобы сделать заключение о том, что она идентифицирует элементы конфигурации, которые составляют ФБО.

В документации УК следует описать, каким образом система УК идентифицирует элементы конфигурации, составляющие ФБО. Оценщику следует осуществить выборку элементов конфигурации для охвата всех типов элементов, а особенно содержащих элементы ФБО и не-ФБО, и проверить, что все они правильно классифицированы системой УК.

Руководство по выборке см. в приложении А.2 «Выборка».

ИСО/МЭК 15408-3 ALC_CMC.5.9C: *Система УК должна поддерживать аудит всех изменений ОО автоматизированными средствами с указанием пользователя, инициирующего изменение, а также даты и времени изменения в журнале аудита.*

12.2.5.3.11 Шаг оценивания ALC_CMC.5-11

Оценщик должен исследовать систему УК, чтобы сделать заключение о том, что она поддерживает аудит всех изменений ОО автоматизированными средствами с указанием пользователя, инициирующего изменение, а также даты и времени изменения в журнале аудита.

Оценщику следует проверить выборку журналов аудита на предмет наличия в них минимального требуемого объема информации.

ИСО/МЭК 15408-3 ALC_CMC.5.10C: *Система УК должна предоставить автоматизированное средство идентификации всех других элементов конфигурации, на которых оказывает влияние изменение данного элемента конфигурации.*

12.2.5.3.12 Шаг оценивания ALC_CMC.5-12

Оценщик должен исследовать систему УК, чтобы сделать заключение о том, что она предоставляет автоматизированное средство идентификации всех других элементов конфигурации, на которых оказывает влияние изменение данного элемента конфигурации.

В документации УК следует описать, каким образом система УК идентифицирует все другие элементы конфигурации, которые затронуты изменением данного пункта конфигурации. Оценщику следует осуществить выборку элементов конфигурации для охвата всех типов элементов и опробовать автоматизированные средства для того, чтобы сделать заключение, идентифицируют ли эти средства все элементы, которые затрагиваются изменением выбранного элемента.

Руководство по выборке см. в приложении А.2 «Выборка».

ИСО/МЭК 15408-3 ALC_CMC.5.11C: *Система УК должна быть в состоянии идентифицировать версию представления реализации, на основании которой сгенерирован ОО.*

12.2.5.3.13 Шаг оценивания ALC_CMC.5-13

Оценщик должен исследовать систему УК, чтобы сделать заключение о том, что она может идентифицировать версию представления реализации, на основании которой сгенерирован ОО.

В документации УК следует описать, каким образом система УК идентифицирует версию представления реализации, на основании которой генерируется ОО. Оценщику следует осуществить выборку частей, используемых для производства ОО и применить систему УК для проверки того, что она идентифицирует соответствующую версию представления реализации.

Руководство по выборке см. в приложении А.2 «Выборка».

ИСО/МЭК 15408-3 ALC_CMC.5.12C: *Документация УК должна включать в себя план УК.*

12.2.5.3.14 Шаг оценивания ALC_CMC.5-14

Оценщик должен проверить, что представленная документация УК содержит план УК.

План УК не обязательно должен быть единым, связанным документом, но рекомендуется, чтобы имелся некий документ с описанием того, где представлены различные части плана УК. На тот случай, если план УК не является единым документом, в следующем шаге оценивания приведен список, содержащий подсказки по поводу его содержания.

ИСО/МЭК 15408-3 ALC_CMC.5.13C: *В плане УК должно содержаться описание того, каким образом система УК используется для разработки ОО.*

12.2.5.3.15 Шаг оценивания ALC_CMC.5-15

Оценщик должен исследовать план УК в целях вынесения заключения о том, что в нем описывается, каким образом система УК используется для разработки ОО.

Описания, содержащиеся в плане УК, могут включать:

a) все операции, выполняемые в среде разработки ОО, которые подчинены процедурам управления конфигурацией (например создание, модификация или удаление элемента конфигурации, создание резервной копии данных, архивация);

b) средства (например инструменты УК, формы), которые должны быть доступны;

c) использование инструментов УК: необходимая детальная информация для пользователя системы УК, чтобы он мог правильно управлять инструментами УК в целях поддержания целостности ОО;

d) процедуры поддержки производства;

e) описание того, какие еще объекты (компоненты разработки, инструменты, среда оценки и т. д.) взяты под управление системы УК;

f) роли и обязанности должностных лиц, требуемые для выполнения операций над отдельными элементами конфигурации (для различных типов элементов конфигурации (например проектная документация или исходный код) могут быть идентифицированы различные пользовательские роли);

g) описание того, каким образом введены и укомплектованы организационно-штатные единицы системы УК (например совет по управлению изменениями, рабочие группы контроля интерфейсов);

h) описание управления изменениями;

i) процедуры, которые используются для обеспечения того, чтобы только уполномоченные лица могли изменять элементы конфигурации;

j) процедуры, которые используются для исключения проблем параллелизма, возникающих в случае одновременного изменения элементов конфигурации;

k) свидетельство, которое генерируется в результате применения процедур. Например, при изменении элемента конфигурации система УК может зафиксировать описание изменения, ответственность за изменение, идентификацию всех затронутых элементов конфигурации, статус изменения (например «не завершено» или «завершено»), а также дату и время внесения изменения. Эта информация может быть занесена в журнал аудита произведенных изменений или в протокол контроля изменений;

l) подход к контролю версий и уникальной маркировке версий ОО (охватывающий, например выпуск исправлений («патчей») для операционных систем и последующее обнаружение их применения).

ИСО/МЭК 15408-3 ALC_CMC.5.14C: *План УК должен содержать описание процедур, используемых для приемки модифицированных или вновь созданных элементов конфигурации как части ОО.*

12.2.5.3.16 Шаг оценивания ALC_CMC.5-16

Оценщик должен исследовать план УК, чтобы сделать заключение, что в нём описываются процедуры, которые необходимо применять для приемки вновь созданных или модифицированных элементов конфигурации как части ОО.

В описание процедур приемки в плане УК следует включать описание ролей разработчиков или отдельных лиц, ответственных за приемку, а также критериев приемки. Следует учитывать все возможные при приемке ситуации:

a) первичную приемку элемента в систему УК, в особенности модулей программного, аппаратного и программно-аппаратного обеспечения других производителей в ОО (интеграция);

b) перевод элементов конфигурации на следующий этап жизненного цикла для каждой стадии сборки ОО (например для модулей, подсистем и систем);

c) приемку при транспортировке между различными объектами, на которых производится разработка.

ИСО/МЭК 15408-3 ALC_CMC.5.15C: *В свидетельствах должно быть продемонстрировано, что все элементы конфигурации сопровождаются системой УК.*

12.2.5.3.17 Шаг оценивания ALC_CMC.5-17

Оценщик должен проверить, что элементы конфигурации, идентифицированные в списке конфигурации, сопровождаются системой УК.

Следует, чтобы система УК, используемая разработчиком, поддерживала целостность ОО. Оценщику следует проверить, что для каждого типа элементов конфигурации (например для проектной документации или модулей исходного кода), содержащихся в списке элементов конфигурации, есть примеры свидетельств, которые являются результатами производимых процедур, описанных в плане УК. В этом случае подход к осуществлению выборки будет зависеть от степени детализации, используемой в системе УК для управления элементами УК. Там, где, например в списке элементов конфигурации идентифицировано 10 000 модулей исходного кода, должна быть применена иная стратегия осуществления выборки по сравнению с тем случаем, где идентифицировано только пять таких модулей или вовсе один. Деятельность в рамках данного шага оценивания следует в первую очередь направить на оценку того, правильно ли функционирует система УК, а не на обнаружение любой незначительной ошибки.

Руководство по выборке см. в приложении А.2 «Выборка».

ИСО/МЭК 15408-3 ALC_CMC.5.16C: *В свидетельствах должно быть продемонстрировано, что система УК функционирует в соответствии с планом УК.*

12.2.5.3.18 Шаг оценивания ALC_CMC.5-18

Оценщик должен проверить документацию УК, чтобы удостовериться, что она включает записи системы УК, определенные планом УК.

Следует, чтобы выходные материалы системы УК обеспечили свидетельство, необходимое оценщику для уверенности, что план УК применяется, а все элементы конфигурации поддерживаются системой УК, как это требуется в ALC_CMC.5.15C. Пример выходных материалов может включать формы контроля изменений или формы разрешения доступа к элементам конфигурации.

12.2.5.3.19 Шаг оценивания ALC_CMC.5-19

Оценщик должен исследовать свидетельство, чтобы сделать заключение, что система УК используется в соответствии с планом УК.

Оценщику следует осуществить и исследовать выборку из свидетельства, охватывающую каждый тип операций по УК, выполняемых над элементами конфигурации (например создание, модификацию, удаление, возврат к более ранней версии), чтобы подтвердить, что все операции системы УК выполнялись в соответствии с задокументированными процедурами. Оценщик подтверждает, что свидетельство включает всю информацию, идентифицированную для этой операции в плане УК. При исследовании свидетельства может потребоваться доступ к используемым инструментальным средствам УК. Оценщику разрешается остановиться на выборочной проверке свидетельства.

Руководство по выборке см. в приложении А.2 «Выборка».

Дополнительное доверие правильному функционированию системы УК и эффективному сопровождению элементов конфигурации может быть получено посредством проведения интервью с выбранными для этого участниками разработки. При проведении подобных интервью оценщику следует стремиться получить более глубокое понимание практического применения системы УК, а также удостовериться, что процедуры УК применяются в соответствии с документацией УК. Отметим, что такие интервью следует проводить скорее в дополнение, а не вместо исследования документального свиде-

тельства; при этом они могут и не потребоваться, если документальное свидетельство само по себе удовлетворяет требованиям. Тем не менее, учитывая широкую область применения плана УК, возможно, что некоторые аспекты (например роли и обязанности) могут быть непонятны из одного только плана и протоколов УК. Это один из случаев, когда для разъяснения понадобится интервью.

Предполагается, что для поддержки этих действий оценщик посетит объект разработки.

Руководство по посещению объектов см. в приложении А.4 «Посещение объектов».

12.2.5.4 Действие ALC_CMC.5.2E

12.2.5.4.1 Шаг оценивания ALC_CMC.5-20

Оценщик должен исследовать процедуры поддержки производства, чтобы сделать заключение о том, что при выполнении этих процедур ОО будет произведен таким же образом, как образец ОО, предоставленный разработчиком оценщику для тестирования.

Если ОО — небольшой программный продукт, и производство состоит из процедур компилирования и объединения, оценщик может подтвердить достаточность процедур поддержки производства путем повторного их применения.

Если производственный процесс ОО более сложен (например в случае производства смарт-карты), но уже начался, оценщику следует оценить применение процедур поддержки производства во время посещения объекта разработки. Он может сравнить копию ОО, произведенную в его присутствии, с образцами, используемыми для тестирования.

Руководство по посещению объектов см. в приложении А.4 «Посещение объектов».

В ином случае заключение оценщика рекомендуется основывать на письменном свидетельстве, предоставленном разработчиком.

Этот шаг оценивания может быть выполнен вместе с действиями по оценке семейства «Представление реализации» (ADV_IMP).

12.3 Область УК (ALC_CMS)

12.3.1 Подвид деятельности по оценке (ALC_CMS.1)

12.3.1.1 Цели

Цель данного подвида деятельности — сделать заключение, выполняет ли разработчик управление конфигурацией ОО и свидетельствами оценки. Этими элементами конфигурации управляют в соответствии с семейством «Возможности УК» (ALC_CMC).

12.3.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) список элементов конфигурации.

12.3.1.3 Действие ALC_CMS.1.1E

ИСО/МЭК 15408-3 ALC_CMS.1.1C: *Список элементов конфигурации должен включать следующее: сам ОО и свидетельства оценки, необходимые по ТДБ в ЗБ.*

12.3.1.3.1 Шаг оценивания ALC_CMS.1-1

Оценщик должен проверить, что список элементов конфигурации содержит следующий набор элементов:

a) сам ОО;

b) свидетельства оценки, необходимые по требованиям доверия к безопасности в ЗБ.

ИСО/МЭК 15408-3 ALC_CMS.1.2C: *Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.*

12.3.1.3.2 Шаг оценивания ALC_CMS.1-2

Оценщик должен исследовать список элементов конфигурации, чтобы сделать заключение о том, что он уникально идентифицирует каждый элемент конфигурации.

Список элементов конфигурации содержит достаточную информацию, чтобы уникально идентифицировать, какая версия каждого элемента использовалась (как правило, для этого достаточно номера версии). Использование этого списка позволит оценщику проверить, что во время проведения оценки использовались правильные элементы конфигурации и правильная версия каждого элемента.

12.3.2 Подвид деятельности по оценке (ALC_CMS.2)

12.3.2.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, включает ли список элементов конфигурации сам ОО, его составные части и необходимые свидетельства оценки. Этими пунктами конфигурации управляют в соответствии с семейством «Возможности УК» (ALC_CMC).

12.3.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) список элементов конфигурации.

12.3.2.3 Действие ALC_CMS.2.1E

ИСО/МЭК 15408-3 ALC_CMS.2.1C: *Список элементов конфигурации должен включать следующее: сам ОО и свидетельства оценки, необходимые по требованиям доверия к безопасности, а также части, которые входят в состав ОО.*

12.3.2.3.1 Шаг оценивания ALC_CMS.2-1

Оценщик должен проверить, что список конфигурации включает следующий набор элементов:

a) сам ОО;

b) его составные части;

c) свидетельства оценки, необходимые по ТДБ.

ИСО/МЭК 15408-3 ALC_CMS.2.2C: *Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.*

12.3.2.3.2 Шаг оценивания ALC_CMS.2-2

Оценщик должен исследовать список элементов конфигурации, чтобы сделать заключение о том, что он уникально идентифицирует каждый элемент конфигурации.

Список элементов конфигурации содержит достаточную информацию, чтобы уникально идентифицировать, какая версия каждого элемента использовалась (как правило, для этого достаточно номера версии). Использование этого списка позволит оценщику проверить, что во время проведения оценки использовались правильные элементы конфигурации и правильная версия каждого элемента.

ИСО/МЭК 15408-3 ALC_CMS.2.3C: *Для каждого значимого для ФБО элемента конфигурации в списке элементов конфигурации должен быть указан разработчик.*

12.3.2.3.3 Шаг оценивания ALC_CMS.2-3

Оценщик должен проверить, что в списке элементов конфигурации указан разработчик каждого соответствующего элемента конфигурации ФБО.

Если в разработке ОО участвует только один разработчик, то этот шаг оценивания не применим и потому считается удовлетворенным.

12.3.3 Подвид деятельности по оценке (ALC_CMS.3)

12.3.3.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, включает ли список элементов конфигурации сам ОО, его составные части, представление реализации и необходимые свидетельства оценки. Этими пунктами конфигурации управляют в соответствии с семейством «Возможности УК» (ALC_CMC).

12.3.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) список элементов конфигурации.

12.3.3.3 Действие ALC_CMS.3.1E

ИСО/МЭК 15408-3 ALC_CMS.3.1C: *Список элементов конфигурации должен включать следующее: сам ОО и свидетельства оценки, необходимые по требованиям доверия к безопасности, части, которые входят в состав ОО, а также представление реализации.*

12.3.3.3.1 Шаг оценивания ALC_CMS.3-1

Оценщик должен проверить, что список конфигурации включает следующий набор элементов:

a) сам ОО;

b) его составные части;

c) представление реализации ОО;

d) свидетельства оценки, необходимые по ТДБ в ЗБ.

ИСО/МЭК 15408-3 ALC_CMS.3.2C: *Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.*

12.3.3.3.2 Шаг оценивания ALC_CMS.3-2

Оценщик должен исследовать список элементов конфигурации, чтобы сделать заключение о том, что он уникально идентифицирует каждый элемент конфигурации.

Список элементов конфигурации содержит достаточную информацию, чтобы уникально идентифицировать, какая версия каждого элемента использовалась (как правило, для этого достаточно номера версии). Использование этого списка позволит оценщику проверить, что во время проведения оценки использовались правильные элементы конфигурации и правильная версия каждого элемента.

ИСО/МЭК 15408-3 ALC_CMS.3.3C: *Для каждого значимого для ФБО элемента конфигурации в списке элементов конфигурации должен быть указан разработчик.*

12.3.3.3.3 Шаг оценивания ALC_CMS.3-3

Оценщик должен проверить, что в списке элементов конфигурации указан разработчик каждого соответствующего элемента конфигурации ФБО.

Если в разработке ОО участвует только один разработчик, то этот шаг оценивания не применим и потому считается удовлетворенным.

12.3.4 Подвид деятельности по оценке (ALC_CMS.4)

12.3.4.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, включает ли список элементов конфигурации сам ОО, его составные части, представление реализации, недостатки защиты и необходимые свидетельства оценки. Этими пунктами конфигурации управляют в соответствии с семейством «Возможности УК» (ALC_CMC).

12.3.4.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) список элементов конфигурации.

12.3.4.3 Действие ALC_CMS.4.1E

ИСО/МЭК 15408-3 ALC_CMS.4.1C: *Список элементов конфигурации должен включать следующее: сам ОО; свидетельства оценки, необходимые по требованиям доверия к безопасности; представление реализации; сведения о недостатках безопасности и стадии их устранения.*

12.3.4.3.1 Шаг оценивания ALC_CMS.4-1

Оценщик должен проверить, что список конфигурации включает следующий набор элементов:

a) сам ОО;

b) его составные части;

c) представление реализации ОО;

d) свидетельства оценки, необходимые по ТДБ в ЗБ;

e) документацию, используемую для записи детальных сведений о недостатках безопасности, связанных с реализацией проекта ОО (например отчеты о стадии устранения проблемы, полученные из базы данных разработчика о проблемах).

ИСО/МЭК 15408-3 ALC_CMS.4.2C: *Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.*

12.3.4.3.2 Шаг оценивания ALC_CMS.4-2

Оценщик должен исследовать список элементов конфигурации, чтобы сделать заключение о том, что он уникально идентифицирует каждый элемент конфигурации.

Список элементов конфигурации содержит достаточную информацию, чтобы уникально идентифицировать, какая версия каждого элемента использовалась (как правило, для этого достаточно номера версии). Использование этого списка позволит оценщику проверить, что во время проведения оценки использовались правильные элементы конфигурации и правильная версия каждого элемента.

ИСО/МЭК 15408-3 ALC_CMS.4.3C: *Для каждого значимого для ФБО элемента конфигурации в списке элементов конфигурации должен быть указан разработчик.*

12.3.4.3.3 Шаг оценивания ALC_CMS.4-3

Оценщик должен проверить, что в списке элементов конфигурации указан разработчик каждого соответствующего элемента конфигурации ФБО.

Если в разработке ОО участвует только один разработчик, то этот шаг оценивания не применим и потому считается удовлетворенным.

12.3.5 Подвид деятельности по оценке (ALC_CMS.5)

12.3.5.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, включает ли список элементов конфигурации сам ОО, его составные части, представление реализации, недостатки защиты, средства разработки и связанную с ними информацию, а также необходимые свидетельства оценки. Этими пунктами конфигурации управляют в соответствии с семейством «Возможности УК» (ALC_CMC).

12.3.5.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) список элементов конфигурации.

12.3.5.3 Действие ALC_CMS.5.1E

ИСО/МЭК 15408-3 ALC_CMS.5.1C: *Список элементов конфигурации должен включать следующее: сам ОО; составные части ОО; представление реализации; сведения о недостатках безопасности и стадии их устранения; инструментальные средства разработки и связанную с ними информацию, а также свидетельства оценки, необходимые по требованиям доверия к безопасности.*

12.3.5.3.1 Шаг оценивания ALC_CMS.5-1

Оценщик должен проверить, что список конфигурации включает следующий набор элементов:

a) сам ОО;

b) его составные части;

c) представление реализации ОО;

d) свидетельства оценки, необходимые по ТДБ в ЗБ;

e) документацию, используемую для записи детальных сведений о недостатках безопасности, связанных с реализацией проекта ОО (например отчеты о стадии устранения проблемы, полученные из базы данных разработчика о проблемах);

f) все инструменты (включая программное обеспечение для тестирования, если это применимо), используемые в разработке и производстве ОО, с указанием наименования, версии, конфигурации, роли каждого инструмента разработки, а также связанную с ними документацию.

ИСО/МЭК 15408-3 ALC_CMS.5.2C: *Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.*

12.3.5.3.2 Шаг оценивания ALC_CMS.5-2

Оценщик должен исследовать список элементов конфигурации, чтобы сделать заключение о том, что он уникально идентифицирует каждый элемент конфигурации.

Список элементов конфигурации содержит достаточную информацию, чтобы уникально идентифицировать, какая версия каждого элемента использовалась (как правило, для этого достаточно номера версии). Использование этого списка позволит оценщику проверить, что во время проведения оценки использовались правильные элементы конфигурации и правильная версия каждого элемента.

ИСО/МЭК 15408-3 ALC_CMS.5.3C: *Для каждого значимого для ФБО элемента конфигурации в списке элементов конфигурации должен быть указан разработчик.*

12.3.5.3.3 Шаг оценивания ALC_CMS.5-3

Оценщик должен проверить, что в списке элементов конфигурации указан разработчик каждого соответствующего элемента конфигурации ФБО.

Если в разработке ОО участвует только один разработчик, то этот шаг оценивания не применим и потому считается удовлетворенным.

12.4 Поставка (ALC_DEL)

12.4.1 Подвид деятельности по оценке (ALC_DEL.1)

12.4.1.1 Цели

Цель данного подвида деятельности — сделать заключение, описаны ли в документации поставки все процедуры, применяемые для поддержания безопасности ОО.

12.4.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) документация поставки.

12.4.1.3 Действие ALC_DEL.1.1E

ИСО/МЭК 15408-3 ALC_DEL.1.1C: *Документация поставки должна содержать описание всех процедур, необходимых для поддержания безопасности при распространении версий ОО потребителю.*

12.4.1.3.1 Шаг оценивания ALC_DEL.1-1

Оценщик должен исследовать документацию поставки, чтобы сделать заключение, описаны ли в ней все процедуры, необходимые для поддержания безопасности при рассылке версий ОО или его компонентов потребителям.

Документация поставки описывает надлежащие процедуры для определения идентификации ОО и поддержания целостности ОО или его составных частей во время пересылки.

В документации поставки следует охватывать весь ОО, но она может содержать различные процедуры для различных частей ОО. При оценке следует рассмотреть все возможные процедуры.

Процедуры поставки следует применять на всех стадиях поставки от среды производства до среды установки (например при упаковке, хранении и рассылке). Может оказаться приемлемой стандарт-

ная коммерческая практика упаковки и поставки. Она предусматривает упаковку в пластиковую пленку, применение ленты безопасности или запечатанного конверта. Для рассылки могут применяться как процедуры для распространения физических копий (например с использованием общедоступной почты или частной службы доставки), так и для рассылки в электронном виде (например письмом электронной почты или при загрузке из сети Интернет).

Для обеспечения того, что попытка вмешательства или атаки типа «маскарад» будет обнаружена, разработчик может использовать криптографическую контрольную сумму или электронно-цифровую подпись. Кроме того, печати для защиты от вмешательства могут служить и как средство обнаружения нарушения конфиденциальности. Для программных ОО конфиденциальность может обеспечить использование средств шифрования. Если же основной проблемой является обеспечение доступности, то может потребоваться защита при транспортировке.

При интерпретации термина «необходимые» требуется учитывать:

a) природу ОО (то есть является ли он программным или аппаратным продуктом);

b) общий уровень безопасности для данного ОО, указанный на основании выбранного уровня при оценке уязвимостей. Если требуется, чтобы ОО в предполагаемой среде функционирования противостоял атакам нарушителей, обладающих определенным потенциалом нападения, это требование следует применять и на этапе поставки. Оценщику следует сделать заключение о сбалансированности выбранного подхода, при котором поставка не является очевидно слабым звеном по отношению к безопасному в остальном процессу разработки;

c) цели безопасности, содержащиеся в ЗБ. Особое внимание в документации поставки будет, скорее всего, уделено обеспечению целостности, т.к целостность ОО всегда очень важна. Однако для некоторых ОО при поставке важно и обеспечение конфиденциальности и доступности; процедуры, относящиеся к данным аспектам безопасной поставки, следует также рассмотреть в документации.

12.4.1.4 Подразумеваемое действие оценщика

ИСО/МЭК 15408-3 ALC_DEL.1.2D: *Разработчик должен использовать процедуры поставки.*

12.4.1.4.1 Шаг оценивания ALC_DEL.1-2

Оценщик должен исследовать аспекты процесса поставки, чтобы сделать заключение о применении процедур поставки.

Подход, предпринятый оценщиком для проверки применения процедур поставки, будет зависеть от природы ОО и самого процесса поставки. В дополнение к исследованию собственно процедур, оценщику следует приобрести и доверие их фактическому практическому применению. Некоторые возможные подходы перечислены ниже.

a. Посещение объекта (объектов) рассылки, где можно наблюдать практическое применение процедур.

b. Исследование ОО на некоторой стадии поставки или после передачи пользователю (например проверка наличия печатей для защиты от вмешательства).

c. Наблюдение за практическим выполнением процесса при получении ОО оценщиком по обычным каналам.

d. Опрос конечных пользователей о том, как им поставлен ОО.

Руководство по посещению объектов см. в приложении А.4 «Посещение объектов».

Для только что разработанного ОО возможно, что процедуры поставки еще необходимо отработать. В подобных случаях оценщику придется удовлетвориться тем, что имеются соответствующие процедуры и средства выполнения предстоящих поставок, и что весь привлекаемый персонал знает свои обязанности. Оценщик может запросить «пробный прогон» поставки, если это практически осуществимо. Если разработчик производит другие подобные продукты, то для приобретения доверия может быть полезно исследовать процедуры при их применении.

12.5 Безопасность разработки (ALC_DVS)

12.5.1 Подвид деятельности по оценке (ALC_DVS.1)

12.5.1.1 Цели

Цель данного подвида деятельности — сделать заключение, являются ли меры и средства контроля безопасности в среде разработки достаточными для обеспечения конфиденциальности и целостности проекта и реализации ОО. Это необходимо для обеспечения того, чтобы безопасная эксплуатация ОО не была скомпрометирована.

12.5.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) документация по безопасности разработки.

Кроме того, оценщику может понадобиться исследование других поставок, чтобы сделать заключение о том, что меры и средства контроля безопасности полностью определены и применяются. В частности, оценщику может понадобиться исследование документации разработчика по управлению конфигурацией (исходные данные подвидов деятельности ACM_CAP.4 «Поддержка производства, процедуры приемки» и ACM_SCP.2 «Охват УК отслеживания проблем»). Также требуется свидетельство применения процедур.

12.5.1.3 Действие ALC_DVS.1.1E

ИСО/МЭК 15408-3 ALC_DVS.1.1C: *Документация по безопасности разработки должна содержать описание всех физических, процедурных, организационных и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта ОО и его реализации в среде разработки.*

12.5.1.3.1 Шаг оценивания ALC_DVS.1-1

Оценщик должен исследовать документацию по безопасности разработки, чтобы сделать заключение, содержит ли она подробное описание всех используемых в среде разработки мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта и реализации ОО.

Оценщик определяет, какая информация из ЗБ нужна в первую очередь при вынесении заключения о необходимой защите.

Если в ЗБ не имеется такой информации в явном виде, оценщику нужно будет принять решение о необходимых мерах, основываясь на рассмотрении предполагаемой среды для ОО. В тех случаях, когда меры разработчика признаются недостаточными, рекомендуется, чтобы было представлено четкое и логическое обоснование для оценки уязвимостей, потенциально пригодных для использования.

При исследовании документации оценщиком рассматриваются следующие типы мер безопасности:

a) *физические*, например средства управления физическим доступом, применяемые для предотвращения несанкционированного доступа к среде разработки ОО (в рабочие часы и в другое время);

b) *процедурные*, например распространяющиеся на:

- предоставление доступа к среде разработки или к конкретным объектам среды, таким как оборудование разработки;
- отмену прав доступа лиц при их исключении из состава разработчиков;
- передачу защищаемого материала из среды разработки;
- встречу и сопровождение посетителей среды разработки;
- роли и обязанности по обеспечению непрерывного применения мер безопасности и обнаружения нарушений безопасности;

c) *относящиеся к персоналу* разработчиков или *организационные меры*, например средства контроля или проверки, позволяющие установить, заслуживают ли доверия принимаемые на работу;

d) *прочие меры безопасности*, например средства логической защиты оборудования разработки.

В документации по безопасности разработки следует идентифицировать участки разработки и описать виды выполняемых работ вместе с мерами безопасности, применяемыми в каждом из участков разработки и на транспортных средствах при перевозках между различными участками. Например, разработка может происходить в нескольких производственных помещениях внутри одного здания, в нескольких зданиях, расположенных на одной территории, или в нескольких различных местах. Транспортировка частей ОО или незаконченного ОО между различными участками разработки должна быть охвачена требованиями компонентов семейств «Безопасность разработки» (ALC_DVS), тогда как транспортировка готового ОО пользователю рассматривается в семействе «Поставка» (ALC_DEL).

К разработке относят и производство ОО.

12.5.1.3.2 Шаг оценивания ALC_DVS.1-2

Оценщик должен исследовать политики обеспечения конфиденциальности и целостности при разработке, чтобы сделать заключение о достаточности применявшихся мер безопасности.

Оценщику следует исследовать, включаются ли следующие аспекты в политики:

a) какая информация, относящаяся к разработке ОО, нуждается в сохранении конфиденциальности и кому из персонала разработчиков разрешен доступ к таким материалам;

b) какие материалы должны быть защищены от несанкционированной модификации для сохранения целостности ОО и кому из персонала разработчиков разрешено вносить изменения в такие материалы.

Оценщику следует сделать заключение, описаны ли эти политики в документации по безопасности разработки, совместимы ли применяемые меры безопасности с политиками, являются ли они достаточно полными.

Следует отметить, что процедуры управления конфигурацией способствуют защите целостности ОО, и оценщику следует избегать частичного перекрытия с шагами оценивания, проводимыми в рамках подвида деятельности ALC_CMC «Возможности УК». Например, документация УК может описывать процедуры безопасности, необходимые для контроля ролей или лиц, которым следует предоставить доступ к среде разработки и которые могут модифицировать ОО.

Тогда как требования ALC_CMC «Возможности УК» зафиксированы, требования для ALC_DVS «Безопасность разработки», предписывающие только необходимые меры, зависят от типа ОО и от информации, которая может быть представлена в разделе ЗБ «Среда безопасности». Например, ЗБ может идентифицировать политику безопасности организации, в которой требуется наличие формы допуска у персонала разработчиков ОО. Тогда оценщику в ходе выполнения данного подвида деятельности необходимо сделать заключение, применялась ли такая политика.

12.5.1.4 Действие ALC_DVS.1.2E

12.5.1.4.1 Шаг оценивания ALC_DVS.1-3

Оценщик должен исследовать документацию по безопасности разработки и связанные с ней свидетельства, чтобы сделать заключение, применяются ли меры безопасности.

На этом шаге оценивания от оценщика требуется сделать заключение, применяются ли меры безопасности, описанные в документации по безопасности разработки, таким образом, при котором целостность ОО и конфиденциальность связанной с ним документации защищены в достаточной степени. Например, данное заключение могло бы быть сделано по результатам исследования представленных документальных свидетельств. Документальные свидетельства следует дополнить непосредственным ознакомлением со средой разработки. Непосредственное ознакомление со средой разработки при посещении предоставит оценщику возможность:

a) наблюдать применение мер безопасности (например физических мер);

b) исследовать документальные свидетельства применения процедур;

c) посредством интервью с персоналом разработчиков проверить знание ими политик и процедур безопасности разработки, а также своих обязанностей.

Посещение объекта разработки является полезным способом приобретения уверенности в применяемых мерах. Решение отказаться от такого посещения следует принимать после консультации с органом оценки.

Руководство по посещению объектов см. в приложении А.4 «Посещение объектов».

12.5.2 Подвид деятельности по оценке (ALC_DVS.2)

12.5.2.1 Цели

Цель данного подвида деятельности — сделать заключение, являются ли меры и средства контроля безопасности в среде разработки достаточными для обеспечения конфиденциальности и целостности проекта и реализации ОО. Это необходимо для обеспечения того, чтобы безопасная эксплуатация ОО не была скомпрометирована. Кроме того, достаточность применяемых мер должна быть обоснована.

12.5.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) документация по безопасности разработки.

Кроме того, оценщику может понадобиться исследование других поставок, чтобы сделать заключение о том, что меры и средства контроля безопасности полностью определены и применяются. В частности, оценщику может понадобиться исследование документации разработчика по управлению конфигурацией (исходные данные подвидов деятельности ACM_CAP.4 «Поддержка производства, процедуры приемки» и ACM_SCP.2 «Охват УК отслеживания проблем»). Также требуется свидетельство применения процедур.

12.5.2.3 Действие ALC_DVS.2.1E

ИСО/МЭК 15408-3 ALC_DVS.2.1C: *Документация по безопасности разработки должна содержать описание всех физических, процедурных, организационных и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта ОО и его реализации в среде разработки.*

12.5.2.3.1 Шаг оценивания ALC_DVS.2-1

Оценщик должен исследовать документацию по безопасности разработки, чтобы сделать заключение, содержит ли она подробное описание всех используемых в среде разработки мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта и реализации ОО.

Оценщик определяет, какая информация из ЗБ нужна в первую очередь при вынесении заключения о необходимой защите.

Если в ЗБ не имеется такой информации в явном виде, оценщику нужно будет принять решение о необходимых мерах, основываясь на рассмотрении предполагаемой среды для ОО. В тех случаях, когда меры разработчика признаются недостаточными, рекомендуется, чтобы было представлено четкое и логическое обоснование для оценки уязвимостей, потенциально пригодных для использования.

При исследовании документации оценщиком рассматриваются следующие типы мер безопасности:

a) *физические,* например средства управления физическим доступом, применяемые для предотвращения несанкционированного доступа к среде разработки ОО (в рабочие часы и в другое время);

b) *процедурные*, например распространяющиеся на:

- предоставление доступа к среде разработки или к конкретным объектам среды, таким как оборудование разработки,
- отмену прав доступа лиц при их исключении из состава разработчиков,
- передачу защищаемого материала из среды разработки,
- встречу и сопровождение посетителей среды разработки,
- роли и обязанности по обеспечению непрерывного применения мер безопасности и обнаружения нарушений безопасности;

c) *относящиеся к персоналу* разработчиков или *организационные меры*, например средства контроля или проверки, позволяющие установить, заслуживают ли доверия принимаемые на работу;

d) *прочие меры безопасности*, например средства логической защиты оборудования разработки.

В документации по безопасности разработки следует идентифицировать участки разработки и описать виды выполняемых работ вместе с мерами безопасности, применяемыми в каждом из участков разработки и на транспортных средствах при перевозках между различными участками. Например, разработка может происходить в нескольких производственных помещениях внутри одного здания, в нескольких зданиях, расположенных на одной территории, или в нескольких различных местах. Транспортировка частей ОО или незаконченного ОО между различными участками разработки должна быть охвачена требованиями компонентов семейств «Безопасность разработки» (ALC_DVS), тогда как транспортировка готового ОО пользователю рассматривается в семействе «Поставка» (ALC_DEL).

К разработке относят и производство ОО.

ИСО/МЭК 15408-3 ALC_DVS.2.2C: *Свидетельство должно содержать логическое обоснование того, что меры безопасности обеспечивают необходимый уровень защиты для поддержания конфиденциальности и целостности ОО.*

12.5.2.3.2 Шаг оценивания ALC_DVS.2-2

Оценщик должен исследовать документацию по безопасности разработки для того, чтобы сделать заключение, содержится ли в ней соответствующее логическое обоснование того, что меры безопасности обеспечивают необходимый уровень защиты для поддержания конфиденциальности и целостности ОО.

Так как атаки на ОО или на связанную с ним информацию могут быть предприняты на различных стадиях проектирования и производства, меры и процедуры должны быть на надлежащем уровне, необходимом для предотвращения этих атак или для затруднения их осуществления.

Так как этот уровень зависит от общего потенциала нападения, требуемого ОО (см. выбранный компонент семейства AVA_VAN «Анализ уязвимостей»), рекомендуется, чтобы документация по безопасности разработки содержала обоснование необходимого для поддержания конфиденциальности и целостности ОО уровня защиты. Этот уровень должен быть достигнут применяемыми мерами по безопасности.

Концепции мер защиты следует быть последовательной, и в обоснование следует включать анализ того, каким образом меры взаимно поддерживают друг друга. Должны быть проанализированы все аспекты разработки и производства на всех различных местах разработки с учетом всех ролей, вовлеченных в процедуры разработки вплоть до поставки ОО.

В обосновании может содержаться и анализ потенциальных уязвимостей с учетом применяемых мер по безопасности.

Могут быть приведены убедительные аргументы, доказывающие, например что:

- технические меры и механизмы инфраструктуры разработки являются достаточными для того, чтобы поддерживать соответствующий уровень безопасности (например механизмы шифрования, механизмы физической защиты, свойства системы УК (см. ALC_CMC.4-5));
- система, содержащая представление реализации ОО (включая относящиеся к нему руководящие документы), обеспечивает эффективную защиту от логических атак, например с применением кода «трояна» или вируса. Этого может быть достаточно, если представление реализации хранится

на изолированной системе, где установлено только программное обеспечение, необходимое для поддержания её функционирования, и где впоследствии не устанавливается никакое дополнительное программное обеспечение.

- данные, вносимые в данную систему, должны быть тщательно рассмотрены в целях предотвращения установки в систему неких скрытых функциональных возможностей. Эффективность этих мер должна быть протестирована, например попыткой независимо получить доступ к машине, установить некоторые дополнительные выполняемые программы, макросы и т. д. или получить из машины некоторую информацию, используя логические атаки.
- соответствующие организационные (процедурные и организационные) меры безусловно осуществлены.

12.5.2.3.3 Шаг оценивания ALC_DVS.2-3

Оценщик должен исследовать политики обеспечения конфиденциальности и целостности при разработке, чтобы сделать заключение о достаточности применявшихся мер безопасности.

Оценщику следует исследовать, включается ли в политики управления следующее:

a) какая информация, относящаяся к разработке ОО, нуждается в сохранении конфиденциальности и кому из персонала разработчиков разрешен доступ к таким материалам;

b) какие материалы должны быть защищены от несанкционированной модификации для сохранения целостности ОО и кому из персонала разработчиков разрешено вносить изменения в такие материалы.

Оценщику следует сделать заключение, описаны ли эти политики в документации по безопасности разработки, совместимы ли применяемые меры безопасности с политиками, являются ли они достаточно полными.

Следует отметить, что процедуры управления конфигурацией способствуют защите целостности ОО, и оценщику следует избегать частичного перекрытия с шагами оценивания, проводимыми в рамках подвида деятельности ALC_CMC «Возможности УК». Например, документация УК может описывать процедуры безопасности, необходимые для контроля ролей или лиц, которым следует предоставить доступ к среде разработки и которые могут модифицировать ОО.

Тогда как требования ACM_CAP зафиксированы, требования для ALC_DVS «Безопасность разработки», предписывающие только необходимые меры, зависят от типа ОО и от информации, которая может быть представлена в ЗБ. Например, ЗБ может идентифицировать политику безопасности организации, в которой требуется наличие формы допуска у персонала разработчиков ОО. Тогда оценщику в ходе выполнения данного подвида деятельности необходимо сделать заключение, применялась ли такая политика.

12.5.2.4 Действие ALC_DVS.2.2E

12.5.2.4.1 Шаг оценивания ALC_DVS.2-4

Оценщик должен исследовать документацию по безопасности разработки и связанные с ней свидетельства, чтобы сделать заключение, применяются ли меры безопасности.

На этом шаге оценивания от оценщика требуется сделать заключение, применяются ли меры безопасности, описанные в документации по безопасности разработки, таким образом, при котором целостность ОО и конфиденциальность связанной с ним документации адекватно защищены. Например, данное заключение могло бы быть сделано по результатам исследования представленных документальных свидетельств. Документальные свидетельства следует дополнить непосредственным ознакомлением со средой разработки. Непосредственное ознакомление со средой разработки предоставит оценщику возможность:

a) наблюдать применение мер безопасности (например физических мер);

b) исследовать документальные свидетельства применения процедур;

c) посредством интервью с персоналом разработчиков проверить знание ими политик и процедур безопасности разработки, а также своих обязанностей.

Посещение объекта разработки является полезным способом приобретения уверенности в применяемых мерах. Решение отказаться от такого посещения следует принимать после консультации с органом оценки.

Руководство по посещению объектов см. в приложении А.4 «Посещение объектов».

12.6 Устранение недостатков (ALC_FLR)

12.6.1 Подвид деятельности по оценке (ALC_FLR.1)

12.6.1.1 Цели

Цель данного подвида деятельности — сделать заключение, установил ли разработчик процедуры устранения недостатков, которые описывают отслеживание недостатков безопасности, идент-

фикацию корректирующих действий по их исправлению и доведение информации об этих действиях до пользователей ОО.

12.6.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является документация процедур устранения недостатков.

12.6.1.3 Действие ALC_FLR.1.1E

ИСО/МЭК 15408-3 ALC_FLR.1.1C: *Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.*

12.6.1.3.1 Шаг оценивания ALC_FLR.1-1

Оценщик должен исследовать документацию процедур устранения недостатков, чтобы сделать заключение, описывает ли она процедуры отслеживания всех ставших известными недостатков безопасности в каждом релизе ОО.

Эти процедуры описывают действия, которые предпринимаются разработчиком с момента приведения в отчете каждого предполагаемого недостатка безопасности до момента реализации решения по нему. Это включает временные рамки всей деятельности, связанной с отдельным недостатком, начиная от его обнаружения, включая выяснение, что недостаток является недостатком безопасности, и заканчивая реализацией решения по нему.

Если выявленный недостаток не влияет на безопасность, то не понадобится выполнять (согласно требованиям ALC_FLR «Устранение недостатков») процедуры устранения недостатков для его дальнейшего отслеживания; только при этом необходимо объяснение, почему недостаток не влияет на безопасность.

Хотя эти требования не обязательно определяют способ широкого оповещения пользователей ОО о недостатках безопасности, они обязывают, чтобы все недостатки безопасности, которые уже приведены в отчете, отслеживались. То есть недостаток безопасности, о котором имеется информация в отчете, не может игнорироваться просто потому, что отчет поступил не из организации разработчика.

ИСО/МЭК 15408-3 ALC_FLR.1.2C: *Процедуры устранения недостатков должны содержать требование представления описания сути и последствий каждого недостатка безопасности, а также состояния процесса исправления этого недостатка.*

12.6.1.3.2 Шаг оценивания ALC_FLR.1-2

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, сопровождается ли применение этих процедур описанием каждого недостатка безопасности с точки зрения его сути и последствий.

Процедуры идентифицируют конкретные действия, которые приняты разработчиком для достаточно детального описания сути и последствий каждого недостатка безопасности, дающего возможность его воспроизведения. Описание сути недостатка безопасности раскрывает, является ли он ошибкой в документации, недостатком в проекте ФБО, недостатком в реализации ФБО и т. д. Описание последствий недостатка безопасности идентифицирует фрагменты реализации ФБО, подвергаемые воздействию, и результаты воздействия на эти фрагменты. Например, недостаток безопасности в реализации может быть в том, что он влияет на идентификацию и аутентификацию, осуществляемую ФБО, разрешая аутентификацию с паролем «ТАЙНЫЙ ВХОД».

12.6.1.3.3 Шаг оценивания ALC_FLR.1-3

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, будет ли идентифицировано при применении этих процедур состояние процесса исправления каждого недостатка безопасности.

Процедуры устранения недостатков идентифицируют различные стадии недостатков безопасности. Эта дифференциация, по крайней мере, включает: предполагаемые недостатки безопасности, которые приводятся в отчете; предполагаемые недостатки безопасности, для которых подтверждено, что они на самом деле являются недостатками безопасности; недостатки безопасности, решение по которым реализовано. Допустимо включение дополнительных стадий (например: недостатки, которые приведены в отчете, но которые еще не подвергались исследованию; недостатки, которые исследуются в настоящее время; недостатки безопасности, для которых решение найдено, но пока не реализовано).

ИСО/МЭК 15408-3 ALC_FLR.1.3C: *Процедуры устранения недостатков должны содержать требование, что для каждого недостатка безопасности должны быть идентифицированы корректирующие действия.*

12.6.1.3.4 Шаг оценивания ALC_FLR.1-4

Оценщик должен проверить процедуры устранения недостатков, чтобы сделать заключение, будут ли идентифицированы при применении этих процедур корректирующие действия по каждому недостатку безопасности.

Корректирующие действия могут заключаться как в восстановлении аппаратных средств, программно-аппаратных средств или программ, входящих в ОО, так и во внесении изменений в руководства по ОО или же могут включать и то, и другое. Корректирующие действия, приводящие к внесению изменений в руководства ОО (например к детализации процедурных мер, которые необходимо предпринять для нейтрализации недостатка безопасности), включают меры, обеспечивающие как одни лишь промежуточные решения (пока исправление не закончено), так и окончательное решение (для которого определено, что данная процедурная мера является наилучшим решением).

Если источником недостатка безопасности является ошибка в документации, то корректирующее действие сводится к обновлению соответствующего руководства ОО. Если корректирующее действие является процедурной мерой, то эта мера будет включать обновление соответствующего руководства ОО для отражения этих процедур.

ИСО/МЭК 15408-3 ALC_FLR.1.4C: *Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.*

12.6.1.3.5 Шаг оценивания ALC_FLR.1-5

Оценщик должен исследовать документацию процедур устранения недостатков, чтобы сделать заключение, содержит ли она описание методов, используемых для предоставления пользователям ОО необходимой информации о каждом недостатке безопасности.

Необходимая информация о каждом недостатке безопасности состоит из его описания (не обязательно такого же подробного, как это предусматривается на шаге оценивания ALC_FLR.1-2), предписанного корректирующего действия и соответствующего руководства по реализации исправления.

Такая информация, материалы по исправлению и обновленная документация могут быть предоставлены пользователям ОО любым способом, например путем размещения их на веб-сайте, рассылки пользователям ОО или заключения соглашения об установке и внедрении необходимых исправлений разработчиком. В тех случаях, когда способ предоставления этой информации требует действий, инициируемых пользователем ОО, оценщик исследует руководство ОО, чтобы удостовериться, содержит ли оно инструкции по получению такой информации.

Наиболее подходящая метрика оценки достаточности метода, используемого для предоставления информации, материалов по исправлению и руководств — это та, которая дает основание надеяться, что пользователи ОО смогут получить их. Например, рассмотрим метод рассылки, при котором необходимые данные размещаются на веб-сайте на один месяц, а пользователи ОО осведомлены о том, что это произойдет и когда это произойдет. Он может быть не так уж приемлем или эффективен (как, скажем, при постоянном размещении на веб-сайте), но все же позволяет пользователю ОО получить необходимую информацию. С другой стороны, если бы информация была размещена на веб-сайте всего лишь на один час, причем пользователи ОО никак не оповещались об этом и не знали бы заранее о времени размещения, то получение ими необходимой информации было бы практически невозможно.

12.6.2 Подвид деятельности по оценке (ALC_FLR.2)

12.6.2.1 Цели

Цель данного подвида деятельности — сделать заключение, установил ли разработчик процедуры устранения недостатков, которые описывают отслеживание недостатков безопасности, идентификацию корректирующих действий и доведение информации об этих действиях до пользователей ОО. Дополнительно по этому подвиду деятельности делается заключение, предусматривают ли процедуры разработчика исправление недостатков безопасности, получение отчетов о недостатках от пользователей ОО и обеспечение уверенности, что исправления не приведут ни к каким новым недостаткам безопасности.

Чтобы разработчики имели возможность соответствующим образом реагировать на отчеты пользователей ОО о недостатках безопасности, пользователям ОО необходимо понимать, как представлять отчеты о недостатках безопасности разработчикам, а разработчикам необходимо знать, каким образом получать эти отчеты. Руководство по устранению недостатков, предназначенное для пользователя ОО, обеспечивает осведомленность пользователей ОО о том, как установить связь с разработчиком, а процедуры устранения недостатков описывают роль разработчика при таком взаимодействии.

12.6.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) документация процедур устранения недостатков;

b) документация руководств по устранению недостатков.

12.6.2.3 Действие ALC_FLR.2.1E

ИСО/МЭК 15408-3 ALC_FLR.2.1C: *Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.*

12.6.2.3.1 Шаг оценивания ALC_FLR.2-1

Оценщик должен исследовать документацию процедур устранения недостатков, чтобы сделать заключение, описывает ли она процедуры отслеживания всех ставших известными недостатков безопасности в каждом релизе ОО.

Эти процедуры описывают действия, которые предпринимаются разработчиком с момента приведения информации о каждом предполагаемом недостатке безопасности в отчете до момента реализации решения по нему. Это включает временные рамки всей деятельности, связанной с отдельным недостатком, начиная от его обнаружения, включая выяснение, что недостаток является недостатком безопасности, и заканчивая реализацией решения по нему.

Если выявленный недостаток не влияет на безопасность, то не понадобится выполнять (согласно требованиям ALC_FLR «Устранение недостатков) процедуры устранения недостатков для его дальнейшего отслеживания; только при этом необходимо объяснение, почему недостаток не влияет на безопасность.

ИСО/МЭК 15408-3 ALC_FLR.2.2C: *Процедуры устранения недостатков должны содержать требование представления описания сути и последствий каждого недостатка безопасности, а также состояния процесса исправления этого недостатка.*

12.6.2.3.2 Шаг оценивания ALC_FLR.2-2

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, сопровождается ли применение этих процедур описанием каждого недостатка безопасности с точки зрения его сути и последствий.

Процедуры идентифицируют конкретные действия, которые приняты разработчиком для достаточно детального описания сути и последствий каждого недостатка безопасности, дающего возможность его воспроизведения. Описание сути недостатка безопасности раскрывает, является ли он ошибкой в документации, недостатком в проекте ФБО, недостатком в реализации ФБО и т. д. Описание последствий недостатка безопасности идентифицирует фрагменты реализации ФБО, подвергаемые воздействию, и результаты воздействия на эти фрагменты. Например, недостаток безопасности в реализации может быть в том, что он влияет на идентификацию и аутентификацию, осуществляемую ФБО, разрешая аутентификацию с паролем «ТАЙНЫЙВХОД».

12.6.2.3.3 Шаг оценивания ALC_FLR.2-3

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, будет ли идентифицировано при применении этих процедур состояние процесса исправления каждого недостатка безопасности.

Процедуры устранения недостатков идентифицируют различные стадии недостатков безопасности. Эта дифференциация, по крайней мере, включает: предполагаемые недостатки безопасности, которые приводятся в отчете; предполагаемые недостатки безопасности, для которых подтверждено, что они на самом деле являются недостатками безопасности; недостатки безопасности, решение по которым реализовано. Допустимо включение дополнительных стадий (например: недостатки, которые приводятся в отчете, но которые еще не подвергались исследованию; недостатки, которые исследуются в настоящее время; недостатки безопасности, для которых решение найдено, но пока не реализовано).

ИСО/МЭК 15408-3 ALC_FLR.2.3C: *Процедуры устранения недостатков должны содержать требование к тому, что для каждого недостатка безопасности должны быть идентифицированы корректирующие действия.*

12.6.2.3.4 Шаг оценивания ALC_FLR.2-4

Оценщик должен проверить процедуры устранения недостатков, чтобы сделать заключение, будут ли идентифицированы при применении этих процедур корректирующие действия по каждому недостатку безопасности.

Корректирующие действия могут заключаться как в восстановлении аппаратных средств, программно-аппаратных средств или программ, входящих в ОО, так и во внесении изменений в руководства по ОО, или же могут включать и то, и другое. Корректирующие действия, приводящие к внесению изменений в руководства ОО (например к детализации процедурных мер, которые необходимо

предпринять для нейтрализации недостатка безопасности), включают меры, обеспечивающие как одни лишь промежуточные решения (пока исправление не закончено), так и окончательное решение (для которого определено, что данная процедурная мера является наилучшим решением).

Если источником недостатка безопасности является ошибка в документации, то корректирующее действие сводится к обновлению соответствующего руководства ОО. Если корректирующее действие является процедурной мерой, то эта мера будет включать обновление соответствующего руководства ОО для отражения этих процедур.

ИСО/МЭК 15408-3 ALC_FLR.2.4C: *Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.*

12.6.2.3.5 Шаг оценивания ALC_FLR.2-5

Оценщик должен исследовать документацию процедур устранения недостатков, чтобы сделать заключение, содержит ли она описание методов, используемых для предоставления пользователям ОО необходимой информации о каждом недостатке безопасности.

Необходимая информация о каждом недостатке безопасности состоит из его описания (не обязательно такого же подробного, как это предусматривается на шаге оценивания ALC_FLR.2-2), предписанного корректирующего действия и соответствующего руководства по реализации исправления.

Такая информация, материалы по исправлению и обновленная документация могут быть предоставлены пользователям ОО любым способом, например путем размещения их на веб-сайте, рассылки пользователям ОО или заключения соглашения об установке и внедрении необходимых исправлений разработчиком. В тех случаях, когда способ предоставления этой информации требует действий, инициируемых пользователем ОО, оценщик исследует руководство ОО, чтобы удостовериться, содержит ли оно инструкции по получению такой информации.

Наиболее подходящая метрика оценки достаточности метода, используемого для предоставления информации, материалов по исправлению и руководств — это та, которая дает основание надеяться, что пользователи ОО смогут получить их. Например, рассмотрим метод рассылки, при котором необходимые данные размещаются на веб-сайте на один месяц, а пользователи ОО осведомлены о том, что это произойдет и когда это произойдет. Он может быть не так уж приемлем или эффективен (как, скажем, при постоянном размещении на веб-сайте), но все же позволяет пользователю ОО получить необходимую информацию. С другой стороны, если бы информация была размещена на веб-сайте всего лишь на один час, причем пользователи ОО никак не оповещались об этом и не знали бы заранее о времени размещения, то получение ими необходимой информации было бы практически невозможно.

ИСО/МЭК 15408-3 ALC_FLR.2.5C: *Процедуры устранения недостатков должны описывать средства, посредством которых разработчик получает от пользователей ОО сообщения и запросы о предполагаемых недостатках безопасности в ОО.*

12.6.2.3.6 Шаг оценивания ALC_FLR.2-6

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, описывается ли в них порядок получения разработчиком от пользователей ОО сообщений о предполагаемых недостатках безопасности или запросов на исправление таких недостатков.

Процедуры обеспечивают наличие у пользователей ОО способа связи с разработчиком ОО. Располагая таким способом, пользователь может сообщить о недостатках безопасности, справиться о статусе недостатков безопасности или запросить материалы по исправлению недостатков. Этот способ связи может быть в общем случае частью общих услуг связи для сообщения о проблемах, не относящихся к безопасности.

Использование этих процедур не ограничивается пользователями ОО; однако только пользователям ОО данные процедуры доводятся во всех подробностях. Другие лица из числа имеющих доступ к ОО или возможность ознакомиться с ним могут использовать эти же процедуры представления сообщений разработчику для их предполагаемой последующей обработки. Любые способы представления сообщений разработчику, кроме идентифицированных им, выходят за рамки этого шага оценивания, поэтому нет необходимости рассматривать сообщения, созданные другими способами.

ИСО/МЭК 15408-3 ALC_FLR.2.6C: *Процедуры обработки ставших известными недостатков безопасности должны обеспечить, чтобы любые ставшие известными недостатки были исправлены, а для пользователей ОО выпущены процедуры по исправлению.*

12.6.2.3.7 Шаг оценивания ALC_FLR.2-7

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, помогает ли применение этих процедур обеспечить исправление каждого недостатка, о котором получено сообщение.

Процедуры устранения недостатков распространяются на те недостатки безопасности, которые обнаружены и о которых получено сообщение как от участников разработки, так и от пользователей ОО. Процедуры детализированы в достаточной степени для описания того, как обеспечивается исправление каждого недостатка, о котором получено сообщение. Процедуры содержат обоснованные шаги, которые показывают прогресс в получении окончательного решения.

Процедуры описывают процесс, начиная с момента признания предполагаемого недостатка безопасности реальным до момента принятия решения по нему.

12.6.2.3.8 Шаг оценивания ALC_FLR.2-8

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, помогает ли применение этих процедур обеспечить доведение до пользователей ОО действий по исправлению для каждого недостатка безопасности.

Эти процедуры описывают процесс, выполняемый от момента принятия решения по недостатку безопасности до момента предоставления действия по исправлению. Процедурам для поставки действий по исправлению следует быть согласованными в целях безопасности; они не обязательно идентичны процедурам, используемым для поставки ОО, документированным для удовлетворения ALC_DEL при включении компонента этого семейства в требования доверия. Например, если аппаратная часть ОО была изначально доставлена курьерской связью, то при обновлении аппаратных средств для устранения недостатков по аналогии ожидалось бы их распределение курьерской связью. Обновления, не связанные с устранением недостатков, выполнялись бы согласно процедурам, сформулированным в документации, удовлетворяющей требованиям ALC_DEL «Поставка».

ИСО/МЭК 15408-3 ALC_FLR.2.7C: *Процедуры обработки ставших известными недостатков безопасности должны обеспечить такие защитные меры, чтобы любые исправления этих недостатков не приводили к появлению новых.*

12.6.2.3.9 Шаг оценивания ALC_FLR.2-9

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, предусматривает ли применение этих процедур такие защитные меры, что предполагаемые исправления не приведут к нежелательным последствиям.

Применяя анализ, тестирование или их сочетание, разработчик может уменьшить вероятность того, что исправление недостатка безопасности повлечет за собой нежелательные последствия. Оценщик определяет, предусматривают ли процедуры во всех деталях, как для данного исправления устанавливается необходимое сочетание анализа и действий по тестированию.

Для случая, когда источником недостатка безопасности является ошибка в документации, оценщик делает также заключение, включают ли процедуры защитные меры по предотвращению противоречий с остальной документацией.

ИСО/МЭК 15408-3 ALC_FLR.2.8C: *Руководство по устранению недостатков должно описывать средства, с помощью которых пользователи ОО могут сообщать разработчикам о любых предполагаемых недостатках безопасности в ОО.*

12.6.2.3.10 Шаг оценивания ALC_FLR.2-10

Оценщик должен исследовать руководство по устранению недостатков, чтобы сделать заключение, предоставляет ли применение этого руководства пользователю ОО способ представления сообщений о предполагаемых недостатках или запросов на исправление таких недостатков.

Данное руководство предоставляет пользователям ОО описание способа связи с разработчиком ОО. Располагая таким способом связи, пользователь может сообщить о недостатках безопасности, справиться о статусе недостатков безопасности или запросить материалы по исправлению недостатков.

12.6.3 Подвид деятельности по оценке (ALC_FLR.3)

12.6.3.1 Цели

Цель данного подвида деятельности — сделать заключение, установил ли разработчик процедуры устранения недостатков, которые описывают отслеживание недостатков безопасности, идентификацию действий по устранению и доведение информации об этих действиях до пользователей ОО. Дополнительно по этому подвиду деятельности делается заключение, предусматривают ли процедуры разработчика исправление недостатков безопасности, получение сообщений о недостатках от пользователей ОО, обеспечение уверенности, что исправления не приведут ни к каким новым недостаткам безопасности, определение контактных данных каждого пользователя ОО и своевременное доведение до пользователей ОО действий по их исправлению.

Чтобы разработчики имели возможность соответствующим образом реагировать на сообщения пользователей ОО о недостатках безопасности, пользователям ОО необходимо понимать, как представ-

лять сообщения о недостатках безопасности разработчикам, а разработчикам необходимо знать, каким образом получать эти сообщения. Руководство по устранению недостатков, предназначенное для пользователя ОО, обеспечивает, что пользователи ОО осведомлены о том, как установить связь с разработчиком, а процедуры устранения недостатков описывают роль разработчика при таком взаимодействии.

12.6.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) документация процедур устранения недостатков;

b) документация руководств по устранению недостатков.

12.6.3.3 Действие ALC_FLR.3.1E

ИСО/МЭК 15408-3 ALC_FLR.3.1C: *Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.*

12.6.3.3.1 Шаг оценивания ALC_FLR.3-1

Оценщик должен исследовать документацию процедур устранения недостатков, чтобы сделать заключение, описывает ли она процедуры отслеживания всех ставших известными недостатков безопасности в каждом релизе ОО.

Эти процедуры описывают действия, которые предпринимаются разработчиком с момента сообщения о каждом предполагаемом недостатке безопасности до момента реализации решения по нему. Это включает временные рамки всей деятельности, связанной с отдельным недостатком, начиная от его обнаружения, включая выяснение, что недостаток является недостатком безопасности, и заканчивая реализацией решения по нему.

Если выявленный недостаток не влияет на безопасность, то не понадобится выполнять (согласно требованиям ALC_FLR «Устранение недостатков») процедуры устранения недостатков для его дальнейшего отслеживания; только при этом необходимо объяснение, почему недостаток не влияет на безопасность.

ИСО/МЭК 15408-3 ALC_FLR.3.2C: *Процедуры устранения недостатков должны содержать требование представления описания сути и последствий каждого недостатка безопасности, а также состояния процесса исправления этого недостатка.*

12.6.3.3.2 Шаг оценивания ALC_FLR.3-2

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, сопровождается ли применение этих процедур описанием каждого недостатка безопасности с точки зрения его сути и последствий.

Процедуры идентифицируют действия, которые приняты разработчиком для достаточно детального описания сути и последствий каждого недостатка безопасности, дающего возможность его воспроизведения. Описание сути недостатка безопасности раскрывает, является ли он ошибкой в документации, недостатком в проекте ФБО, недостатком в реализации ФБО и т.д. Описание последствий недостатка безопасности идентифицирует фрагменты реализации ФБО, подвергаемые воздействию, и результаты воздействия на эти фрагменты. Например, недостаток безопасности в реализации может быть в том, что он влияет на идентификацию и аутентификацию, осуществляемую ФБО, разрешая аутентификацию с паролем «ТАЙНЫЙВХОД».

12.6.3.3.3 Шаг оценивания ALC_FLR.3-3

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, будет ли идентифицировано при применении этих процедур состояние процесса исправления каждого недостатка безопасности.

Процедуры устранения недостатков идентифицируют различные стадии недостатков безопасности. Эта дифференциация, по крайней мере, включает: предполагаемые недостатки безопасности, о которых выпущено сообщение; предполагаемые недостатки безопасности, для которых подтверждено, что они на самом деле являются недостатками безопасности; недостатки безопасности, решение по которым реализовано. Допустимо включение дополнительных стадий (например: недостатки, о которых сообщено, но они еще не исследовались; недостатки, которые исследуются в настоящее время; недостатки безопасности, для которых решение найдено, но пока не реализовано).

ИСО/МЭК 15408-3 ALC_FLR.3.3C: *Процедуры устранения недостатков должны содержать требование к тому, что для каждого недостатка безопасности должны быть идентифицированы корректирующие действия.*

12.6.3.3.4 Шаг оценивания ALC_FLR.3-4

Оценщик должен проверить процедуры устранения недостатков, чтобы сделать заключение, будут ли идентифицированы при применении этих процедур корректирующие действия по каждому недостатку безопасности.

Корректирующие действия могут заключаться как в восстановлении аппаратных средств, программно-аппаратных средств или программ, входящих в ОО, так и во внесении изменений в руководства по ОО, или же могут включать и то, и другое. Корректирующие действия, приводящие к внесению изменений в руководства ОО (например к детализации процедурных мер, которые необходимо предпринять для нейтрализации недостатка безопасности), включают меры, обеспечивающие как одни лишь промежуточные решения (пока исправление не закончено), так и окончательное решение (для которого определено, что данная процедурная мера является наилучшим решением).

Если источником недостатка безопасности является ошибка в документации, то корректирующее действие сводится к обновлению соответствующего руководства ОО. Если корректирующее действие является процедурной мерой, то эта мера будет включать обновление соответствующего руководства ОО для отражения этих процедур.

ИСО/МЭК 15408-3 ALC_FLR.3.4C: *Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.*

12.6.3.3.5 Шаг оценивания ALC_FLR.3-5

Оценщик должен исследовать документацию процедур устранения недостатков, чтобы сделать заключение, содержит ли она описание методов, используемых для предоставления пользователям ОО необходимой информации о каждом недостатке безопасности.

Необходимая информация о каждом недостатке безопасности состоит из его описания (не обязательно такого же подробного, как это предусматривается на шаге оценивания ALC_FLR.3-2), предписанного корректирующего действия и соответствующего руководства по реализации исправления.

Такая информация, материалы по исправлению и обновленная документация могут быть предоставлены пользователям ОО любым способом, например путем размещения их на веб-сайте, рассылки пользователям ОО или заключения соглашения об установке и внедрении необходимых исправлений разработчиком. В тех случаях, когда способ предоставления этой информации требует действий, инициируемых пользователем ОО, оценщик исследует руководство ОО, чтобы удостовериться, содержит ли оно инструкции по получению такой информации.

Наиболее подходящая метрика оценки достаточности метода, используемого для предоставления информации, материалов по исправлению и руководств — это та, которая дает основание надеяться, что пользователи ОО смогут получить их. Например, рассмотрим метод рассылки, при котором необходимые данные размещаются на веб-сайте на один месяц, а пользователи ОО осведомлены о том, что это произойдет и когда это произойдет. Он может быть не так уж приемлем или эффективен (как, скажем, при постоянном размещении на веб-сайте), но все же позволяет пользователю ОО получить необходимую информацию. С другой стороны, если бы информация была размещена на веб-сайте всего лишь на один час, причем пользователи ОО никак не оповещались об этом и не знали бы заранее о времени размещения, то получение ими необходимой информации было бы практически невозможно.

Для пользователей ОО, зарегистрированных у разработчика (см. шаг оценивания ALC_FLR.3-12), простого обеспечения доступности этой информации недостаточно. Разработчикам необходимо самим целенаправленно рассылать данную информацию (или уведомление о ее доступности) зарегистрированным пользователям ОО.

ИСО/МЭК 15408-3 ALC_FLR.3.5C: *Процедуры устранения недостатков должны описывать средства, с помощью которых разработчик получает от пользователей ОО сообщения и запросы о предполагаемых недостатках безопасности в ОО.*

12.6.3.3.6 Шаг оценивания ALC_FLR.3-6

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, описывается ли в них порядок получения разработчиком от пользователей ОО сообщений о предполагаемых недостатках безопасности или запросов на исправление таких недостатков.

Процедуры обеспечивают наличие у пользователей ОО способа связи с разработчиком ОО. Располагая таким способом, пользователь может сообщить о недостатках безопасности, справиться о статусе недостатков безопасности или запросить материалы по исправлению недостатков. Этот способ связи может быть в общем случае частью общих услуг связи для сообщения о проблемах, не относящихся к безопасности.

Использование этих процедур не ограничивается пользователями ОО; однако только пользователям ОО данные процедуры доводятся во всех подробностях. Другие лица из числа имеющих доступ к ОО или возможность ознакомиться с ним могут использовать эти же процедуры представления сообщений разработчику для их предполагаемой последующей обработки. Любые способы представления

сообщений разработчику, кроме идентифицированных им, лежат вне области этого шага оценивания, поэтому нет необходимости рассматривать сообщения, созданные другими способами.

ИСО/МЭК 15408-3 ALC_FLR.3.6C: *Процедуры устранения недостатков должны включать процедуру своевременного реагирования для автоматического распространения сообщений о недостатках безопасности и материалов по их исправлению зарегистрированным пользователям, для которых эти недостатки могут иметь последствия.*

12.6.3.3.7 Шаг оценивания ALC_FLR.3-7

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, предусматривает ли применение этих процедур способ своевременного доведения сообщений о недостатках безопасности и материалов по их исправлению зарегистрированным пользователям ОО, для которых эти недостатки могут иметь последствия.

Вопрос своевременности относится к выпуску как сообщений о недостатках безопасности, так и связанных с ними материалов по исправлению. Однако нет необходимости выпускать их одновременно. Считается, что сообщения о недостатках следует формировать и выпускать, как только найдено промежуточное решение, даже если это решение так же радикально, как «Выключить ОО». Аналогично, когда найдено более долговременное (и менее радикальное) решение, его следует издать без лишней задержки.

Нет необходимости в ограничении числа получателей сообщений и исправлений только теми пользователями ОО, для которых данный недостаток безопасности может иметь последствия; допустимо, чтобы до всех пользователей ОО доводились такие сообщения и исправления для всех недостатков безопасности при условии, что это делается своевременно.

12.6.3.3.8 Шаг оценивания ALC_FLR.3-8

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, будет ли результатом применения этих процедур автоматизированной рассылки сообщений о недостатках безопасности и материалов по их исправлению зарегистрированным пользователям, для которых эти недостатки могут иметь последствия.

Автоматизированная рассылка не подразумевает полного исключения участия человека в рассылке. В действительности метод рассылки может состоять полностью из выполняемых вручную процедур, возможно, с использованием строго контролируемой процедуры, предписывающей усиление мер контроля за выпуском сообщений или материалов по исправлению.

Нет необходимости в ограничении числа получателей сообщений и исправлений только теми пользователями ОО, для которых данный недостаток безопасности может иметь последствия; допустимо, чтобы до всех пользователей ОО доводились такие сообщения и исправления всех недостатков безопасности при условии, что это делается автоматически.

ИСО/МЭК 15408-3 ALC_FLR.3.7C: *Процедуры обработки ставших известными недостатков безопасности должны обеспечить, чтобы любые ставшие известными недостатки были исправлены, а для пользователей ОО выпущены процедуры по исправлению.*

12.6.3.3.9 Шаг оценивания ALC_FLR.3-9

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, помогает ли применение этих процедур обеспечить исправление каждого недостатка, о котором получено сообщение.

Процедуры устранения недостатков распространяются на те недостатки безопасности, которые обнаружены и о которых получено сообщение как от участников разработки, так и от пользователей ОО. Процедуры детализированы в достаточной степени для описания того, как обеспечивается исправление каждого недостатка, о котором получено сообщение. Процедуры содержат обоснованные шаги, которые демонстрируют прогресс в принятии окончательного решения.

Процедуры описывают процесс, начиная с момента признания предполагаемого недостатка безопасности реальным и до момента принятия решения по нему.

12.6.3.3.10 Шаг оценивания ALC_FLR.3-10

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, помогает ли применение этих процедур обеспечить доведение до пользователей ОО действий по исправлению каждого недостатка безопасности.

Процедуры описывают процесс, выполняемый от момента принятия решения по недостатку безопасности до момента предоставления действия по исправлению. Процедуры о действиях по исправлению должны быть согласованы с целями безопасности; они не обязательно идентичны процедурам, используемым для поставки ОО, документированным для удовлетворения ADO_DEL «Постав-

ка» при включении компонента этого семейства в требования доверия. Например, если аппаратная часть ОО была изначально доставлена курьерской связью, то при обновлении аппаратных средств для устранения недостатков по аналогии ожидалось бы их распределение курьерской связью. Обновления, не связанные с устранением недостатков, выполнялись бы согласно процедурам, сформулированным в документации, удовлетворяющей требованиям ADO_DEL «Поставка».

ИСО/МЭК 15408-3 ALC_FLR.3.8C: *Процедуры обработки ставших известными недостатков безопасности должны обеспечить такие защитные меры, чтобы любые исправления этих недостатков не приводили к появлению новых недостатков.*

12.6.3.3.11 Шаг оценивания ALC_FLR.3-11

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, предусматривает ли применение этих процедур такие защитные меры, что предполагаемые исправления не приведут к нежелательным последствиям.

Применяя анализ, тестирование или их сочетание, разработчик может уменьшить вероятность того, что исправление недостатка безопасности повлечет за собой нежелательные последствия. Оценщик определяет, предусматривают ли процедуры во всех деталях, как для данного исправления устанавливается необходимое сочетание анализа и действий по тестированию.

Для случая, когда источником недостатка безопасности является ошибка в документации, оценщик делает также заключение, включают ли процедуры защитные меры по предотвращению противоречий с остальной документацией.

ИСО/МЭК 15408-3 ALC_FLR.3.9C: *Руководство по устранению недостатков должно описывать средства, посредством которых пользователи ОО могут сообщать разработчикам о любых предполагаемых недостатках безопасности в ОО.*

12.6.3.3.12 Шаг оценивания ALC_FLR.3-12

Оценщик должен исследовать руководство по устранению недостатков, чтобы сделать заключение, предоставляет ли применение этого руководства пользователю ОО способ представления сообщений о предполагаемых недостатках или запросов на исправление таких недостатков.

Данное руководство предоставляет пользователям ОО описание способа связи с разработчиком ОО. Располагая таким способом связи, пользователь может сообщить о недостатках безопасности, справиться о статусе недостатков безопасности или запросить материалы по исправлению недостатков.

ИСО/МЭК 15408-3 ALC_FLR.3.10C: *Руководство по устранению недостатков должно описывать средства, посредством которых пользователи ОО могут регистрироваться у разработчика, чтобы иметь право получать сообщения о недостатках безопасности и исправления.*

12.6.3.3.13 Шаг оценивания ALC_FLR.3-13

Оценщик должен исследовать руководство по устранению недостатков, чтобы сделать заключение, описан ли в нем способ предоставления пользователям ОО возможности регистрации у разработчика.

Предоставление пользователям ОО возможности регистрации у разработчика означает всего лишь наличие у каждого пользователя ОО возможности предоставить разработчику свои контактные данные; эти контактные данные используются для обеспечения пользователя ОО информацией, связанной как с недостатками безопасности, которые могли бы иметь последствия для этого пользователя ОО, так и с исправлениями недостатков безопасности. Регистрация пользователя ОО может осуществляться как часть стандартных процедур, которые выполняются пользователями ОО, чтобы идентифицировать себя у разработчика, зарегистрировать лицензию на программное обеспечение или получать обновления и другую полезную информацию.

Нет необходимости в отдельном зарегистрированном пользователе для каждой инсталляции ОО; в организации вполне достаточно иметь одного зарегистрированного пользователя ОО. Например, корпоративный пользователь ОО может иметь централизованную службу комплектования для всех мест его размещения. В этом случае достаточно осуществлять контакт через службу комплектования для всех мест размещения ОО у корпоративного пользователя и, таким образом, обеспечить для каждой пользовательской инсталляции ОО зарегистрированные контактные данные.

В любом случае необходимо иметь возможность ассоциировать каждый поставленный ОО с конкретной организацией, чтобы обеспечить наличие зарегистрированного пользователя для каждого ОО. Для организаций, имеющих несколько различных адресов, это позволит удостовериться в отсутствии пользователей, которые ошибочно будут считаться охваченными регистрацией.

Следует отметить, что пользователи ОО не обязаны регистрироваться, но такую возможность им необходимо предоставить. Тем не менее, пользователям, выбравшим регистрацию, необходимо прямо посылать информацию (или уведомление о ее доступности).

ИСО/МЭК 15408-3 ALC_FLR.3.11C: *В руководстве по устранению недостатков должна быть идентифицирована контактная информация для всех сообщений и запросов по вопросам безопасности, связанных с ОО.*

12.6.3.3.14 Шаг оценивания ALC_FLR.3-14

Оценщик должен исследовать руководство по устранению недостатков, чтобы сделать заключение, идентифицированы ли в нем конкретные контактные данные для всех сообщений и запросов пользователя относительно проблем безопасности, относящихся к ОО.

Руководство включает способ, посредством которого зарегистрированные пользователи ОО могут взаимодействовать с разработчиком, чтобы сообщать ему об обнаруженных недостатках безопасности в ОО или делать запросы относительно обнаруженных недостатков безопасности в ОО.

12.7 Определение жизненного цикла (ALC_LCD)

12.7.1 Подвид деятельности по оценке (ALC_LCD.1)

12.7.1.1 Цели

Цель данного подвида деятельности — сделать заключение, использовал ли разработчик задокументированную модель жизненного цикла ОО.

12.7.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) документация определения жизненного цикла.

12.7.1.3 Действие ALC_LCD.1.1E

ИСО/МЭК 15408-3 ALC_LCD.1.1C: *Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО.*

12.7.1.3.1 Шаг оценивания ALC_LCD.1-1

Оценщик должен исследовать документированное описание используемой модели жизненного цикла, чтобы сделать заключение, распространяется ли она на процессы разработки и сопровождения ОО.

В описание модели жизненного цикла следует включать:

a) информацию о фазах жизненного цикла ОО и границах между последовательными фазами;

b) информацию о процедурах, инструментальных средствах и методах, используемых разработчиком (например при проектировании, кодировании, тестировании, исправлении ошибок);

c) информацию об общей структуре управления применением процедур (например идентификацию и описание персональной ответственности за каждую из процедур, требуемых в процессе разработки и сопровождения ОО согласно модели жизненного цикла);

d) информацию о том, какие части ОО поставляются субподрядчиками, если субподрядчики вовлечены в процесс разработки и сопровождения.

Оценка подвида деятельности ALC_LCD.1 не содержит утверждение о соответствии используемой модели какой-либо стандартизованной модели жизненного цикла.

ИСО/МЭК 15408-3 ALC_LCD.1.2C: *Модель жизненного цикла должна обеспечить необходимый контроль за разработкой и сопровождением ОО.*

12.7.1.3.2 Шаг оценивания ALC_LCD.1-2

Оценщик должен исследовать модель жизненного цикла, чтобы сделать заключение, будет ли использование процедур, инструментальных средств и методов, описанных в модели жизненного цикла, оказывать необходимое положительное влияние на разработку и сопровождение ОО.

Информация, представленная в модели жизненного цикла, дает оценщику определенную уверенность в том, что принятые процедуры разработки и сопровождения минимизируют вероятность недостатков безопасности. Например, если в модели жизненного цикла содержится описание процесса проверки, но не предусмотрено протоколирование внесения изменений в компоненты, то оценщик будет менее уверен, что в ОО не будут внесены ошибки. Оценщик может достичь большей уверенности, сравнивая описание модели со своим пониманием процесса разработки, полученным при выполнении других своих действий, относящихся к анализу процесса разработки ОО (например тех действий, на которые распространяется деятельность по оценке «Возможности УК» ALC_CMC). Выявленным недостаткам в модели жизненного цикла следует уделить особое внимание, если можно ожидать, что они приведут к случайному или преднамеренному внесению ошибок в ОО.

ИСО/МЭК 15408 не предписывает какого-либо конкретного подхода к разработке; следует оценивать каждый подход по существу. Например, такие подходы к проектированию, как спиральный, быстрого макетирования или каскадный, могут быть использованы для создания качественного ОО, если они применяются в контролируемой среде.

12.7.2 Подвид деятельности по оценке (ALC_LCD.2)

12.7.2.1 Цели

Цель данного подвида деятельности — сделать заключение, использовал ли разработчик задокументированную и измеримую модель жизненного цикла ОО.

12.7.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) документация определения жизненного цикла;

c) информация о используемом стандарте;

d) документация на выходе жизненного цикла.

12.7.2.3 Действие ALC_LCD.2.1E

ИСО/МЭК 15408-3 ALC_LCD.2.1C: *Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО, в том числе детализацию арифметических параметров и/или метрик, используемых для измерения качества ОО и/или его разработки.*

12.7.2.3.1 Шаг оценивания ALC_LCD.2-1

Оценщик должен исследовать документированное описание используемой модели жизненного цикла, чтобы сделать заключение, распространяется ли она на процессы разработки и сопровождения ОО, включая детальное описание её арифметических параметров и/или метрик, используемых для измерения разработки ОО.

Описание модели жизненного цикла включает:

a) информацию о фазах жизненного цикла ОО и границах между последовательными фазами;

b) информацию о процедурах, инструментальных средствах и методах, используемых разработчиком (например при проектировании, кодировании, тестировании, исправлении ошибок);

c) информацию об общей структуре управления применением процедур (например идентификацию и описание персональной ответственности за каждую из процедур, требуемых в процессе разработки и сопровождения ОО согласно модели жизненного цикла);

d) информацию о том, какие части ОО поставляются субподрядчиками, если субподрядчики вовлечены в процесс разработки и сопровождения;

e) информацию по поводу параметров/метрик, которые используются для измерения разработки ОО. Стандартные метрики обычно включают рекомендации по проведению измерений и по производству надежных продуктов, охватывая аспекты надежности, качества, эффективности работы, сложности продукта и его стоимости. Для оценивания все эти метрики являются значимыми, что применяется для повышения качества путем снижения вероятности недостатков и таким образом, в свою очередь, повышая уровень доверия к безопасности данного ОО.

ИСО/МЭК 15408-3 ALC_LCD.2.2C: *В модели жизненного цикла должен быть обеспечен необходимый контроль над разработкой и сопровождением ОО.*

12.7.2.3.2 Шаг оценивания ALC_LCD.2-2

Оценщик должен исследовать модель жизненного цикла, чтобы сделать заключение, будет ли использование процедур, инструментальных средств и методов, описанных в модели жизненного цикла, оказывать необходимое положительное влияние на разработку и сопровождение ОО.

Информация, представленная в модели жизненного цикла, дает оценщику определенную уверенность в том, что принятые процедуры разработки и сопровождения минимизируют вероятность недостатков безопасности. Например, если в модели жизненного цикла содержится описание процесса проверки, но не предусмотрено протоколирование внесения изменений в компоненты, то оценщик будет менее уверен, что в ОО не будут внесены ошибки. Оценщик может достичь большей уверенности, сравнивая описание модели со своим пониманием процесса разработки, полученным при выполнении других своих действий, относящихся к анализу процесса разработки ОО (например тех действий, на которые распространяется деятельность по оценке «Возможности УК» ALC_CMC). Выявленным недостаткам в модели жизненного цикла следует уделить особое внимание, если можно ожидать, что они приведут к случайному или преднамеренному внесению ошибок в ОО.

ИСО/МЭК 15408 не предписывает какого-либо конкретного подхода к разработке; следует оценивать каждый подход по существу. Например, такие подходы к проектированию, как спиральный, быстрого макетирования или каскадный, могут быть использованы для создания качественного ОО, если они применяются в контролируемой среде.

Для метрик/измерений, используемых в модели жизненного цикла, должны быть представлены свидетельства того, каким образом эти метрики/измерения способствуют минимизации вероятности недостатков. Это можно рассматривать как общую цель измерений в контексте ALC. Вследствие это-

го, метрики/измерения должны быть отобраны на основании их способности достигнуть этой цели или способствовать её достижению. Во-первых, метрика/измерение является подходящей относительно ALC, если корреляция между метрикой/измерением и количеством недостатков может быть заявлена с определенной степенью надежности. Но также полезной является метрика, использующаяся в управленческих целях, например при планировании и контроле качества разработки ОО, так как проекты, которыми недостаточно хорошо управляют, подвергаются риску плохого функционирования и появления недостатков.

Можно использовать метрики для повышения качества даже в тех случаях, когда это использование не очевидно. Например, метрика, используемая для оценки ожидаемой стоимости разработки продукта, может помочь повысить качество, если разработчик сумеет показать, что эта метрика используется для обеспечения достаточного финансирования проектов разработки и что её применение помогает избежать проблем качества, являющихся результатом нехватки ресурсов.

Не требуется, чтобы каждый этап жизненного цикла ОО был измерим. Однако оценщику следует из описания мер и процедур увидеть, что метрики являются приемлемыми для управления общим качеством ОО и таким образом для минимизации возможных недостатков безопасности.

ИСО/МЭК 15408-3 ALC_LCD.2.3C: *В документации по выходным данным жизненного цикла должны быть представлены результаты измерения качества разработки ОО с использованием стандартизированной модели.*

12.7.2.3.3 Шаг оценивания ALC_LCD.2-3

Оценщик должен исследовать документацию на выходе жизненного цикла, чтобы сделать заключение о том, что она предоставляет результаты измерений разработки ОО, используя измеримую модель жизненного цикла.

Результатам измерений и развитию жизненного цикла ОО следует соответствовать модели жизненного цикла.

Документация на выходе включает в себя не только численные значения метрик, но также и документы по действиям, предпринятым в результате измерений и в соответствии с моделью. Например, в этой документации может быть требование того, чтобы определенная стадия проектирования была произведена повторно в случае, если величина некоторых ошибок, измеренных во время тестирования, оказалась за пределами определенного допустимого порога. В этом случае в документации следует показать, что такие действия были приняты, если пороговое значение действительно не было достигнуто.

Если оценка проводится параллельно с разработкой ОО, то возможен случай, что измерения качества ОО применяются впервые. В этом случае, если результаты измерений качества отклоняются от некоторого порога, оценщику следует использовать документацию запланированных процедур, чтобы приобрести доверие тому, что корректирующие действия определены.

12.8 Инструментальные средства и методы (ALC_TAT)

12.8.1 Подвид деятельности по оценке (ALC_TAT.1)

12.8.1.1 Цели

Цель данного подвида деятельности — сделать заключение, использовал ли разработчик полностью определенные инструментальные средства разработки (например языки программирования или системы автоматизированного проектирования (САПР)), которые дают непротиворечивые и предсказуемые результаты.

12.8.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) документация инструментальных средств разработки;

b) подмножество представления реализации.

12.8.1.3 Замечания по применению

Эта работа может выполняться параллельно с действиями по оценке «Представление реализации» ADV_IMP, а особенно в части, касающейся определения используемых характеристик инструментальных средств, которые повлияют на объектный код (например опции компиляции).

12.8.1.4 Действие ALC_TAT.1.1E

ИСО/МЭК 15408-3 ALC_TAT.1.1C: *Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.*

12.8.2 Шаг оценивания ALC_TAT.1-1

Оценщик должен исследовать представленную документацию инструментальных средств разработки, чтобы сделать заключение, все ли инструментальные средства разработки полностью определены.

Например, полностью определенными могут считаться те языки, компиляторы или САПР, которые соответствуют общепризнанным стандартам, таким как стандарты ИСО. Полностью определенным языком является тот, для которого имеется четкое и полное описание его синтаксиса и детальное описание семантики каждой из его конструкций.

ИСО/МЭК 15408-3 ALC_TAT.1.2C: *В документации по инструментальным средствам разработки должны быть однозначно определены значения всех языковых конструкций, используемых в реализации.*

12.8.2.1.1 Шаг оценивания ALC_TAT.1-2

Оценщик должен исследовать документацию каждого инструментального средства, чтобы сделать заключение, однозначно ли определены в ней значения всех конструкций (формулировок, условностей, директив), используемых в представлении реализации.

В документации инструментальных средств разработки (например в спецификациях языка программирования и в руководствах пользователя) следует охватить все конструкции, используемые в представлении реализации ОО, и для каждой такой конструкции следует предоставить четкое и однозначное определение предназначения и результата выполнения этой конструкции. Эта работа может быть выполнена в сочетании с исследованием оценщиком представления реализации, выполняемого в рамках подвида деятельности ADV_IMP. Главные усилия оценщика следует направить на выяснение того, действительно ли документация достаточно ясна для понимания представления реализации. Например, в документации не следует предполагать, что читатель является экспертом по используемому языку программирования.

Ссылка на использование документированного стандарта — приемлемый подход для удовлетворения этого требования, при условии, что данный стандарт доступен для оценщика. Любые отклонения от этого стандарта следует документировать.

Важная проверка состоит в том, может ли оценщик понять исходный код ОО при выполнении анализа исходного кода, включенного в подвид деятельности «Представление реализации» (ADV_IMP). Несмотря на это, для поиска проблемных областей может использоваться следующий проверочный список:

a) на естественном языке такие фразы, как «цель данной конструкции не определена», и такие термины, как «зависит от реализации» или «ошибочный» могут указывать на плохо определенные области;

b) использование псевдонимов (альтернативных имен, которые позволяют ссылаться на одну и ту же часть памяти различными способами) — распространенный источник возникновения проблемы неоднозначности;

c) обработка исключительных событий (например что должно происходить после исчерпания свободной памяти или переполнения стека) часто плохо определена.

Большинство широко используемых языков, как бы хорошо они не были разработаны, могут иметь некоторые проблемные конструкции. Если язык реализации в целом хорошо определен, но все же существуют некоторые проблемные конструкции, то до окончания исследования исходных текстов следует вынести неокончательный вердикт.

Оценщику в процессе исследования исходных кодов следует верифицировать, что любое использование проблемных конструкций не вносит уязвимостей. Оценщику следует также удостовериться, что конструкции, не предусмотренные соответствующим стандартом, не используются.

В документации по инструментальным средствам разработки следует определять все формулировки, условности, директивы, использованные в представлении реализации.

ИСО/МЭК 15408-3 ALC_TAT.1.3C: *В документации по инструментальным средствам разработки должны быть однозначно определены значения всех опций, обусловленных реализацией.*

12.8.2.1.2 Шаг оценивания ALC_TAT.1-3

Оценщик должен исследовать документацию инструментальных средств, чтобы сделать заключение, однозначно ли определены в ней значения всех опций, обусловленных реализацией.

В документацию инструментальных средств разработки программного обеспечения следует включать определения опций, обусловленных реализацией, которые могут повлиять на содержание выполняемого кода, и тех, которые отличаются от стандарта используемого языка. В случаях, когда оценщику предоставляется исходный код, ему также следует предоставить информацию по используемым опциям компиляции и сборки.

В документации инструментальных средств проектирования и разработки аппаратных средств следует описать использование всех опций, которые влияют на результаты применения инструментальных средств (например детальные аппаратные спецификации или сами аппаратные средства).

12.8.3 Подвид деятельности по оценке (ALC_TAT.2)

12.8.3.1 Цели

Цель данного подвида деятельности — сделать заключение, использовал ли разработчик полностью определенные инструментальные средства разработки (например языки программирования или системы автоматизированного проектирования (САПР)), которые дают непротиворечивые и предсказуемые результаты, а также применялись ли стандарты реализации.

12.8.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) документация инструментальных средств разработки;

b) подмножество представления реализации;

c) представление реализации ФБО.

12.8.3.3 Замечания по применению

Эта работа может выполняться параллельно с действиями по оценке «Представление реализации» ADV_IMP, а особенно в части, касающейся определения используемых характеристик инструментальных средств, которые повлияют на объектный код (например опции компиляции).

12.8.3.4 Действие ALC_TAT.2.1E

ИСО/МЭК 15408-3 ALC_TAT.2.1C: *Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.*

12.8.3.4.1 Шаг оценивания ALC_TAT.2-1

Оценщик должен исследовать представленную документацию инструментальных средств разработки, чтобы сделать заключение, все ли инструментальные средства разработки полностью определены.

Например, полностью определенными могут считаться те языки, компиляторы или САПР, которые соответствуют общепризнанным стандартам, таким как стандарты ИСО. Полностью определенным языком является тот, для которого имеется четкое и полное описание его синтаксиса и детальное описание семантики каждой из его конструкций.

ИСО/МЭК 15408-3 ALC_TAT.2.2C: *В документации по инструментальным средствам разработки должны быть однозначно определены значения всех конструкций языка, используемых в реализации.*

12.8.3.4.2 Шаг оценивания ALC_TAT.2-2

Оценщик должен исследовать документацию каждого инструментального средства, чтобы сделать заключение, однозначно ли определены в ней значения всех конструкций (формулировок, условностей, директив), используемых в представлении реализации.

В документации инструментальных средств разработки (например в спецификациях языка программирования и в руководствах пользователя) следует охватить все конструкции, используемые в представлении реализации ОО, и для каждой такой конструкции следует предоставить четкое и однозначное определение предназначения и результата выполнения этой конструкции. Эта работа может быть выполнена в сочетании с исследованием оценщиком представления реализации, выполняемого в рамках подвида деятельности ADV_IMP. Главные усилия оценщика следует направить на выяснение того, действительно ли документация достаточно ясна для понимания представления реализации. Например, в документации не следует предполагать, что читатель является экспертом по используемому языку программирования.

Ссылка на использование документированного стандарта — приемлемый подход для удовлетворения этого требования, при условии, что данный стандарт доступен для оценщика. Любые отклонения от этого стандарта следует документировать.

Важная проверка состоит в том, может ли оценщик понять исходный код ОО при выполнении анализа исходного кода, включенного в подвид деятельности «Представление реализации» (ADV_IMP). Несмотря на это, для поиска проблемных областей может использоваться следующий проверочный список:

a) на естественном языке такие фразы, как «цель данной конструкции не определена», и такие термины, как «зависит от реализации» или «ошибочный» могут указывать на плохо определенные области;

b) использование псевдонимов (альтернативных имен, которые позволяют ссылаться на одну и ту же часть памяти различными способами) — распространенный источник возникновения проблемы неоднозначности;

c) обработка исключительных событий (например что должно происходить после исчерпания свободной памяти или переполнения стека) часто плохо определена.

Большинство широко используемых языков, как бы хорошо они не были разработаны, могут иметь некоторые проблемные конструкции. Если язык реализации в целом хорошо определен, но все же су-

ществуют некоторые проблемные конструкции, то до окончания исследования исходных текстов следует вынести неокончательный вердикт.

Оценщику в процессе исследования исходных кодов следует верифицировать, что любое использование проблемных конструкций не вносит уязвимостей. Оценщику следует также удостовериться, что конструкции, не предусмотренные соответствующим стандартом, не используются.

В документации по инструментальным средствам разработки следует определять все формулировки, условности, директивы, использованные в представлении реализации.

ИСО/МЭК 15408-3 ALC_TAT.2.3C: *В документации по инструментальным средствам разработки должны быть однозначно определены значения всех опций, обусловленных реализацией.*

12.8.3.4.3 Шаг оценивания ALC_TAT.2-3

Оценщик должен исследовать документацию инструментальных средств, чтобы сделать заключение, однозначно ли определены в ней значения всех опций, обусловленных реализацией.

В документацию инструментальных средств разработки программного обеспечения следует включать определения опций, обусловленных реализацией, которые могут повлиять на содержание выполняемого кода, и тех, которые отличаются от стандарта используемого языка. В случаях, когда оценщику предоставляется исходный код, ему также следует предоставить информацию по используемым опциям компиляции и сборки.

В документации инструментальных средств проектирования и разработки аппаратных средств следует описать использование всех опций, которые влияют на результаты применения инструментальных средств (например детальные аппаратные спецификации или сами аппаратные средства).

12.8.3.5 Действие ALC_TAT.2.2E

12.8.3.5.1 Шаг оценивания ALC_TAT.2-4

Оценщик должен исследовать аспекты процесса реализации, чтобы сделать заключение о том, что были применены документированные стандарты реализации.

Этот шаг оценивания требует, чтобы оценщик проанализировал предоставленное ему представление реализации ОО для вынесения заключения о том, были ли применены документированные стандарты реализации.

Оценщику следует верифицировать, что конструкции, исключенные из документированного стандарта, не используются.

Кроме того, оценщику следует проверить процедуры разработчика, которые обеспечивают применение определенных стандартов в пределах процесса проектирования и реализации ОО. Поэтому, помимо получения письменного свидетельства, оценщику следует посетить среду проектирования. Посещение среды проектирования позволит оценщику:

a) наблюдать за применением определенных стандартов;

b) исследовать письменное свидетельство применения процедур, описывающих использование определенных стандартов;

c) провести интервью с сотрудниками, ответственными за разработку, чтобы проверить наличие у них понимания относительно применения определенных стандартов и процедур.

Посещение участка разработки — полезное средство для приобретения доверия к используемым процедурам. Решение не совершать такой визит следует принимать только после консультации с органом оценки.

Оценщик сравнивает предоставленное ему представление реализации с описанием применяемых стандартов реализации и верифицирует их использование.

На этом уровне доверия не требуется, чтобы всё представление реализации ФБО было целиком основано на стандартах реализации; требование касается только тех частей, которые непосредственно разработаны самим разработчиком ОО. Оценщик может сверяться со списком конфигурации, требуемым в семействе «Область УК» (ALC_CMS), для получения информации о том, какие части разработаны непосредственно разработчиком ОО, а какие — сторонними разработчиками.

Если стандарты реализации, на которые ссылаются, не применяются хотя бы к части предоставленного оценщику представления реализации, то результат данного шага оценивания отрицательный.

Следует отметить, что части ОО, которые не относятся к ФБО, не должны исследоваться.

Этот шаг оценивания может быть выполнен в сочетании с действиями оценивания по ADV_IMP.

12.8.4 Подвид деятельности по оценке (ALC_TAT.3)

12.8.4.1 Цели

Цель данного подвида деятельности — сделать заключение, использовал ли разработчик или его субподрядчики полностью определенные инструментальные средства разработки (например языки

программирования или системы автоматизированного проектирования (САПР)), которые дают непротиворечивые и предсказуемые результаты, а также применялись ли стандарты реализации.

12.8.4.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) документация инструментальных средств разработки;

b) подмножество представления реализации;

c) представление реализации ФБО.

12.8.4.3 Замечания по применению

Эта работа может выполняться параллельно с действиями по оценке «Представление реализации» ADV_IMP, а особенно в части, касающейся определения используемых характеристик инструментальных средств, которые повлияют на объектный код (например опции компиляции).

12.8.4.4 Действие ALC_TAT.3.1E

ИСО/МЭК 15408-3 ALC_TAT.3.1C: *Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.*

12.8.4.4.1 Шаг оценивания ALC_TAT.3-1

Оценщик должен исследовать представленную документацию инструментальных средств разработки, чтобы сделать заключение, все ли инструментальные средства разработки полностью определены.

Например, полностью определенными могут считаться те языки, компиляторы или САПР, которые соответствуют общепризнанным стандартам, таким как стандарты ИСО. Полностью определенным языком является тот, для которого имеется четкое и полное описание его синтаксиса и детальное описание семантики каждой из его конструкций.

На этом уровне доверия документация инструментальных средств разработки, используемых субподрядчиками ОО, должна быть также исследована оценщиком.

ИСО/МЭК 15408-3 ALC_TAT.3.2C: *В документации по инструментальным средствам разработки должны быть однозначно определены значения всех конструкций языка, используемых в реализации.*

12.8.4.4.2 Шаг оценивания ALC_TAT.3-2

Оценщик должен исследовать документацию каждого инструментального средства, чтобы сделать заключение, однозначно ли определены в ней значения всех конструкций (формулировок, условностей, директив), используемых в представлении реализации.

В документации инструментальных средств разработки (например в спецификациях языка программирования и в руководствах пользователя) следует охватить все конструкции, используемые в представлении реализации ОО, и для каждой такой конструкции следует предоставить четкое и однозначное определение предназначения и результата выполнения этой конструкции. Эта работа может быть выполнена в сочетании с исследованием оценщиком представления реализации, выполняемого в рамках подвида деятельности ADV_IMP. Главные усилия оценщика должны быть направлены на выяснение того, действительно ли документация достаточно ясна для понимания представления реализации. Например, в документации не следует предполагать, что читатель является экспертом по используемому языку программирования.

Ссылка на использование документированного стандарта — приемлемый подход для удовлетворения этого требования, при условии, что данный стандарт доступен для оценщика. Любые отклонения от этого стандарта следует документировать.

Важная проверка состоит в том, может ли оценщик понять исходный код ОО при выполнении анализа исходного кода, включенного в подвид деятельности «Представление реализации» (ADV_IMP). Несмотря на это, для поиска проблемных областей может использоваться следующий проверочный список:

a) на естественном языке такие фразы, как «цель данной конструкции не определена», и такие термины, как «зависит от реализации» или «ошибочный» могут указывать на плохо определенные области;

b) использование псевдонимов (альтернативных имен, которые позволяют ссылаться на одну и ту же часть памяти различными способами) — распространенный источник возникновения проблемы неоднозначности;

c) обработка исключительных событий (например что должно происходить после исчерпания свободной памяти или переполнения стека) часто плохо определена.

Большинство широко используемых языков, как бы хорошо они не были разработаны, могут иметь некоторые проблемные конструкции. Если язык реализации в целом хорошо определен, но все же существуют некоторые проблемные конструкции, то до окончания исследования исходных текстов следует вынести неокончательный вердикт.

Оценщику в процессе исследования исходных кодов следует верифицировать, что любое использование проблемных конструкций не вносит уязвимостей. Оценщику следует также удостовериться, что конструкции, не предусмотренные соответствующим стандартом, не используются.

В документации по инструментальным средствам разработки следует определять все формулировки, условности, директивы, использованные в представлении реализации.

На этом уровне доверия документация инструментальных средств разработки, используемых субподрядчиками ОО, должна быть также исследована оценщиком.

ИСО/МЭК 15408-3 ALC_TAT.3.3C: *В документации по инструментальным средствам разработки должны быть однозначно определены значения всех опций, обусловленных реализацией.*

12.8.4.4.3 Шаг оценивания ALC_TAT.3-3

Оценщик должен исследовать документацию инструментальных средств, чтобы сделать заключение, однозначно ли определены в ней значения всех опций, обусловленных реализацией.

В документацию инструментальных средств разработки программного обеспечения следует включать определения опций, обусловленных реализацией, которые могут повлиять на содержание выполняемого кода, и тех, которые отличаются от стандарта используемого языка. В случаях, когда оценщику предоставляется исходный код, ему также следует предоставить информацию по используемым опциям компиляции и сборки.

В документации инструментальных средств проектирования и разработки аппаратных средств следует описать использование всех опций, которые влияют на результаты применения инструментальных средств (например детальные аппаратные спецификации или сами аппаратные средства).

На этом уровне доверия документация инструментальных средств разработки, используемых субподрядчиками ОО, должна быть также исследована оценщиком.

12.8.4.5 Действие ALC_TAT.3.2E

12.8.4.5.1 Шаг оценивания ALC_TAT.3-4

Оценщик должен исследовать аспекты процесса реализации, чтобы сделать заключение о том, что были применены документированные стандарты реализации.

Этот шаг оценивания требует, чтобы оценщик проанализировал предоставленное ему представление реализации ОО для вынесения заключения о том, были ли применены документированные стандарты реализации.

Оценщику следует верифицировать, что конструкции, исключенные из документированного стандарта, не используются.

Кроме того, оценщику следует проверить процедуры разработчика, которые обеспечивают применение определенных стандартов в пределах процесса проектирования и реализации ОО. Поэтому, помимо получения письменного свидетельства, оценщику следует посетить среду проектирования. Посещение среды проектирования позволит оценщику:

a) наблюдать за применением определенных стандартов;

b) исследовать письменное свидетельство применения процедур, описывающих использование определенных стандартов;

c) провести интервью с сотрудниками, ответственными за разработку, чтобы проверить наличие у них понимания относительно применения определенных стандартов и процедур.

Посещение участка разработки — полезное средство для приобретения доверия к используемым процедурам. Решение не совершать такой визит следует принимать только после консультации с органом оценки.

Оценщик сравнивает предоставленное ему представление реализации с описанием применяемых стандартов реализации и верифицирует их использование.

На этом уровне доверия требуется, чтобы всё представление реализации ФБО было целиком основано на стандартах реализации, включая части, разработанные субподрядчиками и сторонними разработчиками. Из-за этого оценщику может потребоваться посетить заявителей. Оценщик может сверяться со списком конфигурации, требуемым в семействе «Область УК» (ALC_CMS), для получения информации о том, какие именно части разработаны какими разработчиками.

Следует отметить, что части ОО, которые не относятся к ФБО, не должны исследоваться.

Этот шаг оценивания может быть выполнен в сочетании с действиями оценивания по ADV_IMP.

13 Класс ATE: Тестирование

13.1 Введение

Вид деятельности «Тестирование» предназначен для того, чтобы сделать заключение, ведет ли себя ОО так, как описано в ЗБ и как определено в свидетельствах оценки (описанных в классе ADV). Данная цель достигается путем комбинирования функционального тестирования, проводимого разработчиком (ATE_FUN «Функциональное тестирование») и независимого тестирования, проводимого оценщиком (ATE_IND «Независимое тестирование»). На самом низком уровне доверия нет требования по вовлечению в процесс оценки разработчика. Таким образом, единственное тестирование проводится оценщиком, причем он использует только некоторую ограниченную информацию об ОО, доступную ему. Дополнительное доверие приобретается путем всё большего вовлечения разработчика и в процесс тестирования и в процесс предоставления оценщику дополнительной информации об ОО, а также последовательным увеличением проводимых оценщиком действий по независимому тестированию.

13.2 Замечания по применению

Тестирование ФБО проводится оценщиком и, в большинстве случаев, разработчиком. Усилия по тестированию оценщика состоят не только из создания и проведения оригинальных тестов, но также и из оценки достаточности тестов разработчика и повторного проведения всего их подмножества.

Оценщик анализирует тесты, проведённые разработчиком, чтобы сделать заключение о том, насколько они достаточны для демонстрации того, что ИФБО (см. ADV_FSP «Функциональная спецификация») функционируют определенным образом, и для понимания подхода разработчика к тестированию. Точно так же оценщик анализирует тесты, проведённые разработчиком, чтобы сделать заключение о том, насколько они достаточны для демонстрации внутреннего режима функционирования и свойств ФБО.

Оценщик также выполняет подмножество документированных тестов разработчика в целях приобретения доверия к результатам испытаний, проводимых разработчиком: оценщик будет использовать результаты этого анализа как исходные данные для независимого тестирования подмножества ФБО. Относительно этого подмножества оценщик применяет подход к тестированию, который отличается от подхода, применяемого разработчиком, особенно если в тестировании, проводимом разработчиком, имеются недостатки.

Для вынесения заключения о том, является ли тестовая документация разработчика достаточной, или для разработки новых тестов, оценщику необходимо понять желаемый и ожидаемый режим функционирования ФБО, как внутренний, так и явный через ИФБО, в контексте тех ФТБ, которым должны удовлетворять эти ФБО. Оценщик может решить разделить ФБО и ИФБО по подмножествам согласно функциональным областям ЗБ (подсистема аудита, связанный с аудитом ИФБО, модуль аутентификации, связанный с аутентификацией ИФБО, и т.д.), если они не были уже разделены подобным образом в ЗБ, и сосредоточить усилия на одном подмножестве ФБО и ИФБО единовременно, исследуя требования в ЗБ и соответствующие части документации разработки и руководств в целях получения понимания ожидаемого режима функционирования ОО. Эта зависимость от документации разработки подчеркивает необходимость зависимости семейств «Покрытие» (ATE_COV) и «Глубина» (ATE_DPT) от класса ADV.

В ИСО/МЭК 15408 для повышения гибкости при применении компонентов семейств вопросы тестирования покрытия глубины рассматриваются отдельно от функциональных тестов. Однако требования соответствующих семейств предназначены для совместного применения для подтверждения того, что ФБО выполняются согласно их спецификации. Такая тесная связь семейств приводит к некоторому дублированию работы оценщика по подвидам деятельности. Настоящие замечания по применению используются для минимизации повторения текста при описании подвидов деятельности.

13.2.1 Понимание ожидаемого режима функционирования ОО

Прежде чем достаточность тестовой документации может быть надлежащим образом оценена, и прежде чем могут быть созданы новые тесты, оценщику необходимо понять желательный ожидаемый режим выполнения функций безопасности в контексте требований, которым они должны удовлетворять.

Как упоминалось ранее, оценщик может решить разделить ФБО и ИФБО по подмножествам в соответствии с ФТБ в ЗБ (аудит, аутентификация и т.д.) и анализировать подмножества поочередно, по одному за раз. Оценщик исследует каждое требование в ЗБ и соответствующие части функциональной спецификации и руководств для получения понимания ожидаемого режима функционирования ОО. А также оценщик исследует соответствующие части проекта ОО и документации по архитектуре безопасности для получения понимания ожидаемого режима функционирования связанных модулей подсистем ФБО.

С пониманием ожидаемого режима функционирования, оценщик исследует план тестирования, чтобы понять подход к тестированию. В большинстве случаев подход к тестированию будет предусматривать инициирование выполнения некоторой функции безопасности через интерфейсы и наблюдение ее реакции. Внешне видимые функции могут быть протестированы напрямую; однако, могут быть случаи, когда функция безопасности не является внешне видимой для ОО и не может быть адекватно протестирована через интерфейс (как, например в случае с тестированием функциональных возможностей защиты остаточной информации); в подобных случаях необходимо использовать другой способ.

13.2.2 Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности

В тех случаях, когда практически нецелесообразно или несоразмерно осуществлять тестирование конкретной функции (в случае, если для неё не предусмотрено внешнего интерфейса ФБО), в плане тестирования следует определить альтернативный подход к верификации ожидаемого режима выполнения. Сделать заключение о пригодности альтернативного подхода — обязанность оценщика. Оценивая пригодность альтернативных подходов, следует учесть, что:

a) приемлемым альтернативным подходом является анализ представления реализации для заключения, что требуемый режим функционирования демонстрируется ОО. Это может означать исследование кода для программного ОО или, возможно, исследование фотошаблона (маски) микросхем для аппаратного ОО.

b) приемлемым является использование свидетельства помодульного или интегрированного тестирования разработчиком, даже если заявленные требования доверия не включают доступность описаний нижнего уровня модулей ОО (например «Подвид деятельности по оценке» ADV_TDS.3) или представления реализации («Представление реализации» ADV_IMP). Если при верификации ожидаемого режима выполнения функции безопасности используется свидетельство помодульного или интегрированного тестирования разработчиком, следует внимательно отнестись к подтверждению того, что данное свидетельство тестирования отражает текущую реализацию ОО. Если конкретная подсистема или модули подверглись изменению после проведения тестирования, то обычно требуется свидетельство, что изменения были отслежены и учтены в ходе анализа или проведения последующего тестирования.

Следует подчеркнуть, что дополнительные по отношению к тестированию усилия с использованием альтернативных подходов следует предпринять только тогда, когда и разработчик, и оценщик сделают заключение, что не существует других практичных способов проведения тестирования ожидаемого режима выполнения некоторой функции безопасности.

13.2.3 Верификация достаточности тестов

Для тестов необходимо заранее установить требуемые начальные условия их выполнения. Они могут быть определены через параметры, которые должны быть установлены, или через установление порядка проведения тестов в тех случаях, когда завершение одного теста устанавливает необходимые предварительные условия выполнения другого теста. Оценщик должен сделать заключение о полноте предварительных условий выполнения тестов и их приемлемости с точки зрения того, что они не приведут к смещению наблюдаемых результатов тестирования по отношению к ожидаемым результатам тестирования.

Шаги тестирования и ожидаемые результаты тестирования определяют действия и параметры, относящиеся к интерфейсам, а также способ верификации ожидаемых результатов, и что они собой представляют. Оценщику следует сделать заключение о согласованности шагов тестирования и ожидаемых результатов тестирования с описаниями ИФБО в функциональной спецификации. Это означает, что для каждой характеристики режима выполнения ИФБО, явным образом описанной в функциональной спецификации, рекомендуется, чтобы имелись тесты и описание ожидаемых результатов тестирования для верифицирования данного режима функционирования.

Основная цель данного вида деятельности состоит в том, чтобы сделать заключение о достаточности тестирования каждой подсистемы, каждого модуля и каждого ИФБО на соответствие режимам выполнения, заявленным в функциональной спецификации, проекте ОО и «Описании архитектуры безопасности». На более высоких уровнях доверия в тестирование включается также тестирование границ и тестирование недостатков. Процедуры тестирования обеспечат понимание того, каким образом разработчиком в ходе тестирования опробовались ИФБО, модули и подсистемы. Оценщик будет использовать данную информацию при разработке дополнительных тестов для независимого тестирования ОО.

13.3 Покрытие (ATE_COV)

13.3.1 Подвид деятельности по оценке (ATE_COV.1)

13.3.1.1 Цели

Цель данного подвида деятельности — сделать заключение, протестировал ли разработчик ИФБО, и демонстрирует ли свидетельство разработчика о покрытии тестами разработчика соответствие между тестами, идентифицированными в тестовой документации, и ИФБО, описанными в функциональной спецификации.

13.3.1.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) тестовая документация;

d) свидетельство о покрытии тестами.

13.3.1.3 Замечания по применению

Материалы анализа покрытия тестами, представляемые разработчиком, требуются для того, чтобы показать соответствие между тестами, предоставленными в качестве свидетельства оценки, и функциональной спецификацией. Однако нет необходимости в том, чтобы в материалах анализа покрытия демонстрировалось, что все ИФБО были подвергнуты тестированию, или что все внешние интерфейсы ОО были подвергнуты тестированию. Подобные недостатки, если они имеют место, рассматриваются оценщиком в процессе выполнения подвида деятельности по независимому тестированию (ATE_IND.2).

13.3.1.4 Действие ATE_COV.1.1E

ИСО/МЭК 15408-3 ATE_COV.1.1C: *Свидетельство покрытия тестами должно демонстрировать соответствие между тестами из тестовой документации и ИФБО из функциональной спецификации.*

13.3.1.4.1 Шаг оценивания ATE_COV.1-1

Оценщик должен исследовать свидетельство о покрытии тестами, чтобы сделать заключение, является ли точным соответствие между тестами, идентифицированными в тестовой документации, и описанными в функциональной спецификации ИФБО.

Демонстрация соответствия может принимать форму таблицы или матрицы. Свидетельство о покрытии тестами, требуемое для рассматриваемого компонента, скорее покажет степень покрытия тестами, а не его полноту. В тех случаях, когда показана недостаточность покрытия, оценщику, чтобы это компенсировать, следует повысить уровень независимого тестирования.

13.3.2 Подвид деятельности по оценке (ATE_COV.2)

13.3.2.1 Цели

Цель данного подвида деятельности — сделать заключение, протестировал ли разработчик ИФБО, и демонстрирует ли свидетельство разработчика о покрытии тестами разработчика соответствие между тестами, идентифицированными в тестовой документации, и ИФБО, описанными в функциональной спецификации.

13.3.2.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) тестовая документация;

d) свидетельство о покрытии тестами.

13.3.2.3 Действие ATE_COV.2.1E

ИСО/МЭК 15408-3 ATE_COV.2.1C: *Анализ покрытия тестами должен демонстрировать соответствие между тестами из тестовой документации и ИФБО из функциональной спецификации.*

13.3.2.3.1 Шаг оценивания ATE_COV.2-1

Оценщик должен исследовать материалы анализа покрытия тестами, чтобы сделать заключение, является ли точным соответствие между тестами, идентифицированными в тестовой документации, и описанными интерфейсами в функциональной спецификации.

Для демонстрации соответствия может быть достаточно простой перекрёстной таблицы. Идентификация тестов и интерфейсов, представленных в испытательном анализе покрытия, должна быть однозначной. Оценщику следует помнить, что это не означает, что все тесты в тестовой документации должны быть прослежены к интерфейсам в функциональной спецификации.

13.3.2.3.2 Шаг оценивания ATE_COV.2-2

Оценщик должен исследовать план тестирования, чтобы сделать заключение, является ли подход к тестированию для каждого интерфейса пригодным для демонстрации ожидаемого режима выполнения данного интерфейса.

Руководство по выполнению этого шага оценивания представлено в:

a) пункте 13.2.1 «Понимание ожидаемого режима функционирования ОО»;

b) пункте 13.2.2 «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

13.3.2.3.3 Шаг оценивания ATE_COV.2-3

Оценщик должен исследовать процедуры тестирования, чтобы сделать заключение, достаточно ли описание предварительных условий тестирования, шагов тестирования и ожидаемого результата (ожидаемых результатов) для тестирования каждого интерфейса.

Руководство по выполнению этих шагов оценивания, которые относятся к функциональной спецификации, представлено в пункте 13.2.3 «Верификация достаточности тестов».

ИСО/МЭК 15408-3 ATE_COV.2.2C: *Анализ покрытия тестами должен демонстрировать, что все ИФБО из функциональной спецификации были подвергнуты тестированию.*

13.3.2.3.4 Шаг оценивания ATE_COV.2-4

Оценщик должен исследовать материалы анализа покрытия тестами, чтобы сделать заключение о полноте соответствия между интерфейсами, описанными в функциональной спецификации, и тестами, идентифицированными в тестовой документации.

Все интерфейсы, которые описаны в функциональной спецификации, должны быть представлены в материалах анализа покрытия тестами и сопоставлены с тестами для утверждения о полноте, хотя исчерпывающее тестирование интерфейсов спецификации не требуется. Неполнота покрытия была бы очевидна, если бы некоторый интерфейс функции безопасности был идентифицирован в материалах анализа покрытия тестами, но никакие тесты не были бы при этом прослежены к нему.

Оценщику следует помнить, что это не означает, что все тесты в тестовой документации должны быть прослежены к интерфейсам в функциональной спецификации.

13.3.3 Подвид деятельности по оценке (ATE_COV.3)

Общее руководство отсутствует; за консультациями по выполнению данного подвида деятельности следует обращаться в конкретную систему оценки.

13.4 Глубина (ATE_DPT)

13.4.1 Подвид деятельности по оценке (ATE_DPT.1)

13.4.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, провел ли разработчик тестирование подсистем ФБО относительно проекта ОО и описания архитектуры безопасности.

13.4.1.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект ОО;

d) описание архитектуры безопасности;

e) тестовая документация;

f) материалы анализа глубины тестирования.

13.4.1.3 Действие ATE_DPT.1.1E

ИСО/МЭК 15408-3 ATE_DPT.1.1C: *Анализ глубины тестирования должен демонстрировать соответствие между тестами из тестовой документации и подсистемами ФБО из проекта ОО.*

13.4.1.3.1 Шаг оценивания ATE_DPT.1-1

Оценщик должен исследовать материалы анализа глубины тестирования, чтобы сделать заключение, что описание режима функционирования подсистем ФБО и их интерфейсов включено в тестовую документацию.

Этот шаг оценивания верифицирует содержание соответствия между тестами и описаниями в проекте ОО. В случаях, когда описание архитектурной прочности ФБО (в семействе ADV_ARC «Архитектура безопасности») ссылается на определенные механизмы, в этом шаге оценивания также верифицируется соответствие между тестами и описаниями режима функционирования таких механизмов.

Для демонстрации соответствия может быть достаточно простой перекрёстной таблицы. Идентификация тестов и взаимодействий/режимов функционирования, представленных в испытательном анализе глубины покрытия, должна быть однозначной.

Оценщику следует помнить, что это не означает, что все тесты в тестовой документации должны быть прослежены к режимам функционирования подсистем или описанию взаимодействий.

13.4.1.3.2 Шаг оценивания ATE_DPT.1-2

Оценщик должен исследовать план тестирования, необходимые предварительные условия, шаги оценивания и ожидаемые результаты оценивания, чтобы сделать заключение, демонстрирует ли подход к тестированию описания режима функционирования режим функционирования подсистем так, как описано в проекте ОО.

Руководство по выполнению этого шага оценивания представлено в:

a) пункте 13.2.1 «Понимание ожидаемого режима функционирования ОО»;

b) пункте 13.2.2 «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

Если описаны интерфейсы подсистем ФБО, режимы функционирования этих подсистем тестируются непосредственно по этим интерфейсам. В ином случае режимы функционирования тестируются по ИФБО. Также тестирование может быть выполнено с использованием комбинации тех и других интерфейсов. Независимо от того, какая стратегия используется, оценщик будет рассматривать ее пригодность для адекватного тестирования режимов функционирования, описанных в проекте ОО.

13.4.1.3.3 Шаг оценивания ATE_DPT.1-3

Оценщик должен исследовать план тестирования, необходимые предварительные условия, шаги оценивания и ожидаемые результаты оценивания, чтобы сделать заключение, демонстрирует ли подход к тестированию описания режима функционирования все взаимодействия между подсистемами так, как описано в проекте ОО.

В то время как предыдущий шаг оценивания касался оценки режимов функционирования подсистем, данный шаг оценивания касается взаимодействия подсистем.

Руководство по выполнению этого шага оценивания представлено в:

a) пункте 13.2.1 «Понимание ожидаемого режима функционирования ОО»;

b) пункте 13.2.2 «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

Если описаны интерфейсы подсистем ФБО, взаимодействие этих подсистем тестируется непосредственно по этим интерфейсам. В ином случае режимы функционирования должны подразумеваться по ИФБО. Независимо от того, какая стратегия используется, оценщик будет рассматривать ее пригодность для адекватного тестирования взаимодействий, описанных в проекте ОО.

ИСО/МЭК 15408-3 ATE_DPT.1.2C: *Анализ глубины тестирования должен демонстрировать, что все подсистемы ФБО в проекте ОО были подвергнуты тестированию.*

13.4.1.3.4 Шаг оценивания ATE_DPT.1-4

Оценщик должен исследовать процедуры тестирования, чтобы сделать заключение о том, тестируются ли все описания режимов функционирования и взаимодействия подсистем ФБО.

На этом шаге оценивания проверяется полнота выполнения шага оценивания ATE_DPT.1-1. Все описания режимов функционирования и взаимодействий подсистем ФБО, представленные в проекте ОО, должны быть подвергнуты тестированию. Неполная глубина тестирования была бы очевидна, если бы описание режима функционирования подсистем ФБО или взаимодействий между ними было бы идентифицировано в проекте ОО, и при этом не проводилось никаких тестов, связанных с этим описанием.

Оценщику следует помнить, что это не означает, что все тесты в тестовой документации должны быть прослежены к взаимодействиям подсистем в проекте ОО.

13.4.2 Подвид деятельности по оценке (ATE_DPT.2)

13.4.2.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, провел ли разработчик тестирование всех подсистем ФБО и осуществляющих выполнение ФТБ модулей относительно проекта ОО и описания архитектуры безопасности.

13.4.2.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект ОО;

d) описание архитектуры безопасности;

e) тестовая документация;

f) материалы анализа глубины тестирования.

13.4.2.3 Действие ATE_DPT.2.1E

ИСО/МЭК 15408-3 ATE_DPT.2.1C: *Анализ глубины тестирования должен демонстрировать соответствие между тестами в тестовой документации и подсистемами ФБО, а также осуществляющими выполнение ФТБ модулями из проекта ОО.*

13.4.2.3.1 Шаг оценивания ATE_DPT.2-1

Оценщик должен исследовать материалы анализа глубины тестирования в целях вынесения заключения о том, что описания режима функционирования подсистем ФБО и их взаимодействий включены в тестовую документацию.

Этот шаг оценивания верифицирует содержание соответствия между тестами и описаниями в проекте ОО. В случаях, когда описание архитектурной прочности ФБО (в семействе ADV_ARC «Архитектура безопасности») ссылается на определенные механизмы, в этом шаге оценивания также верифицируется соответствие между тестами и описаниями режима функционирования таких механизмов.

Для демонстрации соответствия может быть достаточно простой перекрёстной таблицы. Идентификация тестов и взаимодействий/режимов функционирования, представленных в испытательном анализе глубины покрытия, должна быть однозначной.

Оценщику следует помнить, что это не означает, что все тесты в тестовой документации должны быть прослежены к режимам функционирования подсистем или описанию взаимодействий.

13.4.2.3.2 Шаг оценивания ATE_DPT.2-2

Оценщик должен исследовать план тестирования, необходимые предварительные условия, шаги оценивания и ожидаемые результаты оценивания, чтобы сделать заключение, демонстрирует ли подход к тестированию описания режима функционирования режим функционирования подсистем так, как описано в проекте ОО.

Руководство по выполнению этого шага оценивания представлено в:

a) пункте 13.2.1 «Понимание ожидаемого режима функционирования ОО»;

b) пункте 13.2.2 «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

Если описаны интерфейсы подсистем ФБО, режимы функционирования этих подсистем тестируются непосредственно по этим интерфейсам. В ином случае режимы функционирования тестируются по ИФБО. Тестирование может быть выполнено также с использованием комбинации тех и других интерфейсов. Независимо от того, какая стратегия используется, оценщик будет рассматривать ее пригодность для адекватного тестирования режимов функционирования, описанных в проекте ОО.

13.4.2.3.3 Шаг оценивания ATE_DPT.2-3

Оценщик должен исследовать план тестирования, необходимые предварительные условия, шаги оценивания и ожидаемые результаты оценивания, чтобы сделать заключение, демонстрирует ли подход к тестированию описания режима функционирования все взаимодействия между подсистемами так, как описано в проекте ОО.

В то время как предыдущий шаг оценивания касался оценки режимов функционирования подсистем, данный шаг оценивания касается взаимодействия подсистем.

Руководство по выполнению этого шага оценивания представлено в:

a) пункте 13.2.1 «Понимание ожидаемого режима функционирования ОО»;

b) пункте 13.2.2 «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

Если описаны интерфейсы подсистем ФБО, взаимодействие этих подсистем тестируется непосредственно по этим интерфейсам. В ином случае режимы функционирования должны подразумеваться по ИФБО. Независимо от того, какая стратегия используется, оценщик будет рассматривать ее пригодность для адекватного тестирования взаимодействий, описанных в проекте ОО.

13.4.2.3.4 Шаг оценивания ATE_DPT.2-4

Оценщик должен исследовать материалы анализа глубины тестирования в целях вынесения заключения о том, что интерфейсы осуществляющих ФТБ модулей включены в тестовую документацию.

Этот шаг оценивания верифицирует содержание соответствия между тестами и описаниями в проекте ОО. В случаях, когда описание архитектурной прочности ФБО (в семействе ADV_ARC «Архитектура безопасности») ссылается на определенные механизмы на модульном уровне, в этом шаге оценивания также верифицируется соответствие между тестами и описаниями режима функционирования таких механизмов.

Для демонстрации соответствия может быть достаточно простой перекрёстной таблицы. Идентификация тестов и взаимодействий/режимов функционирования, представленных в испытательном анализе глубины покрытия, должна быть однозначной.

Оценщику следует помнить, что это не означает, что все тесты в тестовой документации должны быть прослежены к режимам функционирования подсистем или описанию взаимодействий.

13.4.2.3.5 Шаг оценивания ATE_DPT.2-5

Оценщик должен исследовать план тестирования, необходимые предварительные условия, шаги оценивания и ожидаемые результаты оценивания, чтобы сделать заключение, демонстрирует ли подход к тестированию для каждого интерфейса модуля, осуществляющего выполнение ФТБ, ожидаемый режим функционирования данного интерфейса.

В то время как предыдущий шаг оценивания касался ожидаемого режима функционирования подсистем, данный шаг оценивания касается ожидаемого режима функционирования интерфейсов модулей, осуществляющих выполнение ФТБ, которые охвачены шагом оценивания ATE_DPT.2-4.

Руководство по выполнению этого шага оценивания представлено в:

a) пункте 13.2.1 «Понимание ожидаемого режима функционирования ОО»;

b) пункте 13.2.2 «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

Тестирование ФБО может быть выполнено непосредственно с использованием внешних интерфейсов, внутренних интерфейсов или комбинации тех и других. Независимо от того, какая стратегия используется, оценщик будет рассматривать ее пригодность для адекватного тестирования функций безопасности. В частности, оценщик делает заключение, является ли тестирование с использованием внутренних интерфейсов функций безопасности необходимым, или эти внутренние интерфейсы могут быть надлежащим образом протестированы (хотя и неявным образом) с использованием внешних интерфейсов. Это решение, как и его логическое обоснование, остается за оценщиком.

ИСО/МЭК 15408-3 ATE_DPT.2.2C: *Анализ глубины тестирования должен демонстрировать, что все подсистемы ФБО из проекта ОО были подвергнуты тестированию.*

13.4.2.3.6 Шаг оценивания ATE_DPT.2-6

Оценщик должен исследовать процедуры тестирования, чтобы сделать заключение о том, тестируются ли все описания режимов функционирования и взаимодействия подсистем ФБО.

На этом шаге проверяется полнота выполнения шага оценивания ATE_DPT.2-1. Все описания режимов функционирования и взаимодействий подсистем ФБО, представленные в проекте ОО, должны быть подвергнуты тестированию. Неполная глубина тестирования была бы очевидна, если бы описание режима функционирования подсистем ФБО или взаимодействий между ними было бы идентифицировано в проекте ОО и при этом не проводилось бы никаких тестов, связанных с этим описанием.

Оценщику следует помнить, что это не означает, что все тесты в тестовой документации должны быть прослежены к взаимодействиям подсистем в проекте ОО.

ИСО/МЭК 15408-3 ATE_DPT.2.3C: ***Анализ глубины тестирования должен демонстрировать, что осуществляющие выполнение ФТБ модули из проекта ОО были подвергнуты тестированию.***

13.4.2.3.7 Шаг оценивания ATE_DPT.2-7

Оценщик должен исследовать процедуры тестирования, чтобы сделать заключение о том, тестируются ли все интерфейсы осуществляющих выполнение ФТБ модулей.

На этом шаге проверяется полнота выполнения шага оценивания ATE_DPT.2-4. Все интерфейсы осуществляющих выполнение ФТБ модулей, представленные в проекте ОО, должны быть подвергнуты тестированию. Неполная глубина тестирования была бы очевидна, если бы интерфейс осуществляющего выполнение ФТБ модуля был бы идентифицирован в проекте ОО и при этом не проводилось никаких тестов, связанных с этим интерфейсом.

Оценщику следует помнить, что это не означает, что все тесты в тестовой документации должны быть прослежены к интерфейсам осуществляющих выполнение ФТБ модулей в проекте ОО.

13.4.3 Подвид деятельности по оценке (ATE_DPT.3)

13.4.3.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, провел ли разработчик тестирование всех подсистем ФБО и модулей относительно проекта ОО и описания архитектуры безопасности.

13.4.3.2 Исходные данные

a) ЗБ;

b) функциональная спецификация;

c) проект ОО;

d) описание архитектуры безопасности;

e) тестовая документация;

f) материалы анализа глубины тестирования.

13.4.3.3 Действие ATE_DPT.3.1E

ИСО/МЭК 15408-3 ATE_DPT.3.1C: *Анализ глубины тестирования должен демонстрировать соответствие между тестами из тестовой документации и подсистемами и модулями ФБО из проекта ОО.*

13.4.3.3.1 Шаг оценивания ATE_DPT.3-1

Оценщик должен исследовать материалы анализа глубины тестирования в целях вынесения заключения о том, что описания режима функционирования подсистем ФБО и их взаимодействий включены в тестовую документацию.

Этот шаг оценивания верифицирует содержание соответствия между тестами и описаниями в проекте ОО. Для демонстрации соответствия может быть достаточно простой перекрёстной таблицы. Идентификация тестов и взаимодействий/режимов функционирования, представленных в испытательном анализе глубины покрытия, должна быть однозначной.

Оценщику следует помнить, что это не означает, что все тесты в тестовой документации должны быть прослежены к режимам функционирования подсистем или описанию взаимодействий.

13.4.3.3.2 Шаг оценивания ATE_DPT.3-2

Оценщик должен исследовать план тестирования, необходимые предварительные условия, шаги оценивания и ожидаемые результаты оценивания, чтобы сделать заключение, демонстрирует ли подход к тестированию описания режима функционирования режим функционирования подсистем так, как описано в проекте ОО.

Руководство по выполнению этого шага оценивания представлено в:

a) пункте 13.2.1 «Понимание ожидаемого режима функционирования ОО»;

b) пункте 13.2.2 «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

Если описаны интерфейсы подсистем ФБО, режимы функционирования этих подсистем тестируются непосредственно по этим интерфейсам. В ином случае режимы функционирования тестируются по ИФБО. Также тестирование может быть выполнено с использованием комбинации тех и других интерфейсов. Независимо от того, какая стратегия используется, оценщик будет рассматривать ее пригодность для адекватного тестирования режимов функционирования, описанных в проекте ОО.

13.4.3.3.3 Шаг оценивания ATE_DPT.3-3

Оценщик должен исследовать план тестирования, необходимые предварительные условия, шаги оценивания и ожидаемые результаты оценивания, чтобы сделать заключение, демонстрирует ли подход к тестированию описания режима функционирования взаимодействия между подсистемами так, как описано в проекте ОО.

Руководство по выполнению этого шага оценивания представлено в:

a) пункте 13.2.1 «Понимание ожидаемого режима функционирования ОО»;

b) пункте 13.2.2 «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

В то время как предыдущий шаг оценивания касался оценки режимов функционирования подсистем, данный шаг оценивания касается взаимодействия подсистем.

Если описаны интерфейсы подсистем ФБО, взаимодействие этих подсистем тестируется непосредственно по этим интерфейсам. В ином случае режимы функционирования должны подразумеваться по ИФБО. Независимо от того, какая стратегия используется, оценщик будет рассматривать ее пригодность для адекватного тестирования взаимодействий, описанных в проекте ОО.

13.4.3.3.4 Шаг оценивания ATE_DPT.3-4

Оценщик должен исследовать материалы анализа глубины тестирования в целях вынесения заключения о том, что интерфейсы осуществляющих ФТБ модулей включены в тестовую документацию.

Этот шаг оценивания верифицирует содержание соответствия между тестами и описаниями в проекте ОО. Для демонстрации соответствия может быть достаточно простой перекрёстной таблицы. Идентификация тестов и взаимодействий/режимов функционирования, представленных в испытательном анализе глубины покрытия, должна быть однозначной.

Оценщику следует помнить, что это не означает, что все тесты в тестовой документации должны быть прослежены к режимам функционирования подсистем или описанию взаимодействий.

13.4.3.3.5 Шаг оценивания ATE_DPT.3-5

Оценщик должен исследовать план тестирования, необходимые предварительные условия, шаги оценивания и ожидаемые результаты оценивания, чтобы сделать заключение, демонстрирует ли под-

ход к тестированию для каждого интерфейса модуля, осуществляющего выполнение ФТБ, ожидаемый режим функционирования данного интерфейса.

Руководство по выполнению этого шага оценивания представлено в:

a) пункте 13.2.1 «Понимание ожидаемого режима функционирования ОО»;

b) пункте 13.2.2 «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

Тестирование ФБО может быть выполнено непосредственно с использованием внешних интерфейсов, внутренних интерфейсов или комбинации тех и других. Независимо от того, какая стратегия используется, оценщик будет рассматривать ее пригодность для адекватного тестирования функций безопасности. В частности, оценщик делает заключение, является ли тестирование с использованием внутренних интерфейсов функций безопасности необходимым, или эти внутренние интерфейсы могут быть надлежащим образом протестированы (хотя и неявным образом) с использованием внешних интерфейсов. Это решение, как и его логическое обоснование, остается за оценщиком.

ИСО/МЭК 15408-3 ATE_DPT.3.2C: *Анализ глубины тестирования должен демонстрировать, что все подсистемы ФБО из проекта ОО были подвергнуты тестированию.*

13.4.3.3.6 Шаг оценивания ATE_DPT.3-6

Оценщик должен исследовать процедуры тестирования, чтобы сделать заключение о том, тестируются ли все описания режимов функционирования и взаимодействия подсистем ФБО.

На этом шаге оценивания проверяется полнота выполнения шага оценивания ATE_DPT.3-1. Все описания режимов функционирования и взаимодействий подсистем ФБО, представленные в проекте ОО, должны быть подвергнуты тестированию. Неполная глубина тестирования была бы очевидна, если бы описание режима функционирования подсистем ФБО или взаимодействий между ними было бы идентифицировано в проекте ОО и при этом не проводилось никаких тестов, связанных с этим описанием.

Оценщику следует помнить, что это не означает, что все тесты в тестовой документации должны быть прослежены к взаимодействиям подсистем в проекте ОО.

ИСО/МЭК 15408-3 ATE_DPT.3.3C: *Анализ глубины тестирования должен демонстрировать, что все модули ФБО из проекта ОО были подвергнуты тестированию.*

13.4.3.3.7 Шаг оценивания ATE_DPT.3-7

Оценщик должен исследовать процедуры тестирования, чтобы сделать заключение о том, тестируются ли все интерфейсы осуществляющих выполнение ФТБ модулей.

На этом шаге оценивания проверяется полнота выполнения шага оценивания ATE_DPT.3-4. Все интерфейсы осуществляющих выполнение ФТБ модулей, представленные в проекте ОО, должны быть подвергнуты тестированию. Неполная глубина тестирования была бы очевидна, если бы интерфейс любого модуля ФБО был бы идентифицирован в проекте ОО, и при этом не проводилось никаких тестов, связанных с этим интерфейсом.

Оценщику следует помнить, что это не означает, что все тесты в тестовой документации должны быть прослежены к интерфейсам модулей ФБО в проекте ОО.

13.4.4 Подвид деятельности по оценке (ATE_DPT.4)

Общее руководство отсутствует; за консультациями по выполнению данного подвида деятельности следует обращаться в конкретную систему оценки.

13.5 Функциональное тестирование (ATE_FUN)

13.5.1 Подвид деятельности по оценке (ATE_FUN.1)

13.5.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, выполнил ли разработчик тесты правильным образом и документировал ли тесты в тестовой документации.

13.5.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) тестовая документация.

13.5.1.3 Замечания по применению

Степень требуемого покрытия ФБО тестовой документацией зависит от соответствующего компонента доверия, связанного с покрытием тестами.

Для представленных тестов разработчика оценщик делает заключение, являются ли тесты повторимыми, и определяет степень возможности использования тестов разработчика при проведении оценщиком независимого тестирования. Любой ИФБО, для которого результаты тестирования разра-

ботчиком указывают, что он может не выполняться в соответствии со спецификациями, оценщику следует подвергнуть независимому тестированию, чтобы сделать заключение, выполняется ли он в соответствии со спецификациями или нет.

13.5.1.4 Действие ATE_FUN.1.1E

ИСО/МЭК 15408-3 ATE_FUN.1.1C: *Тестовая документация должна состоять из планов тестирования, а также ожидаемых и фактических результатов тестирования.*

13.5.1.4.1 Шаг оценивания ATE_FUN.1-1

Оценщик должен проверить, что тестовая документация включает планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.

Оценщик проверяет, что планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования включены в тестовую документацию.

ИСО/МЭК 15408-3 ATE_FUN.1.2C: *В планах тестирования должны быть идентифицированы тесты, которые необходимо выполнить, а также должны содержаться описания сценариев проведения каждого теста. В эти сценарии должны быть включены также любые зависимости последовательности выполнения тестов от результатов других тестов.*

13.5.1.4.2 Шаг оценивания ATE_FUN.1-2

Оценщик должен исследовать план тестирования в целях вынесения заключения о том, описаны ли в нем сценарии проведения каждого теста.

Оценщик делает заключение о том, что план тестирования предоставляет информацию об используемой тестовой конфигурации: как о конфигурации ОО, так и о конфигурации любого используемого тестового оборудования. Эта информация должна быть детализирована в достаточной степени для обеспечения воспроизводимости конфигурации.

Оценщик также делает заключение о том, что план тестирования предоставляет информацию о проведении тестирования: о любых необходимых автоматизированных процедурах настройки и установки (и требуются ли для их запуска особые привилегии), о требуемых исходных данных и способе их применения, о получении выходной информации, о любых автоматизированных процедурах очистки (и требуются ли для их запуска особые привилегии) и т.д. Эту информацию следует детализировать в достаточной степени для обеспечения воспроизводимости хода тестирования.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

13.5.1.4.3 Шаг оценивания ATE_FUN.1-3

Оценщик должен исследовать план тестирования, чтобы сделать заключение, согласована ли тестируемая конфигурация ОО с той конфигурацией, которая идентифицирована в ЗБ.

ОО, упомянутому в плане тестирования разработчика, следует иметь ту же уникальную маркировку, которая установлена в соответствии с подвидами деятельности по семейству «Возможности УК» (ALC_CMC) и идентифицирована во введении ЗБ.

В ЗБ может быть определено несколько подлежащих оценке конфигураций. Оценщик верифицирует, что в тестовой документации разработчика определены тестируемые конфигурации, и они согласованы соответственно с каждой из оцениваемых конфигураций, описанных в ЗБ. Например, в ЗБ могут быть определены параметры конфигурации, которые должны быть установлены, причем эти параметры могут оказать влияние на композицию ОО включением или исключением некоторых дополнительных частей. Оценщик верифицирует, что все подобные конфигурации ОО рассмотрены в тестовой документации.

Оценщику следует рассмотреть описанные в ЗБ цели безопасности среды ОО, которые могут быть применимы для среды тестирования. В ЗБ могут быть цели безопасности среды функционирования, которые не применимы для среды тестирования. Например, цель по допуску пользователей может быть не применима для среды тестирования, однако цель безопасности относительно единой точки подключения к сети, как правило, применима для среды тестирования.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Если этот шаг оценивания применяется к ОО-компоненту, который может использоваться/объединяться с другими ОО в составной ОО (см. класс АСО «Композиция»), то применимо следующее. В тех случаях, когда оцениваемый ОО-компонент зависит от других компонентов среды функционирования для поддержания функционирования, разработчик может рассмотреть использование другого компонента (компонентов) из тех, что будут использоваться в составном ОО для выполнения требования, согласно которому среда функционирования должна являться одной из тестовых конфигураций. Это уменьшит объем дополнительного тестирования, которое потребуется для оценки составного ОО.

13.5.1.4.4 Шаг оценивания ATE_FUN.1-4

Оценщик должен исследовать план тестирования, чтобы сделать заключение о том, представлены ли достаточные инструкции для воспроизведения начальных условий выполнения тестов, в том числе зависимостей, связанных с порядком выполнения тестов, при наличии таких зависимостей.

Чтобы установить начальные условия выполнения тестов, может потребоваться выполнение некоторых дополнительных действий. Например, необходимо добавить учетные записи пользователей прежде, чем начнется проверка возможности их удаления. Пример влияния последовательности выполнения тестов на результаты других тестов — необходимость выполнения до проведения в рамках тестирования действий по поиску и сортировке отчетов по аудиту некоторых действий, которые приведут к созданию таких отчетов по аудиту. Другой пример зависимости, связанной с порядком следования тестов — при выполнении одного набора тестов генерируется файл данных, используемых в качестве исходных данных для другого набора тестов.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

ИСО/МЭК 15408-3 ATE_FUN.1.3C: *Ожидаемые результаты тестирования должны продемонстрировать прогнозируемые данные на выходе успешного выполнения тестов.*

13.5.1.4.5 Шаг оценивания ATE_FUN.1-5

Оценщик должен исследовать тестовую документацию, чтобы сделать заключение о достаточности включенных в нее ожидаемых результатов выполнения тестов.

Ожидаемые результаты тестирования необходимы, чтобы сделать заключение, действительно ли тест был успешно выполнен. Описание ожидаемых результатов тестирования является достаточным, если оно однозначно и согласуется с ожидаемым режимом выполнения ФБО, обусловленным подходом к тестированию.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

ИСО/МЭК 15408-3 ATE_FUN.1.4C: *Фактические результаты тестирования должны соответствовать ожидаемым.*

13.5.1.4.6 Шаг оценивания ATE_FUN.1-6

Сравнение представленных разработчиком фактических и ожидаемых результатов тестирования выявит какие бы то ни было несоответствия результатов. Может оказаться, что непосредственное сравнение фактических результатов не может быть сделано до того, как будет выполнено некоторое преобразование или синтез данных. В подобных случаях в тестовой документации разработчика следует описать процесс преобразования или синтеза фактических данных.

Например, разработчику может потребоваться проверить содержимое буфера сообщений после того, как имело место сетевое соединение. Буфер сообщения будет содержать бинарную последовательность. Эта бинарная последовательность, как правило, преобразуется в другую форму представления данных, чтобы сделать тест более содержательным. Преобразование этого бинарного представления данных в представление более верхнего уровня должно быть достаточно подробно описано разработчиком, чтобы позволить оценщику выполнить процесс преобразования (то есть необходимо описать, используется ли синхронный или асинхронный метод передачи данных, а также указать число стоповых битов, битов четности и т.д.).

Следует отметить, что описание процесса, использовавшегося для преобразования или синтеза фактических данных, используется оценщиком не для того, чтобы фактически исполнить необходимую модификацию, а для того, чтобы оценить корректность этого процесса. Преобразование ожидаемых результатов тестирования в формат, позволяющий их легко сравнивать с фактическими результатами тестов, возлагается на разработчика.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

13.5.1.4.7 Шаг оценивания ATE_FUN.1-7

Оценщик должен привести в отчете информацию об усилиях разработчика по тестированию, выделив подход к тестированию, тестируемую конфигурацию, глубину и результаты тестирования.

Информация о тестировании разработчиком, приведенная в ТОО, позволяет оценщику передать общий подход к тестированию и усилия, затраченные разработчиком на тестирование ОО. Смысл предоставления этой информации состоит в том, чтобы привести содержательный краткий обзор усилий разработчика по тестированию. Нет необходимости в том, чтобы информация о тестировании разработчиком в ТОО была точной копией конкретных шагов тестирования или результатов отдельных тестов. Целью является предоставить достаточные подробности, что позволит другим оценщикам и сотрудникам органов оценки получить некоторое понимание относительно подхода разработчика к тестированию, объема выполненного тестирования, тестируемых конфигураций ОО и общих результатов тестирования разработчиком.

Информация об усилиях разработчика по тестированию, которая обычно представлена в соответствующем разделе ТОО, включает:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые тестировались, включая сведения о том, требовался ли некий привилегированный код для настройки тестирования или для последующей очистки памяти;

b) подход к тестированию. Описание общей стратегии тестирования, которую применил разработчик;

c) результаты тестирования. Описание общих результатов тестирования разработчиком.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы предоставить некоторое представление о типе информации, связанной с усилиями разработчика по тестированию, которую следует привести в ТОО.

13.5.2 Подвид деятельности по оценке (ATE_FUN.2)

Общее руководство отсутствует; за консультациями по выполнению данного подвида деятельности следует обращаться в конкретную систему оценки.

13.6 Независимое тестирование (ATE_IND)

13.6.1 Подвид деятельности по оценке (ATE_IND.1)

13.6.1.1 Цели

Цель данного подвида деятельности состоит в том, чтобы путем независимого тестирования подмножества ФБО определить, функционирует ли ОО в соответствии с тем, как определено в функциональной спецификации и в руководствах.

13.6.1.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) руководство пользователя;

d) руководство по подготовительным процедурам;

e) ОО, пригодный для тестирования.

13.6.1.3 Действие ATE_IND.1.1E

ИСО/МЭК 15408-3 ATE_IND.1.1C: *ОО должен быть пригоден для тестирования.*

13.6.1.3.1 Шаг оценивания ATE_IND.1-1

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, предоставленный оценщику для тестирования, следует иметь ту же уникальную маркировку, которая установлена в соответствии с подвидами деятельности семейства ALC_CMC «Возможности УК» и идентифицирована во введении ЗБ.

В ЗБ может быть определено более одной конфигурации, подлежащей оценке. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию в соответствии с ЗБ. Тестируемые оценщиком конфигурации ОО должны быть согласованы соответственно с каждой из оцениваемых конфигураций, описанных в ЗБ.

Оценщику следует рассмотреть описанные в ЗБ цели безопасности среды ОО, которые могут быть применимы к среде тестирования, и удостовериться, что они достигаются в среде тестирования. В ЗБ могут быть и другие цели безопасности, которые не применимы для среды тестирования. Например, цель безопасности при допуске пользователей не применима к среде тестирования, однако цель безопасности по единой точке подключения к сети применима к среде тестирования.

При использовании каких бы то ни было средств тестирования (например измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика.

13.6.1.3.2 Шаг оценивания ATE_IND.1-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами. Например, предшествующее успешное завершение подвида деятельности AGD_PRE.1 позволит считать удовлетворенным данный шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был правильно установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить, сгенерировать и запустить ОО, используя только поставляемое руководство.

Если оценщику приходится выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данный шаг оценивания мог бы удовлетворить выполнению шага оценивания AGD_PRE.1-3.

13.6.1.4 Действие ATE_IND.1.2E

13.6.1.4.1 Шаг оценивания ATE_IND.1-3

Оценщик должен продумать тестируемое подмножество.

Оценщик выбирает тестируемое подмножество и стратегию тестирования, которые являются приемлемыми для ОО. Одна, крайняя, стратегия тестирования предусматривает наличие тестируемого подмножества, содержащего как можно большее количество интерфейсов, тестируемых с небольшой строгостью. Другая стратегия тестирования предусматривает наличие тестируемого подмножества, содержащего небольшое количество интерфейсов, исходя из их осознанной значимости, и строгое тестирование этих интерфейсов.

Как правило, рекомендуется, чтобы подход к тестированию, принятый оценщиком, находился где-то между этими двумя крайностями. Оценщику следует проверить выполнение большинства интерфейсов, используя, по крайней мере, один тест для каждого, но при этом нет необходимости, чтобы тестирование продемонстрировало исчерпывающую проверку спецификаций.

При выборе подмножества тестируемых интерфейсов оценщику следует рассмотреть следующие факторы:

a) число интерфейсов, из которых необходимо сформировать тестируемое подмножество. В тех случаях, когда у ОО только небольшое число относительно простых интерфейсов, может быть целесообразным строгое тестирование всех функций безопасности. В ином случае это будет нерентабельно и потребуется осуществление выборки;

b) поддержание некоторого баланса между видами деятельности по оценке. Следует, чтобы усилия оценщика по тестированию были соизмеримы с другими усилиями по оценке.

Оценщик выбирает определенные функции безопасности для формирования соответствующего подмножества. Этот выбор будет зависеть от ряда факторов, и рассмотрение этих факторов также может влиять на выбор размера тестируемого подмножества ФБО:

a) значимость интерфейсов. Те интерфейсы, которые более значимы, чем другие, с точки зрения целей безопасности для ОО, следует включать в тестируемое подмножество. Один из основных факторов «значимости» — значение для безопасности (осуществляющие выполнение ФТБ интерфейсы более значимы, чем поддерживающие выполнение ФТБ, а те, в свою очередь, более значимы, чем не влияющие на выполнение ФТБ; см. подраздел ИСО/МЭК 15408-3 ADV_FSP «Функциональная спецификация»). Еще одним важным фактором является число ФТБ, прослеживаемых к данному интерфейсу (как определяется при идентификации соответствия между уровнями представления в классе ADV):

b) сложность интерфейса. Для сложных интерфейсов может потребоваться выполнение сложных тестов, налагающих обременительные требования на разработчика или оценщика, которые, в свою очередь, не будут способствовать экономичным оценкам. С другой стороны, сложные интерфейсы — это вероятная область поиска ошибок и подходящие кандидаты для включения в подмножество. Оценщику необходимо достигнуть баланса между этими соображениями;

c) неявное тестирование. Тестирование некоторых функций безопасности может зачастую сопровождаться неявным тестированием других функций безопасности, и их включение в подмножество может максимизировать (хотя и не в явном виде) число тестируемых функций безопасности. Некоторые интерфейсы обычно могут использоваться для обеспечения нескольких функциональных возможностей безопасности, и их следует сделать объектом эффективного подхода к тестированию;

d) типы интерфейсов ОО (например программный интерфейс, командная строка, протокол). Оценщику следует рассмотреть вопрос о включении тестов для всех различных типов интерфейсов, которые поддерживает данный ОО;

e) интерфейсы, которые вызывают инновационные или необычные функции. В тех случаях, когда в ОО включены инновационные или необычные функции безопасности, которые могут широко быть представлены в маркетинговой литературе и руководствах, им следует быть прямыми кандидатами на тестирование.

В приведенном выше руководстве сформулированы факторы, которые необходимо рассмотреть в процессе выбора приемлемого тестируемого подмножества ФБО, но они ни в коем случае не являются исчерпывающими.

13.6.1.4.2 Шаг оценивания ATE_IND.1-4

Оценщик должен разработать тестовую документацию для тестируемого подмножества, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов.

Уяснив из ЗБ и функциональной спецификации ожидаемый режим выполнения ФБО, оценщик должен определить наиболее подходящий способ тестирования интерфейса. Оценщик особенно внимательно рассматривает:

a) подход, который будет использоваться, например в случае, если будет тестироваться внешний интерфейс, внутренний интерфейс с использованием каких-либо средств автономного тестирования или будет использован альтернативный тестированию подход (например в исключительных обстоятельствах — исследование кода, если оценщику доступно представление реализации);

b) интерфейс(ы), который(е) будет(ут) использоваться для тестирования и наблюдения реакций интерфейса;

c) начальные условия, которые будут необходимы для выполнения теста (т.е. любые конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

d) специальное оборудование для тестирования, которое потребуется либо для инициирования функции безопасности (например генераторы пакетов), либо для наблюдения за функцией безопасности (например сетевые анализаторы).

Оценщик может посчитать целесообразным протестировать каждый интерфейс, используя ряд наборов тестов, где каждый набор будет использоваться для тестирования очень специфичного аспекта ожидаемого режима функционирования интерфейса.

В тестовой документации оценщика следует определить происхождение каждого теста, прослеживая его к соответствующему интерфейсу.

13.6.1.4.3 Шаг оценивания ATE_IND.1-5

Оценщик должен провести тестирование.

Оценщик использует разработанную тестовую документацию как основу для выполнения тестов по отношению к ОО. Тестовая документация используется как основа для тестирования, но это не мешает оценщику выполнить дополнительные специальные тесты. Оценщик может разработать новые тесты, исходя из режима функционирования ОО, обнаруженного в процессе тестирования. Эти новые тесты заносятся в тестовую документацию.

13.6.1.4.4 Шаг оценивания ATE_IND.1-6

Оценщик должен зафиксировать следующую информацию о тестах, которые составляют подмножество тестирования:

a) идентификационную информацию тестируемого режима выполнения интерфейса;

b) инструкции по подключению и настройке всего требуемого тестового оборудования для проведения конкретного теста;

c) инструкции по установке всех предварительных условий выполнения теста;

d) инструкции по инициированию функции безопасности;

e) инструкции по наблюдению режима выполнения интерфейса;

f) описание всех ожидаемых результатов и необходимого анализа, который выполняется по отношению к наблюдаемому режиму выполнения для сравнения с ожидаемыми результатами;

g) инструкции по завершению тестирования и установке необходимого послетестового состояния ОО;

h) фактические результаты тестирования.

Необходимо, чтобы уровень детализации был таким, чтобы другой оценщик мог повторить тесты и получить эквивалентный результат. Хотя некоторые специфические детали результатов выполнения теста могут отличаться (например поля времени и даты в записи аудита), рекомендуется, чтобы общие результаты были идентичными.

Возможны случаи, когда нет необходимости предоставлять всю информацию, представленную на этом шаге оценивания (например фактические результаты тестирования могут не требовать какого бы то ни было анализа до их сравнения с ожидаемыми результатами). Решение опустить эту информацию, как и его логическое обоснование, остается за оценщиком.

13.6.1.4.5 Шаг оценивания ATE_IND.1-7

Оценщик должен проверить, что все фактические результаты тестирования согласуются с ожидаемыми результатами тестирования.

Любые различия в фактических и ожидаемых результатах тестирования могут свидетельствовать либо о том, что ОО не функционирует в соответствии со спецификацией, либо о том, что тестовая документация оценщика может быть некорректной. Не соответствующие ожидаемым фактические результаты тестирования могут потребовать внесения корректив в ОО или тестовую документацию, а также, возможно, повторного выполнения вызвавших коллизию тестов, модификации размера и состава выборки тестов. Это решение, как и его логическое обоснование, остается за оценщиком.

13.6.1.4.6 Шаг оценивания ATE_IND.1-8

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

Информация оценщика о тестировании, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию и усилия, затраченные в течение оценки на вид деятельности по тестированию. Смысл предоставления этой информации состоит в том, чтобы привести содержательный краткий обзор усилий по тестированию. Не имеется в виду, чтобы информация о тестировании в ТОО была точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов. Целью является предоставление достаточных подробностей, чтобы позволить другим оценщикам и сотрудникам органов оценки получить некоторое понимание выбранного подхода к тестированию, объема выполненного тестирования, тестируемых конфигураций ОО и общих результатов вида деятельности по тестированию.

Информация об усилиях оценщика по тестированию, которая обычно представлена в соответствующем разделе ТОО, включает:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые тестировались;

b) выбранный размер подмножества. Количество протестированных в течение оценки интерфейсов и логическое обоснование этого размера;

c) критерии выбора интерфейсов, которые составляют тестируемое подмножество. Краткое изложение факторов, рассмотренных при отборе интерфейсов для включения в подмножество;

d) протестированные интерфейсы. Краткий перечень интерфейсов, обоснованно включенных в подмножество;

e) вердикт по виду деятельности. Общий вывод по результатам тестирования, проведенного в течение оценки.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы предоставить некоторое представление о типе информации, касающейся тестирования, выполненного оценщиком в течение оценки, которую следует привести в ТОО.

13.6.2 Подвид деятельности по оценке (ATE_IND.2)

13.6.2.1 Цели

Цель данного подвида деятельности состоит в том, чтобы путем независимого тестирования некоторого подмножества ФБО сделать заключение, соответствуют ли спецификациям режимы функционирования ОО, и повысить уверенность в результатах тестирования разработчиком путем выполнения выборки тестов разработчика.

13.6.2.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) описание проекта ОО;

d) руководство пользователя;

e) руководство по подготовительным процедурам;

f) документация управления конфигурацией;

g) тестовая документация;

h) ОО, пригодный для тестирования.

13.6.2.3 Действие ATE_IND.2.1E

ИСО/МЭК 15408-3 ATE_IND.2.1C: *ОО должен быть пригоден для тестирования.*

13.6.2.3.1 Шаг оценивания ATE_IND.2-1

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, используемому оценщиком для тестирования, следует иметь ту же уникальную маркировку, которая установлена в соответствии с подвидами деятельности семейства ALC_CMC «Возможности УК» и идентифицирована во введении ЗБ.

В ЗБ может быть определено более одной подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию в соответствии с ЗБ. Тестируемые оценщиком конфигурации ОО должны быть согласованы соответственно с каждой из оцениваемых конфигураций, описанных в ЗБ.

Оценщику следует рассмотреть описанные в ЗБ цели безопасности среды ОО, которые могут быть применимы к среде тестирования, и удостовериться, что они достигаются в среде тестирования. В ЗБ могут быть и другие цели безопасности, которые не применимы для среды тестирования. Например, цель безопасности при допуске пользователей не применима к среде тестирования, однако, цель безопасности по единой точке подключения к сети применима к среде тестирования.

При использовании каких бы то ни было средств тестирования (например измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика.

13.6.2.3.2 Шаг оценивания ATE_IND.2-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами. Например, предшествующее успешное завершение подвида деятельности AGD_PRE.1 позволит считать удовлетворенным данный шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был правильно установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить, сгенерировать и запустить ОО, используя только поставляемое руководство.

Если оценщику приходится выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данный шаг оценивания мог бы удовлетворить выполнению шага оценивания AGD_PRE.1-3.

ИСО/МЭК 15408-3 ATE_IND.2.2C: *Разработчик должен представить набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.*

13.6.2.3.3 Шаг оценивания ATE_IND.2-3

Оценщик должен исследовать набор ресурсов, предоставленных разработчиком, чтобы сделать заключение, эквивалентны ли они набору ресурсов, использовавшимся разработчиком для функционального тестирования ФБО.

Данный набор ресурсов, использовавшихся разработчиком, документируется в плане тестирования, как рассмотрено в семействе ATE_FUN «Функциональное тестирование». Набор ресурсов может, кроме всего прочего, включать доступ к лабораториям и специальное оборудование для тестирования. Ресурсы, которые не являются идентичными ресурсам, использовавшимся разработчиком, должны быть эквивалентны им с точки зрения любого влияния, которое они могут оказать на результаты тестирования.

13.6.2.4 Действие ATE_IND.2.2E

13.6.2.4.1 Шаг оценивания ATE_IND.2-4

Общая цель этого шага оценивания состоит в том, чтобы выполнить достаточное число тестов разработчика для подтверждения обоснованности результатов тестирования, проведенного разработчиком. Оценщик должен выбрать объем выборки и те тесты разработчика, которые будут включены в выборку (см. А.2).

Все тесты разработчика могут быть прослежены до определенных интерфейсов. Поэтому факторы, которые необходимо рассмотреть при выборке тестов, будут такими же, как перечисленные в подмножестве выборки шага оценивания ATE_IND.2-6. Кроме того, оценщик может использовать случайный метод осуществления выборки для выборки тестов, проведенных разработчиком.

13.6.2.4.2 Шаг оценивания ATE_IND.2-5

Оценщик должен проверить, что все фактические результаты тестирования согласуются с ожидаемыми результатами тестирования.

Выявление несогласованностей между ожидаемыми результатами тестирования, проведенного разработчиком и фактическими результатами тестирования, могут заставить оценщика решать такие несоответствия. Несогласованности, которые выявляет оценщик, могут быть решены достаточным обоснованием и дальнейшим разрешением несогласованностей разработчиком.

Если нельзя предоставить достаточное обоснование или решение, доверие оценщика к результатам тестирования, проведенного разработчиком, уменьшается, и оценщику может потребоваться увеличить объем выборки до такой степени, что подмножество, идентифицированное в шаге оценивания ATE_IND.2-4, адекватно протестировано. Недостатки в тестировании, проведенном разработчиком, должны привести или к корректировке тестов разработчика или к разработке оценщиком новых тестов.

13.6.2.5 Действие ATE_IND.2.3E

13.6.2.5.1 Шаг оценивания ATE_IND.2-6

Оценщик должен продумать тестируемое подмножество.

Оценщик выбирает тестируемое подмножество и стратегию тестирования, которые являются приемлемыми для ОО. Одна, крайняя, стратегия тестирования предусматривает наличие тестируемого подмножества, содержащего как можно большее количество интерфейсов, тестируемых с небольшой строгостью. Другая стратегия тестирования предусматривает наличие тестируемого подмножества, содержащего небольшое количество интерфейсов, исходя из их осознанной значимости, и строгое тестирование этих интерфейсов.

Как правило, подход к тестированию, принятый оценщиком, находится где-то между этими двумя крайностями. Оценщику следует проверить выполнение большинства интерфейсов, используя,

по крайней мере, один тест для каждого, но при этом нет необходимости, чтобы тестирование продемонстрировало исчерпывающую проверку спецификаций.

При выборе подмножества тестируемых интерфейсов оценщику следует рассмотреть следующие факторы:

a) свидетельства тестирования разработчиком. Свидетельства тестирования разработчиком включают: анализ покрытия тестами, анализ глубины тестирования и тестовую документацию. Свидетельства тестирования разработчиком будут обеспечивать понимание того, каким образом разработчиком в ходе тестирования опробовались ФБО. Оценщик будет использовать данную информацию при разработке новых тестов для независимого тестирования ОО. Оценщику следует особенно внимательно рассмотреть:

1) усиление тестирования, выполненного разработчиком для определенного интерфейса. Оценщик может захотеть выполнить большее количество тестов того же типа, чтобы путем изменения параметров более строго протестировать интерфейс;

2) дополнение стратегии тестирования, применявшейся разработчиком для определенного интерфейса. Оценщик может захотеть изменить подход к тестированию определенного интерфейса, применяя для его тестирования другую стратегию тестирования;

b) число интерфейсов, из которых необходимо сформировать тестируемое подмножество. В тех случаях, когда у ОО только небольшое число относительно простых интерфейсов, может быть целесообразным провести строгое тестирование всех интерфейсов. Для ОО с большим числом интерфейсов это будет нерентабельно и потребуется осуществление выборки;

c) поддержание некоторого баланса между видами деятельности по оценке. Усилиям оценщика, затраченным на тестирование, следует быть соразмерными с усилиями, затраченными на любой другой вид деятельности по оценке.

Оценщик выбирает определенные интерфейсы для формирования соответствующего подмножества. Этот выбор будет зависеть от ряда факторов, и рассмотрение этих факторов также может влиять на выбор размера тестируемого подмножества:

a) строгость тестирования разработчиком интерфейсов. Те функции безопасности, которые оценщик определил как требующие дополнительного тестирования, следует включить в тестируемое подмножество;

b) результаты тестирования разработчиком. Если результаты тестов разработчика заставляют оценщика сомневаться в том, что интерфейс выполняется в соответствии со спецификациями, то оценщику следует включить подобные интерфейсы в тестируемое подмножество.

c) значимость функций безопасности. Те функции безопасности, которые более значимы, чем другие, с точки зрения целей безопасности для ОО, следует включить в тестируемое подмножество. Один из основных факторов значимости — значение для безопасности (осуществляющие выполнение ФТБ интерфейсы более значимы, чем поддерживающие выполнение ФТБ, а те, в свою очередь, более значимы, чем не влияющие на выполнение ФТБ; см. подраздел ИСО/МЭК 15408-3 ADV_FSP «Функциональная спецификация»). Еще одним важным фактором является число ФТБ, прослеживаемых к данному интерфейсу (как определяется при идентификации соответствия между уровнями представления в классе ADV);

d) сложность интерфейса. Для сложных интерфейсов может потребоваться выполнение сложных тестов, налагающих обременительные требования на разработчика или оценщика, которые, в свою очередь, не будут способствовать экономичным оценкам. С другой стороны, сложные интерфейсы — это вероятная область поиска ошибок и подходящие кандидаты для включения в подмножество. Оценщику необходимо достигнуть баланса между этими соображениями;

e) неявное тестирование. Тестирование некоторых функций безопасности может зачастую сопровождаться неявным тестированием других функций безопасности, и их включение в подмножество может максимизировать (хотя и не в явном виде) число тестируемых функций безопасности. Некоторые интерфейсы обычно могут использоваться для обеспечения нескольких функциональных возможностей безопасности, и их следует сделать объектом эффективного подхода к тестированию;

f) типы интерфейсов ОО (например программный интерфейс, командная строка, протокол). Оценщику следует рассмотреть вопрос о включении тестов для всех различных типов интерфейсов, которые поддерживает данный ОО;

g) интерфейсы, которые вызывают инновационные или необычные функции. В тех случаях, когда в ОО включены инновационные или необычные функции безопасности, которые могут быть широко представлены в маркетинговой литературе и руководствах, им следует быть прямыми кандидатами на тестирование.

В приведенном выше руководстве сформулированы факторы, которые необходимо рассмотреть в процессе выбора приемлемого тестируемого подмножества ФБО, но они ни в коем случае не являются исчерпывающими.

13.6.2.5.2 Шаг оценивания ATE_IND.2-7

Оценщик должен разработать тестовую документацию для тестируемого подмножества, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов.

Уяснив из ЗБ описания проекта ОО и функциональной спецификации ожидаемый режим выполнения ФБО, оценщик должен определить наиболее подходящий способ тестирования интерфейса. Оценщик особенно внимательно рассматривает:

a) подход, который будет использоваться. Например, будет ли тестироваться внешний интерфейс, внутренний интерфейс с использованием каких-либо средств автономного тестирования или будет использован альтернативный тестированию подход (например в исключительных обстоятельствах — исследование кода);

b) интерфейс(ы), который(е) будет(ут) использоваться для тестирования и наблюдения реакции интерфейса;

c) начальные условия, которые будут необходимы для выполнения теста (т.е. любые конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

d) специальное оборудование для тестирования, которое потребуется либо для инициирования выполнения функции безопасности (например, генераторы пакетов), либо для наблюдения за функцией безопасности (например сетевые анализаторы).

Оценщик может посчитать целесообразным тестировать каждый интерфейс, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования очень специфичного аспекта ожидаемого режима выполнения интерфейса.

В тестовой документации оценщика следует определить происхождение каждого теста, прослеживая его к соответствующему интерфейсу или к нескольким интерфейсам.

13.6.2.5.3 Шаг оценивания ATE_IND.2-8

Оценщик должен провести тестирование.

Оценщик использует разработанную тестовую документацию как основу для выполнения тестов по отношению к ОО. Тестовая документация используется как основа для тестирования, но это не мешает оценщику выполнить дополнительные специальные тесты. Оценщик может разработать новые тесты, исходя из режима функционирования ОО, обнаруженного в процессе тестирования. Эти новые тесты заносятся в тестовую документацию.

13.6.2.5.4 Шаг оценивания ATE_IND.2-9

Оценщик должен зафиксировать следующую информацию о тестах, которые составляют подмножество тестов:

a) идентификационную информацию тестируемого режима выполнения интерфейса;

b) инструкции по подключению и настройке всего требуемого оборудования для тестирования, как это требуется для проведения конкретного теста;

c) инструкции по установке всех предварительных условий выполнения теста;

d) инструкции по инициированию интерфейса;

e) инструкции по наблюдению режима выполнения интерфейса;

f) описание всех ожидаемых результатов и необходимого анализа, который выполняется по отношению к наблюдаемому режиму выполнения для сравнения с ожидаемыми результатами;

g) инструкции по завершению тестирования и установке необходимого послетестового состояния ОО;

h) фактические результаты тестирования.

Уровень детализации должен быть таким, чтобы другой оценщик мог повторить тесты и получить эквивалентный результат. Хотя некоторые специфические детали результатов выполнения теста могут отличаться (например поля времени и даты в записи аудита), общие результаты должны быть идентичными.

Возможны случаи, когда нет необходимости предоставлять всю информацию, представленную на этом шаге оценивания (например фактические результаты тестирования могут не требовать какого бы то ни было анализа до их сравнения с ожидаемыми результатами). Решение опустить эту информацию, как и его логическое обоснование, остается за оценщиком.

13.6.2.5.5 Шаг оценивания ATE_IND.2-10

Оценщик должен проверить, что все фактические результаты тестирования согласуются с ожидаемыми результатами тестирования.

Любые различия в фактических и ожидаемых результатах тестирования могут свидетельствовать либо о том, что ОО не функционирует в соответствии со спецификацией, либо о том, что тестовая доку-

ментация оценщика может быть некорректной. Не соответствующие ожидаемым фактические результаты тестирования могут потребовать внесения корректив в ОО или тестовую документацию, а также, возможно, повторного выполнения вызвавших коллизию тестов, модификации размера и состава выборки тестов. Это решение, как и его логическое обоснование, остается за оценщиком.

13.6.2.5.6 Шаг оценивания ATE_IND.2-11

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

Информация оценщика о тестировании, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию и усилия, затраченные в течение оценки на вид деятельности по тестированию. Смысл предоставления этой информации состоит в том, чтобы привести содержательный краткий обзор усилий по тестированию. Не имеется в виду, чтобы информация о тестировании в ТОО была точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органов оценки получить некоторое понимание выбранного подхода к тестированию, объема выполненного оценщиком тестирования, объема выполненного разработчиком тестирования, тестируемых конфигураций ОО и общих результатов вида деятельности по тестированию.

Информация, относящаяся к усилиям оценщика по тестированию, которая обычно представлена в соответствующем разделе ТОО, включает:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые тестировались;

b) выбранный размер подмножества. Количество протестированных в течение оценки интерфейсов и логическое обоснование этого размера;

c) критерии выбора интерфейсов, которые составляют тестируемое подмножество. Краткое изложение факторов, рассмотренных при отборе интерфейсов для включения в подмножество;

d) протестированные интерфейсы. Краткий перечень интерфейсов, обоснованно включенных в подмножество;

e) выполненные тесты разработчика. Количество выполненных тестов разработчика и краткое описание критериев, использовавшихся для выбора данных тестов;

f) вердикт по виду деятельности. Общий вывод по результатам тестирования, проведенного в течение оценки.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы предоставить некоторое представление о типе информации, касающейся тестирования, выполненного оценщиком в процессе оценки, которую следует привести в ТОО.

13.6.3 Подвид деятельности по оценке (ATE_IND.3)

Общее руководство отсутствует; за консультациями по выполнению данного подвида деятельности следует обращаться в конкретную систему оценки.

14 Класс AVA: Оценка уязвимостей

14.1 Введение

Вид деятельности «Оценка уязвимостей» предназначен для того, чтобы сделать заключение о возможности использования недостатков или уязвимостей в ОО в среде функционирования. Это заключение выносится на основании анализа свидетельств оценки и поиска оценщиком общедоступных материалов и поддерживается тестированием проникновения, проводимым оценщиком.

14.2 Анализ уязвимостей (AVA_VAN)

14.2.1 Подвид деятельности по оценке (AVA_VAN.1)

14.2.1.1 Цели

Цель данного подвида деятельности — сделать заключение, имеет ли ОО, находящийся в своей среде функционирования, легко идентифицируемые уязвимости, пригодные для использования.

14.2.1.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) документация руководств;

c) ОО, пригодный для тестирования;

d) общедоступная информация, для поддержки идентификации потенциальных уязвимостей.

Другие исходные данные для данного подвида деятельности:

а) текущая информация, касающаяся потенциальных уязвимостей (например от органа оценки).

14.2.1.3 Замечания по применению

Оценщику следует рассмотреть необходимость выполнения дополнительных тестов в случае, если при проведении других действий по оценке он обнаружил потенциальные уязвимости.

Использование термина «руководства» в этом подвиде деятельности относится к руководству пользователя по эксплуатации и к руководству по подготовительным процедурам.

Информация об уязвимостях может быть или не быть в общедоступных источниках; потенциальные уязвимости могут требовать или не требовать опыта для их использования. Эти два аспекта являются связанными, но различными. Не следует предполагать, что уязвимость может быть легко использована просто потому, что она может быть идентифицирована на основе информации из общедоступных источников.

14.2.1.4 Действие AVA_VAN.1.1E

ИСО/МЭК 15408-3 AVA_VAN.1.1C: *ОО должен быть пригоден для тестирования.*

14.2.1.4.1 Шаг оценивания AVA_VAN.1-1

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, предоставленному разработчиком и идентифицированному в плане тестирования, следует иметь ту же уникальную маркировку, которая установлена в соответствии с подвидами деятельности ALC_CMC «Возможности УК» и идентифицирована во введении ЗБ.

В ЗБ может быть определено более одной подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию в соответствии с ЗБ. Оценщик верифицирует, что все тестируемые конфигурации согласованы с ЗБ.

Оценщику следует рассмотреть описанные в ЗБ цели безопасности для среды функционирования ОО, которые могут быть применимы к среде тестирования, и удостовериться, что они достигаются в среде тестирования. В ЗБ могут быть и другие цели безопасности, которые не применимы для среды тестирования. Например, цель безопасности относительно допусков пользователей не применима к среде тестирования, однако, цель безопасности относительно единой точки подключения к сети могла бы быть применима к среде тестирования.

При использовании каких бы то ни было средств тестирования (например измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика.

14.2.1.4.2 Шаг оценивания AVA_VAN.1-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами. Например, предшествующее успешное завершение подвида деятельности AGD_PRE.1 позволит считать удовлетворенным данный шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был правильно установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить и запустить ОО, используя только поставляемое руководство.

Если оценщику приходится выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данный шаг оценивания мог бы удовлетворить шаг оценивания AGD_PRE.1-3.

14.2.1.5 Действие AVA_VAN.1.2E

14.2.1.5.1 Шаг оценивания AVA_VAN.1-3

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

Оценщик исследует общедоступные источники информации, в целях поддержки идентификации возможных потенциальных уязвимостей в ОО. Существует много общедоступных источников информации, которые следует рассмотреть оценщику. Например, списки рассылки и форумы безопасности в сети Интернет, в которых сообщают об известных уязвимостях в конкретных технологиях.

Оценщику не следует ограничивать рассмотрение общедоступной информации вышеупомянутыми источниками, ему следует рассмотреть любую другую доступную информацию, имеющую отношение к уязвимостям ОО.

В процессе исследования предоставленных разработчиком свидетельств оценщик будет использовать общедоступную информацию для дальнейшего поиска потенциальных уязвимостей. Оценщи-

ку также следует особо рассмотреть всю доступную информацию, касающуюся идентифицированных проблемных областей.

Возможность легкого 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 средств нападения позволяет с высокой степенью вероятности предположить, что данная информация будет использоваться при попытках идентифицировать потенциальные уязвимости в ОО и использовать их. Современные средства поиска 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 сделано в терминах «эффективность-стоимость».

Поиск общедоступной информации следует сосредоточить на тех источниках, которые относятся к конкретному продукту ИТ, на основании которого получен ОО. При определении требуемой широты этого поиска следует рассмотреть следующие факторы: тип ОО, опыт оценщика для данного типа ОО, ожидаемый потенциал нападения и уровень доступных свидетельств согласно классу ADV.

Процесс идентификации является итерационным (повторяющимся), т. е. идентификация одной потенциальной уязвимости может привести к идентификации другой проблемной области, которая требует дальнейшего исследования.

Оценщик приводит в отчете (сообщении), какие действия были предприняты для идентификации потенциальных уязвимостей на основе общедоступной информации. Однако, осуществляя этот тип поиска, оценщик может быть не в состоянии заранее, до начала анализа, описать шаги, которые он предпримет при идентификации потенциальных уязвимостей, поскольку подход может развиваться и претерпевать изменения в зависимости от информации, выявленной в процессе поиска.

Оценщик приводит в отчете, какие свидетельства были исследованы в процессе поиска потенциальных уязвимостей.

14.2.1.5.2 Шаг оценивания AVA_VAN.1-4

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

Может быть идентифицировано, 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 эффективно снизить вероятность использования потенциальной уязвимости для несанкционированного вмешательства в ОО.

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.

14.2.1.6 Действие AVA_VAN.1.3E

14.2.1.6.1 Шаг оценивания AVA_VAN.1-5

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

Оценщик готовит к тестированию проникновения то, что необходимо, чтобы сделать заключение о восприимчивости ОО, находящегося в своей среде функционирования, к потенциальным уязвимостям, идентифицированным в процессе поиска по источникам общедоступной информации. Любая текущая информация об известных потенциальных уязвимостях, предоставленная оценщику третьей стороной (например органом оценки), рассматривается оценщиком наряду с любыми обнаруженными в результате выполнения других действий по оценке потенциальными уязвимостями.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной потенциальной уязвимости.

Не предполагается тестирование оценщиком на предмет наличия потенциальных уязвимостей (в том числе известных из общедоступных источников) помимо тех, для использования которых тре-

буется Базовый потенциал нападения. Однако в некоторых случаях необходимо будет выполнить некоторый тест прежде, чем может быть определена пригодность к использованию. Когда в результате исследований в ходе оценки оценщик обнаруживает некоторую потенциальную уязвимость, для использования которой требуется потенциал нападения выше, чем Базовый, она приводится в ТОО как остаточная уязвимость.

14.2.1.6.2 Шаг оценивания AVA_VAN.1-6

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

a) идентификацию тестируемой потенциальной уязвимости ОО;

b) инструкции по подключению и настройке всего требуемого тестового оборудования, как требуется для проведения конкретного теста проникновения;

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

d) инструкции по инициированию ФБО;

e) инструкции по наблюдению режима выполнения ФБО;

f) описание всех ожидаемых результатов и необходимого анализа, который следует выполнить по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

g) инструкции по завершению теста и установке необходимого послетестового состояния ОО.

Оценщик готовится к тестированию проникновения, основываясь на перечне потенциальных уязвимостей, идентифицированных во время поиска общедоступной информации.

Не предполагается, что оценщик сделает заключение о возможности использования потенциальных уязвимостей помимо тех уязвимостей, для которых требуется Базовый потенциал нападения, чтобы осуществить нападение. Однако в результате исследований в ходе оценки оценщик может обнаружить потенциальную уязвимость, пригодную для использования только нарушителем с большим, чем Базовый, потенциалом нападения. Такие уязвимости необходимо привести в ТОО как остаточные уязвимости.

Поняв потенциальную уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивости ОО. Оценщик особенно внимательно рассматривает:

a) ИФБО или другой интерфейс ОО, который будет использован для инициирования выполнения ФБО и наблюдения их реакции;

b) начальные условия, которые будут необходимы для выполнения теста (т.е. какие-либо конкретные объекты или субъекты, которые необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

c) специальное оборудование для тестирования, которое потребуется либо для инициирования ИФБО, либо для наблюдения за ИФБО (хотя маловероятно, что для использования уязвимости, для которой предполагается Базовый потенциал нападения нарушителя, потребуется специальное оборудование);

d) следует ли заменить теоретическим анализом физическое тестирование, в частности в отношении того, когда результаты первоначального теста могут экстраполироваться для демонстрации того, что повторные попытки нападения, вероятно, будут успешными после выполнения некоторого заданного числа попыток.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной потенциальной уязвимости.

Цель определения данного уровня детализации в тестовой документации — предоставить возможность другому оценщику повторить тесты и получить эквивалентный результат.

14.2.1.6.3 Шаг оценивания AVA_VAN.1-7

Оценщик должен провести тестирование проникновения.

Оценщик использует документацию для тестов проникновения, подготовленную на шаге оценивания AVA_VAN.1-5, как основу для выполнения тестов проникновения по отношению к ОО, но это не препятствует оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может разработать специальные тесты в результате изучения информации в процессе тестирования проникновения, которые, если были выполнены оценщиком, должны быть внесены в документацию тестов проникновения. Такие тесты могут быть необходимы, чтобы исследовать непредвиденные результаты или наблюдения, а также потенциальные уязвимости, о существовании которых оценщик сделал предположение во время предварительно запланированного тестирования.

Не предполагается тестирования оценщиком потенциальных уязвимостей (в том числе известных из общедоступных источников), для использования которых требуется потенциал нападения выше, чем Базовый. Однако, в некоторых случаях необходимо будет выполнить тест прежде, чем может быть определена пригодность к использованию. Если в результате исследований в ходе оценки оценщик обнаружит потенциальную уязвимость, пригодную для использования только нарушителем с большим, чем Базовый, потенциалом нападения, то она должна быть приведена в ТОО как остаточная уязвимость.

14.2.1.6.4 Шаг оценивания AVA_VAN.1-8

Оценщик должен зафиксировать фактические результаты выполнения тестов проникновения.

Хотя некоторые специфические детали фактических результатов выполнения тестов могут отличаться от ожидаемых (например поля времени и даты в записи аудита), общим результатам следует быть идентичными. Следует исследовать любые непредвиденные результаты выполнения тестов. Влияние на оценку следует установить и логически обосновать.

14.2.1.6.5 Шаг оценивания AVA_VAN.1-9

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

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Цель предоставления данной информации состоит в том, чтобы привести содержательный краткий обзор усилий оценщика по тестированию проникновения. Это не означает, что информация в ТОО относительно тестирования проникновения является точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов проникновения. Целью является предоставление достаточных подробностей, чтобы позволить другим оценщикам и сотрудникам органов оценки получить некоторое понимание выбранного подхода к тестированию проникновения, объема выполненного тестирования проникновения, тестируемых конфигураций ОО и общих результатов действий по тестированию проникновения.

Информация об усилиях оценщика по тестированию проникновения, которая обычно представлена в соответствующем разделе ТОО, включает:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые подвергались тестированию проникновения;

b) ИФБО, которые подвергались тестированию проникновения. Краткий перечень ИФБО и других интерфейсов ОО, на которых было сосредоточено тестирование проникновения;

c) вердикт по данному подвиду деятельности. Общий вывод по результатам тестирования проникновения.

Приведенный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы предоставить некоторое представление о типе информации, касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует привести в ТОО.

14.2.1.6.6 Шаг оценивания AVA_VAN.1-10

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 нарушителю, обладающему 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 оценщиком делается отрицательное заключение.

Руководство из приложения В.4 следует использовать для того, чтобы сделать заключение о потенциале нападения, требуемом для использования конкретной уязвимости, и может ли эта уязвимость быть использована в предполагаемой среде функционирования. Может не быть необходимости вычислять потенциал нападения для каждого случая, а только если есть некоторое сомнение относительно того, может ли уязвимость использоваться нарушителем, обладающим потенциалом нападения меньшим, чем Усиленный базовый.

14.2.1.6.7 Шаг оценивания AVA_VAN.1-11

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

a) ее источник (например стала известна при выполнении действий ОМО, известна оценщику, прочитана в публикации);

b) связанные с ней невыполненные ФТБ;

c) описание;

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

e) количество времени, уровень компетентности, уровень знания ОО, уровень возможности доступа, оборудование, требуемые для использования идентифицированных уязвимостей, а также соответствующие значения с использованием таблиц В.2 и В.3 приложения В.4.

14.2.2 Подвид деятельности по оценке (AVA_VAN.2)

14.2.2.1 Цели

Цель данного подвида деятельности — сделать заключение, имеет ли ОО, находящийся в своей среде функционирования, уязвимости, пригодные для использования нарушителями, обладающими Базовым потенциалом нападения.

14.2.2.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект ОО;

d) описание архитектуры безопасности;

e) документация руководств;

f) ОО, пригодный для тестирования;

g) общедоступная информация для поддержки идентификации потенциальных уязвимостей.

Другие неявные свидетельства оценки для этого подвида деятельности зависят от компонентов, которые были включены в пакет доверия. Свидетельства, предоставляемые для каждого компонента, должны использоваться в качестве исходных данных для этого подвида деятельности.

Другие исходные данные для данного подвида деятельности:

a) текущая информация, касающаяся известных из общедоступных источников потенциальных уязвимостей и атак (например от органа оценки).

14.2.2.3 Замечания по применению

Оценщику следует рассмотреть необходимость выполнения дополнительных тестов в случае, если при проведении других действий по оценке он обнаружил потенциальные уязвимости.

14.2.2.4 Действие AVA_VAN.2.1E

ИСО/МЭК 15408-3 AVA_VAN.2.1C: *ОО должен быть пригоден для тестирования.*

14.2.2.4.1 Шаг оценивания AVA_VAN.2-1

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, предоставленному разработчиком и идентифицированному в плане тестирования, следует иметь ту же уникальную маркировку, которая установлена в соответствии с подвидами деятельности ALC_CMC «Возможности УК» и идентифицирована во введении ЗБ.

В ЗБ может быть определено более одной подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию в соответствии с ЗБ. Оценщик верифицирует, что все тестируемые конфигурации согласованы с ЗБ.

Оценщику следует рассмотреть описанные в ЗБ цели безопасности для среды функционирования ОО, которые могут быть применимы к среде тестирования, и удостовериться, что они достигаются в среде тестирования. В ЗБ могут быть и другие цели безопасности, которые не применимы для среды тестирования. Например, цель безопасности относительно допусков пользователей не применима к среде тестирования, однако цель безопасности относительно единой точки подключения к сети применима к среде тестирования.

При использовании каких бы то ни было средств тестирования (например измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика.

14.2.2.4.2 Шаг оценивания AVA_VAN.2-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами. Например, предшествующее успешное завершение подвида деятельности AGD_PRE.1 позволит считать удовлетворенным данный шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был правильно установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить и запустить ОО, используя только поставляемое руководство.

Если оценщику приходится выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данный шаг оценивания мог бы удовлетворить шаг оценивания AGD_PRE.1-3.

14.2.2.5 Действие AVA_VAN.2.2E

14.2.2.5.1 Шаг оценивания AVA_VAN.2-3

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

Оценщик исследует общедоступные источники информации, в целях поддержки идентификации возможных потенциальных уязвимостей в ОО. Существует много общедоступных источников информации, которые следует рассмотреть оценщику. Например, общедоступные ресурсы в мировой сети, включая:

a) специальные публикации (журналы, книги);

b) исследовательские статьи.

Оценщику не следует ограничивать рассмотрение общедоступной информации вышеупомянутыми источниками; ему следует рассмотреть любую другую доступную информацию, имеющую отношение к уязвимостям ОО.

В процессе исследования предоставленных разработчиком свидетельств оценщик будет использовать общедоступную информацию для дальнейшего поиска потенциальных уязвимостей. Оценщику также следует особо рассмотреть всю доступную информацию, касающуюся идентифицированных проблемных областей.

Возможность легкого 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 средств нападения позволяет с высокой степенью вероятности предположить, что данная информация будет использоваться при попытках идентифицировать потенциальные уязвимости в ОО и использовать их. Современные средства поиска 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 сделано в терминах «эффективность-стоимость».

Поиск общедоступной информации следует сосредоточить на тех источниках, которые относятся к конкретному продукту ИТ, на основании которого получен ОО. При определении требуемой широты этого поиска следует рассмотреть следующие факторы: тип ОО, опыт оценщика для данного типа ОО, ожидаемый потенциал нападения и уровень доступных свидетельств согласно классу ADV.

Процесс идентификации является итерационным (повторяющимся), т. е. идентификация одной потенциальной уязвимости может привести к идентификации другой проблемной области, которая требует дальнейшего исследования.

Оценщик приводит в отчете (сообщении), какие действия были предприняты для идентификации потенциальных уязвимостей на основе общедоступной информации. Однако, осуществляя этот тип поиска, оценщик может быть не в состоянии заранее, до начала анализа, описать шаги, которые он предпримет при идентификации потенциальных уязвимостей, поскольку подход может развиваться и претерпевать изменения в зависимости от информации, выявленной в процессе поиска.

Оценщик приводит в отчете, какие свидетельства были исследованы в процессе поиска потенциальных уязвимостей. Выбор свидетельств может производиться на основании идентифицированных оценщиком проблемных областей, связанных со свидетельствами, которые нарушитель, как предполагается, может получить, или согласно другому обоснованию, предложенному оценщиком.

14.2.2.6 Действие AVA_VAN.2.3E

14.2.2.6.1 Шаг оценивания AVA_VAN.2-4

Оценщик должен провести поиск в ЗБ, документации руководств, функциональной спецификации, проекте ОО и описании архитектуры безопасности, чтобы идентифицировать возможные потенциальные уязвимости в ОО.

Следует выполнить поиск свидетельств, посредством которого анализируются спецификации и документация ОО, а после этого выдвигаются гипотезы или делаются предположения о потенциальных уязвимостях в ОО. Затем перечень предполагаемых уязвимостей упорядочивается по приоритетам на основе оцененной вероятности существования потенциальной уязвимости и, предполагая, что уязвимость существует, на основе потенциала нападения, требуемого для ее использования, а также возможностей, предоставляющихся нарушителю, или предполагаемого ущерба, который обусловлен конкретной уязвимостью. Упорядоченный по приоритетам перечень потенциальных уязвимостей используют для управления тестированием проникновения в ОО.

«Описание архитектуры безопасности» предоставляет сведения об анализе уязвимостей, проведенном разработчиком, поскольку в ней документировано, каким образом в ФБО обеспечена собственная защита от вмешательства недоверенных субъектов и предотвращение обхода функциональных возможностей обеспечения безопасности. Поэтому оценщику следует использовать это описание защиты ФБО как основание для поиска возможных способов компрометации ФБО.

Исходя из ФТБ, которые должны выполняться для данного ОО в среде функционирования, оценщику при независимом анализе уязвимостей следует рассмотреть характерные потенциальные уязвимости под каждой из следующих рубрик:

a) потенциальные уязвимости, характерные для конкретного типа оцениваемого ОО, которые могут быть указаны органом оценки;

b) обход;

c) вмешательство;

d) прямые нападения;

e) мониторинг;

f) неправильное применение.

Пункты b) — f) объясняются более детально в приложении В.

«Описание архитектуры безопасности» нужно рассматривать в свете каждой из вышеупомянутых рубрик типовых потенциальных уязвимостей. Каждую потенциальную уязвимость следует рассматривать при поиске возможных способов нарушения защиты ФБО и компрометации ФБО.

14.2.2.6.2 Шаг оценивания AVA_VAN.2-5

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

Может быть идентифицировано, 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 эффективно снизить вероятность использования потенциальной уязвимости для несанкционированного вмешательства в ОО.

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.

14.2.2.7 Действие AVA_VAN.2.4E

14.2.2.7.1 Шаг оценивания AVA_VAN.2-6

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

Оценщик готовит к тестированию проникновения то, что необходимо, чтобы сделать заключение о восприимчивости ОО, находящегося в своей среде функционирования, к потенциальным уязвимостям, идентифицированным в процессе поиска по источникам общедоступной информации. Любая текущая информация об известных потенциальных уязвимостях, предоставленная оценщику третьей стороной (например органом оценки), рассматривается оценщиком наряду с любыми обнаруженными в результате выполнения других действий по оценке потенциальными уязвимостями.

Оценщику следует помнить, что при рассмотрении «Описания архитектуры безопасности» для поиска уязвимостей (как детализировано в AVA_VAN.2-4), следует выполнить тестирование в целях подтверждения архитектурных свойств. Это, вероятно, потребует проведения негативных тестов, чтобы попытаться опровергнуть свойства архитектуры безопасности. При разработке стратегии тестирования проникновения оценщик обеспечивает, чтобы каждая из основных характеристик в «Описании архитектуры безопасности» была протестирована либо при функциональном тестировании (как рассмотрено в разделе 13), либо при тестировании проникновения, проведенном оценщиком.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной потенциальной уязвимости.

Не предполагается тестирования оценщиком на предмет наличия потенциальных уязвимостей (в том числе известных из общедоступных источников) помимо тех, для использования которых требуется Базовый потенциал нападения. Однако в некоторых случаях необходимо будет выполнить некоторый тест прежде, чем может быть определена пригодность к использованию. Когда в результате исследований в ходе оценки оценщик обнаруживает некоторую потенциальную уязвимость, для использования которой требуется потенциал нападения выше, чем Базовый, она приводится в ТОО как остаточная уязвимость.

Руководство по определению необходимого для использования потенциальной уязвимости потенциала нападения представлено в приложении В.4.

Если по поводу потенциальных уязвимостей выдвигают гипотезу, что эти уязвимости могут использовать только нарушители, обладающие усиленным Базовым, Умеренным или Высоким потенциалом нападения, это не приводит к отрицательному заключению по данному действию. В случае, если анализ поддерживает гипотезу, данные потенциальные уязвимости не следует рассматривать далее в качестве исходных данных для тестирования проникновения. Однако такие уязвимости приводятся в ТОО как остаточные.

Потенциальным уязвимостям, по поводу которых выдвигается гипотеза, что эти уязвимости могут использовать нарушители, обладающие Базовым потенциалом нападения и использование которых приводит к нарушению целей безопасности, следует быть самыми высокими по приоритету потенциальными уязвимостями, и их следует включить в перечень, который далее будет использоваться для тестирования проникновения.

14.2.2.7.2 Шаг оценивания AVA_VAN.2-7

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на перечне потенциальных уязвимостей, причем детализация этой документации должна быть достаточна для обеспечения воспроизводимости тестов. Тестовая документация должна включать:

a) идентификацию тестируемой потенциальной уязвимости оцениваемого ОО;

b) инструкции по подключению и настройке всего требуемого тестового оборудования, как требуется для проведения конкретного теста проникновения;

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

d) инструкции по инициированию ФБО;

e) инструкции по наблюдению режима выполнения ФБО;

f) описание всех ожидаемых результатов и необходимого анализа, который следует выполнить по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

g) инструкции по завершению теста и установке необходимого послетестового состояния ОО.

Оценщик готовится к тестированию проникновения, основываясь на перечне потенциальных уязвимостей, идентифицированных во время поиска общедоступной информации и анализа свидетельств.

Не предполагается, что оценщик сделает заключение о возможности использования потенциальных уязвимостей помимо тех, для которых требуется Базовый потенциал нападения, чтобы осуществить нападение. Однако в результате исследований в ходе оценки оценщик может обнаружить потенциальную уязвимость, пригодную для использования только нарушителем с большим, чем Базовый, потенциалом нападения. Такие уязвимости необходимо привести в ТОО как остаточные уязвимости.

Поняв потенциальную уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. Оценщик особенно внимательно рассматривает:

a) ИФБО или другой интерфейс ОО, который будет использован для инициирования выполнения ФБО и наблюдения за их реакцией (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). Следует отметить, что хотя интерфейсы ОО предоставляют средства тестирования свойств ФБО, сами эти интерфейсы не являются предметом тестирования);

b) начальные условия, которые будут необходимы для выполнения теста (т. е. какие-либо конкретные объекты или субъекты, которые необходимы и атрибуты безопасности, которые им необходимо будет иметь);

c) специальное оборудование для тестирования, которое потребуется либо для инициирования ИФБО, либо для наблюдения за ИФБО (хотя маловероятно, что для использования уязвимости, для которой предполагается Базовый потенциал нападения нарушителя, потребуется специальное оборудование);

d) следует ли заменить теоретическим анализом физическое тестирование, в частности в отношении того, когда результаты первоначального теста могут экстраполироваться для демонстрации того, что повторные попытки нападения, вероятно, будут успешными после выполнения некоторого заданного числа попыток.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной потенциальной уязвимости.

Цель определения данного уровня детализации в тестовой документации — предоставить возможность другому оценщику повторить тесты и получить эквивалентный результат.

14.2.2.7.3 Шаг оценивания AVA_VAN.2-8

Оценщик должен провести тестирование проникновения.

Оценщик использует документацию для тестов проникновения, подготовленную на шаге оценивания AVA_VAN.2-6, как основу для выполнения тестов проникновения по отношению к ОО, но это не мешает оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может разработать специальные тесты в результате изучения информации в процессе тестирования проникновения, которые, если были выполнены оценщиком, должны быть внесены в документацию тестов проникновения. Такие тесты могут быть необходимы, чтобы исследовать непредвиденные результаты или наблюдения, а также потенциальные уязвимости, о существовании которых оценщик сделал предположение во время предварительно запланированного тестирования.

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

Не предполагается тестирования оценщиком потенциальных уязвимостей (в том числе известных из общедоступных источников), для использования которых требуется потенциал нападения выше, чем Базовый. Однако в некоторых случаях необходимо будет выполнить тест прежде, чем может быть определена пригодность к использованию. Если в результате исследований в ходе оценки оценщик обнаружит потенциальную уязвимость, пригодную для использования только нарушителем с большим, чем Базовый, потенциалом нападения, то она должна быть приведена в ТОО как остаточная уязвимость.

14.2.2.7.4 Шаг оценивания AVA_VAN.2-9

Оценщик должен зафиксировать фактические результаты тестов проникновения.

Хотя некоторые специфические детали фактических результатов выполнения тестов могут отличаться от ожидаемых (например поля времени и даты в записи аудита), общим результатам следует быть идентичными. Следует исследовать любые непредвиденные результаты выполнения тестов. Влияние на оценку следует установить и логически обосновать.

14.2.2.7.5 Шаг оценивания AVA_VAN.2-10

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

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Цель предоставления данной информации состоит в том, чтобы привести содержательный краткий обзор усилий оценщика по тестированию проникновения. Это не означает, что информация в ТОО относительно тестирования проникновения является точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов проникновения. Целью является предоставление достаточных подробностей, чтобы позволить другим оценщикам и сотрудникам органов оценки получить некоторое понимание выбранного подхода к тестированию проникновения, объема выполненного тестирования проникновения, тестируемых конфигураций ОО и общих результатов действий по тестированию проникновения.

Информация об усилиях оценщика по тестированию проникновения, которая обычно представлена в соответствующем разделе ТОО, включает:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые подвергались тестированию проникновения;

b) ИФБО, которые подвергались тестированию проникновения. Краткий перечень ИФБО и других интерфейсов ОО, на которых было сосредоточено тестирование проникновения;

c) вердикт по данному подвиду деятельности. Общий вывод по результатам тестирования проникновения.

Приведенный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы предоставить некоторое представление о типе информации, касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует привести в ТОО.

14.2.2.7.6 Шаг оценивания 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 нарушителю, обладающему 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 оценщиком делается отрицательное заключение.

Руководство из приложения В.4 следует использовать для того, чтобы сделать заключение о потенциале нападения, требуемом для использования конкретной уязвимости, и может ли эта уязвимость быть использована в предполагаемой среде функционирования. Может не быть необходимости вычислять потенциал нападения для каждого случая, а только если есть некоторое сомнение относительно того, может ли уязвимость использоваться нарушителем, обладающим потенциалом нападения меньшим, чем Усиленный базовый.

14.2.2.7.7 Шаг оценивания AVA_VAN.2-12

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

a) ее источник (например стала известна при выполнении действий ОМО, известна оценщику, прочитана в публикации);

b) связанные с ней невыполненные ФТБ;

c) описание;

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

e) количество времени, уровень компетентности, уровень знания ОО, уровень возможности доступа, оборудование, требуемые для использования идентифицированных уязвимостей, а также соответствующие значения с использованием таблиц В.2 и В.3 приложения В.4.

14.2.3 Подвид деятельности по оценке (AVA_VAN.3)

14.2.3.1 Цели

Цель данного подвида деятельности — сделать заключение, имеет ли ОО, находящийся в своей среде функционирования, уязвимости, пригодные для использования нарушителями, обладающими Усиленным базовым потенциалом нападения.

14.2.3.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект ОО;

d) описание архитектуры безопасности;

e) выбранное подмножество реализации;

f) документация руководств;

g) ОО, пригодный для тестирования;

h) общедоступная информация для поддержки идентификации потенциальных уязвимостей.

Другие неявные свидетельства оценки для этого подвида деятельности зависят от компонентов, которые были включены в пакет доверия. Свидетельства, предоставляемые для каждого компонента, должны использоваться в качестве исходных данных для этого подвида деятельности.

Другие исходные данные для данного подвида деятельности:

a) текущая информация, касающаяся известных из общедоступных источников потенциальных уязвимостей и атак (например от органа оценки).

14.2.3.3 Замечания по применению

В процессе выполнения действий по оценке оценщик может также идентифицировать проблемные области. К ним относятся определенные части свидетельств ОО, которые хотя формально и соответствуют требованиям для конкретной деятельности, с которой связано данное свидетельство, но у оценщика есть по отношению к ним некоторые сомнения. Например, конкретная спецификация интерфейса представляется особенно сложной и поэтому может вызвать ошибку или при разработке ОО, или при функционировании ОО. На данном этапе нет потенциальной уязвимости, поэтому требует-

ся дальнейшее исследование. Это находится вне области выявленных уязвимостей, так как требуется дальнейшее исследование.

Фокусированный подход к идентификации уязвимостей — анализ свидетельств в целях идентификации любых потенциальных уязвимостей, которые становятся очевидны при изучении содержащейся в свидетельствах информации. Такой анализ является неструктурированным, поскольку методика проведения не предопределена. Дальнейшее руководство по поводу направленного анализа уязвимостей представлено в приложении В.2.2.2.2.

14.2.3.4 Действие AVA_VAN.3.1E

ИСО/МЭК 15408-3 AVA_VAN.3.1C: *ОО должен быть пригоден для тестирования.*

14.2.3.4.1 Шаг оценивания AVA_VAN.3-1

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, предоставленному разработчиком и идентифицированному в плане тестирования, следует иметь ту же уникальную маркировку, которая установлена в соответствии с подвидами деятельности семейства ALC_CMC «Возможности УК» и идентифицирована во введении ЗБ.

В ЗБ может быть определено более одной подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию в соответствии с ЗБ. Оценщик верифицирует, что все конфигурации ОО согласованы с ЗБ.

Оценщику следует рассмотреть описанные в ЗБ цели безопасности для среды функционирования ОО, которые могут быть применимы к среде тестирования, и удостовериться, что они достигаются в среде тестирования. В ЗБ могут быть и другие цели безопасности, которые не применимы для среды тестирования. Например, цель безопасности относительно допусков пользователей не применима к среде тестирования, однако цель безопасности относительно единой точки подключения к сети применима к среде тестирования.

При использовании каких бы то ни было средств тестирования (например измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика.

14.2.3.4.2 Шаг оценивания AVA_VAN.3-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами. Например, предшествующее успешное завершение подвида деятельности AGD_PRE.1 позволит считать удовлетворенным данный шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был правильно установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить и запустить ОО, используя только поставляемое руководство.

Если оценщику приходится выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данный шаг оценивания мог бы удовлетворить шаг оценивания AGD_PRE.1-3.

14.2.3.5 Действие AVA_VAN.3.2E

14.2.3.5.1 Шаг оценивания AVA_VAN.3-3

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

Оценщик исследует общедоступные источники информации, в целях поддержки идентификации возможных потенциальных уязвимостей в ОО. Существует много общедоступных источников информации, которые следует рассмотреть оценщику. Например, общедоступные ресурсы в мировой сети, включая:

a) специальные публикации (журналы, книги);

b) исследовательские статьи;

c) материалы конференций.

Оценщику не следует ограничивать рассмотрение общедоступной информации вышеупомянутыми источниками, ему следует рассмотреть любую другую доступную информацию, имеющую отношение к уязвимостям ОО.

В процессе исследования предоставленных разработчиком свидетельств оценщик будет использовать общедоступную информацию для дальнейшего поиска потенциальных уязвимостей. Оценщику также следует особо рассмотреть всю доступную информацию, касающуюся идентифицированных проблемных областей.

Возможность легкого 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 средств нападения позволяет с высокой степенью вероятности предположить, что данная информация будет использоваться при попытках идентифицировать потенциальные уязвимости в ОО и использовать их. Современные средства поиска 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 сделано в терминах «эффективность-стоимость».

Поиск общедоступной информации следует сосредоточить на тех источниках, которые относятся к конкретным технологиям, использованным в разработке продукта ИТ, на основании которого получен ОО. При определении требуемой широты этого поиска следует рассмотреть следующие факторы: тип ОО, опыт оценщика для данного типа ОО, ожидаемый потенциал нападения и уровень доступных свидетельств согласно классу ADV.

Процесс идентификации является итерационным (повторяющимся), т. е. идентификация одной потенциальной уязвимости может привести к идентификации другой проблемной области, которая требует дальнейшего исследования.

Оценщик приводит в отчете (сообщении), какие действия были предприняты для идентификации потенциальных уязвимостей на основе общедоступной информации. Однако, осуществляя этот тип поиска, оценщик может быть не в состоянии заранее, до начала анализа, описать шаги, которые он предпримет при идентификации потенциальных уязвимостей, поскольку подход может развиваться и претерпевать изменения в зависимости от информации, выявленной в процессе поиска.

Оценщик приводит в отчете, какие свидетельства были исследованы в процессе поиска потенциальных уязвимостей. Выбор свидетельств может производиться на основании идентифицированных оценщиком проблемных областей, связанных со свидетельствами, которые нарушитель, как предполагается, может получить, или согласно другому обоснованию, предложенному оценщиком.

14.2.3.6 Действие AVA_VAN.3.3E

14.2.3.6.1 Шаг оценивания AVA_VAN.3-4

Оценщик должен провести фокусированный поиск в ЗБ, документации руководств, функциональной спецификации, проекте ОО и описании архитектуры безопасности и представлении реализации, чтобы идентифицировать возможные потенциальные уязвимости в ОО.

Должна быть использована методология гипотез о недостатках, посредством которой анализируются спецификации и свидетельства разработки, а также руководства, а после этого выдвигаются гипотезы или делаются предположения о потенциальных уязвимостях в ОО.

Оценщик использует знания проекта ОО и функционирования ОО, полученные от изучения поставляемых материалов ОО, чтобы выдвинуть гипотезу о недостатках и идентифицировать потенциальные недостатки в разработке ОО и потенциальные ошибки в специфицированном методе функционирования ОО.

«Описание архитектуры безопасности» предоставляет сведения об анализе уязвимостей, проведенном разработчиком, поскольку в ней документировано, каким образом в ФБО обеспечена собственная защита от вмешательства недоверенных субъектов и предотвращение обхода функциональных возможностей обеспечения безопасности. Таким образом, оценщику следует основываться на своем понимании защиты ФБО, полученном в результате анализа этих свидетельств и расширенном за счет знаний, полученных из других свидетельств по классу ADV, связанных с разработкой.

Принятый подход направлен на проблемные области, идентифицированные во время исследования свидетельств в рамках проведения действий по оценке, и обеспечивает исследование репрезентативной выборки свидетельств, связанных с разработкой и руководствами, предоставленных оценщику.

Руководство по выборке см. в приложении А.2 «Выборка». Это руководство следует использовать при выборе подмножества; в нем даются обоснования:

a) подхода, используемого при выборе;

b) оценки того, что исследуемые свидетельства поддерживают данный подход.

Проблемные области могут касаться достаточности конкретных характеристик безопасности, детализированных в «Описании архитектуры безопасности».

Свидетельства, которые рассматриваются в процессе анализа уязвимостей, могут быть связаны со свидетельствами, к которым, предположительно, может получить доступ нарушитель. Например, разработчик может защищать проект ОО и представления реализации ОО, тогда единственной, предположительно доступной для нарушителя, информацией будет функциональная спецификация

и руководства (общедоступные документы). Таким образом, хотя цели доверия к ОО обеспечивают, что проект ОО и представление реализации отвечают требованиям, эти представления проекта следует исследовать для дальнейшего изучения проблемных областей.

С другой стороны, если источник информации общедоступен, было бы разумно предположить, что нарушитель имеет доступ к данному источнику информации и может использовать эту информацию при попытках осуществления атаки на ОО. Поэтому данный источник нужно рассмотреть при фокусированном подходе к исследованию.

Примеры выборки подмножества свидетельств, которые требуется рассмотреть:

a) Для оценки, когда предоставлены все уровни представления проекта от функциональной спецификации до представления реализации, исследуется информация, которая может быть выбрана в функциональной спецификации и представлении реализации, поскольку в функциональной спецификации предоставлена детализация интерфейсов, доступных нарушителю, и представление реализации включает в себя проектные решения, сделанные для всех других представлений проекта. Поэтому информацию о проекте ОО рассматривают как часть представления реализации.

b) Исследование особого подмножества информации в каждом из представлений проекта, предусматривающем оценку.

c) Охват конкретных ФТБ каждым из представлений проекта, предоставленных для оценки.

d) Исследование каждого из представлений проекта, предоставленных для оценки, с рассмотрением различных ФТБ в рамках каждого представления проекта.

e) Исследование аспектов свидетельств, предоставленных для оценки, касающихся текущей информации о потенциальных уязвимостях, полученной оценщиком (например от системы оценки).

Данный подход к идентификации потенциальных уязвимостей предусматривает упорядоченный планируемый подход; применяется системный подход к исследованию. Оценщик должен описать используемый метод с точки зрения рассматриваемых свидетельств, исследуемой информации этих свидетельств, способа рассмотрения этой информации и выдвигаемых гипотез.

Ниже приводится несколько примеров гипотез, которые могут быть выдвинуты:

a) рассмотрение возможности ввода нарушителем некорректных исходных данных через интерфейсы на уровне внешних интерфейсов;

b) исследование ключевых механизмов безопасности, приведенных в «Описании архитектуры безопасности», таких как разделение процессов, при котором выдвигается гипотеза о возможном переполнении внутреннего буфера, что может привести к нарушению такого разделения;

c) поиск в целях идентификации любых объектов, созданных в представлении реализации ОО, которые не полностью контролируются ФБО, и могут быть использованы нарушителем для компрометации ФТБ.

Например, оценщик может идентифицировать, что интерфейсы являются потенциальной областью слабых мест ОО и определить подход к поиску таким образом, что «все спецификации интерфейсов, представленные в функциональной спецификации и проекте ОО, будут исследованы для выдвижения гипотезы о потенциальных уязвимостях», а затем продолжить объяснение методов, используемых при выдвижении таких гипотез.

Процесс идентификации является итерационным (повторяющимся), т.е. идентификация одной потенциальной уязвимости может привести к идентификации другой проблемной области, которая требует дальнейшего исследования.

Оценщик приводит в отчете (сообщении), какие действия были предприняты для идентификации потенциальных уязвимостей на основе общедоступной информации. Однако, осуществляя этот тип поиска, оценщик может быть не в состоянии заранее, до начала анализа, описать шаги, которые он предпримет при идентификации потенциальных уязвимостей, поскольку подход может развиваться и претерпевать изменения в зависимости от информации, выявленной в процессе поиска.

Оценщик приводит в отчете, какие свидетельства были исследованы в процессе поиска потенциальных уязвимостей. Выбор свидетельств может производиться на основании идентифицированных оценщиком проблемных областей, связанных со свидетельствами, которые нарушитель, как предполагается, может получить, или согласно другому обоснованию, предложенному оценщиком.

Исходя из ФТБ, которые должны выполняться для данного ОО в среде функционирования, оценщику при независимом анализе уязвимостей следует рассмотреть характерные потенциальные уязвимости под каждой из следующих рубрик:

a) потенциальные уязвимости, характерные для конкретного типа оцениваемого ОО, которые могут быть указаны органом оценки;

b) обход ФБО;

c) вмешательство;
d) прямое нападение;
e) мониторинг;
f) неправильное применение.

Пункты b) — f) объясняются более детально в приложении В.

«Описание архитектуры безопасности» следует рассматривать в свете каждой из вышеупомянутых рубрик типовых потенциальных уязвимостей. Каждую потенциальную уязвимость следует рассматривать при поиске возможных способов нарушения защиты ФБО и компрометации ФБО.

14.2.3.6.2 Шаг оценивания AVA_VAN.3-5

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

Может быть идентифицировано, 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 эффективно снизить вероятность использования потенциальной уязвимости для несанкционированного вмешательства в ОО.

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.

14.2.3.7 Действие AVA_VAN.3.4E

14.2.3.7.1 Шаг оценивания AVA_VAN.3-6

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

Оценщик готовит к тестированию проникновения то, что необходимо, чтобы сделать заключение о восприимчивости ОО, находящегося в своей среде функционирования, к потенциальным уязвимостям, идентифицированным в процессе поиска по источникам общедоступной информации. Любая текущая информация об известных потенциальных уязвимостях, предоставленная оценщику третьей стороной (например органом оценки), рассматривается оценщиком наряду с любыми обнаруженными в результате выполнения других действий по оценке потенциальными уязвимостями.

Оценщику следует помнить, что при рассмотрении «Описания архитектуры безопасности» для поиска уязвимостей (как детализировано в AVA_VAN.3-4), следует выполнить тестирование в целях подтверждения архитектурных свойств. Это, вероятно, потребует проведения негативных тестов, чтобы попытаться опровергнуть свойства архитектуры безопасности. При разработке стратегии тестирования проникновения оценщик обеспечивает, чтобы каждая из основных характеристик в «Описании архитектуры безопасности» была протестирована либо при функциональном тестировании (как рассмотрено в разделе 13), либо при тестировании проникновения, проведенном оценщиком.

Вероятно, будет целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной потенциальной уязвимости.

Не предполагается тестирования оценщиком на предмет наличия потенциальных уязвимостей (в том числе известных из общедоступных источников) помимо тех, для использования которых требуется Усиленный базовый потенциал нападения. Однако в некоторых случаях необходимо будет выполнить некоторый тест прежде, чем может быть определена пригодность к использованию. Когда в результате исследований в ходе оценки оценщик обнаруживает некоторую потенциальную уязвимость, для использования которой требуется потенциал нападения выше, чем Усиленный базовый, она приводится в ТОО как остаточная уязвимость.

Руководство по определению необходимого для использования потенциальной уязвимости потенциала нападения представлено в приложении В.4.

Если по поводу потенциальных уязвимостей выдвигают гипотезу, что эти уязвимости могут использовать только нарушители, обладающие Умеренным или Высоким потенциалом нападения, это

не приводит к отрицательному заключению по данному действию. В случае, если анализ поддерживает гипотезу, данные потенциальные уязвимости не следует рассматривать далее в качестве исходных данных для тестирования проникновения. Однако такие уязвимости приводятся в ТОО как остаточные.

Потенциальным уязвимостям, по поводу которых выдвигается гипотеза, что эти уязвимости могут использовать нарушители, обладающие Базовым или Усиленным базовым потенциалом нападения и использование которых приводит к нарушению целей безопасности, следует быть самыми высокими по приоритету потенциальными уязвимостями и их следует включать в перечень, который далее будет использоваться для тестирования проникновения.

14.2.3.7.2 Шаг оценивания AVA_VAN.3-7

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на перечне потенциальных уязвимостей, причем детализация этой документации должна быть достаточна для обеспечения воспроизводимости тестов. Тестовая документация должна включать:

a) идентификацию тестируемой потенциальной уязвимости оцениваемого ОО;

b) инструкции по подключению и настройке всего требуемого тестового оборудования, как требуется для проведения конкретного теста проникновения;

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

d) инструкции по инициированию ФБО;

e) инструкции по наблюдению режима выполнения ФБО;

f) описание всех ожидаемых результатов и необходимого анализа, который следует выполнить по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

g) инструкции по завершению теста и установке необходимого послетестового состояния ОО.

Оценщик готовится к тестированию проникновения, основываясь на перечне потенциальных уязвимостей, идентифицированных во время поиска общедоступной информации и анализа свидетельств.

Не предполагается, что оценщик сделает заключение о возможности использования потенциальных уязвимостей помимо тех, для которых требуется Усиленный базовый потенциал нападения, чтобы осуществить нападение. Однако в результате исследований в ходе оценки оценщик может обнаружить потенциальную уязвимость, пригодную для использования только нарушителем с большим, чем Усиленный базовый, потенциалом нападения. Такие уязвимости необходимо привести в ТОО как остаточные уязвимости.

Поняв потенциальную уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. Оценщик особенно внимательно рассматривает:

a) ИФБО или другой интерфейс ОО, который будет использован для инициирования выполнения ФБО и наблюдения за их реакцией (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). Следует отметить, что хотя интерфейсы ОО предоставляют средства тестирования свойств ФБО, сами эти интерфейсы не являются предметом тестирования);

b) начальные условия, которые будут необходимы для выполнения теста (т.е. какие-либо конкретные объекты или субъекты, которые необходимы и атрибуты безопасности, которые им необходимо будет иметь);

c) специальное оборудование для тестирования, которое потребуется либо для инициирования ИФБО, либо для наблюдения за ИФБО (хотя маловероятно, что для использования уязвимости, для которой предполагается Базовый потенциал нападения нарушителя, потребуется специальное оборудование);

d) следует ли заменить теоретическим анализом физическое тестирование, в частности в отношении того, когда результаты первоначального теста могут экстраполироваться для демонстрации того, что повторные попытки нападения, вероятно, будут успешными после выполнения некоторого заданного числа попыток.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной потенциальной уязвимости.

Цель определения данного уровня детализации в тестовой документации — предоставить возможность другому оценщику повторить тесты и получить эквивалентный результат.

14.2.3.7.3 Шаг оценивания AVA_VAN.3-8

Оценщик должен провести тестирование проникновения.

Оценщик использует документацию для тестов проникновения, подготовленную на шаге оценивания AVA_VAN.3-6, как основу для выполнения тестов проникновения по отношению к ОО, но это

не мешает оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может разработать специальные тесты в результате изучения информации в процессе тестирования проникновения, которые, если были выполнены оценщиком, должны быть внесены в документацию тестов проникновения. Такие тесты могут быть необходимы, чтобы исследовать непредвиденные результаты или наблюдения, а также потенциальные уязвимости, о существовании которых оценщик сделал предположение во время предварительно запланированного тестирования.

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

Не предполагается тестирования оценщиком потенциальных уязвимостей (в том числе известных из общедоступных источников), для использования которых требуется потенциал нападения выше, чем Усиленный базовый. Однако в некоторых случаях необходимо будет выполнить тест прежде, чем может быть определена пригодность к использованию. Если в результате исследований в ходе оценки оценщик обнаружит потенциальную уязвимость, пригодную для использования только нарушителем с большим, чем Усиленный базовый, потенциалом нападения, то она должна быть приведена в ТОО как остаточная уязвимость.

14.2.3.7.4 Шаг оценивания AVA_VAN.3-9

Оценщик должен зафиксировать фактические результаты тестов проникновения.

Хотя некоторые специфические детали фактических результатов выполнения тестов могут отличаться от ожидаемых (например поля времени и даты в записи аудита), общим результатам следует быть идентичными. Следует исследовать любые непредвиденные результаты выполнения тестов. Влияние на оценку следует установить и логически обосновать.

14.2.3.7.5 Шаг оценивания AVA_VAN.3-10

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

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Цель предоставления данной информации состоит в том, чтобы привести содержательный краткий обзор усилий оценщика по тестированию проникновения. Это не означает, что информация в ТОО относительно тестирования проникновения является точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов проникновения. Целью является предоставление достаточных подробностей, чтобы позволить другим оценщикам и сотрудникам органов оценки получить некоторое понимание выбранного подхода к тестированию проникновения, объема выполненного тестирования проникновения, тестируемых конфигураций ОО и общих результатов действий по тестированию проникновения.

Информация об усилиях оценщика по тестированию проникновения, которая обычно представлена в соответствующем разделе ТОО, включает:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые подвергались тестированию проникновения;

b) ИФБО, которые подвергались тестированию проникновения. Краткий перечень ИФБО и других интерфейсов ОО, на которых было сосредоточено тестирование проникновения;

c) вердикт по данному подвиду деятельности. Общий вывод по результатам тестирования проникновения.

Приведенный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы предоставить некоторое представление о типе информации, касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует привести в ТОО.

14.2.3.7.6 Шаг оценивания 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 нарушителю, обладающему 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 оценщиком делается отрицательное заключение.

Руководство из приложения В.4 следует использовать для того, чтобы сделать заключение о потенциале нападения, требуемом для использования конкретной уязвимости, и может ли эта уязвимость быть использована в предполагаемой среде функционирования. Может не быть необходимости вычис-

лять потенциал нападения для каждого случая, а только если есть некоторое сомнение относительно того, может ли уязвимость использоваться нарушителем, обладающим потенциалом нападения меньшим, чем Умеренный.

14.2.3.7.7 Шаг оценивания AVA_VAN.3-12

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

a) ее источник (например стала известна при выполнении действий ОМО, известна оценщику, прочитана в публикации);

b) связанные с ней невыполненные ФТБ;

c) описание;

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

e) количество времени, уровень компетенции, уровень знаний об ОО, уровень возможности доступа и оборудование, требуемые для использования идентифицированных уязвимостей, а также соответствующие значения с использованием таблиц В.2 и В.3 приложения В.4.

14.2.4 Подвид деятельности по оценке (AVA_VAN.4)

14.2.4.1 Цели

Цель данного подвида деятельности — сделать заключение, имеет ли ОО, находящийся в своей среде функционирования, уязвимости, пригодные для использования нарушителями, обладающими Умеренным потенциалом нападения.

14.2.4.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект ОО;

d) описание архитектуры безопасности;

e) выбранное подмножество реализации;

f) документация руководств;

g) ОО, пригодный для тестирования;

h) общедоступная информация для поддержки идентификации потенциальных уязвимостей.

Другие неявные свидетельства оценки для этого подвида деятельности зависят от компонентов, которые были включены в пакет доверия. Свидетельства, предоставляемые для каждого компонента, должны использоваться в качестве исходных данных для этого подвида деятельности.

Другие исходные данные для данного подвида деятельности:

a) текущая информация, касающаяся известных из общедоступных источников потенциальных уязвимостей и атак (например от органа оценки).

14.2.4.3 Замечания по применению

Методический подход к анализу принимает форму структурированного исследования свидетельств. Для данного метода требуется, чтобы оценщик определил структуру и форму анализа (то есть способ, которым будет проведён анализ, является предопределенным, в отличие от фокусированного метода идентификации уязвимостей). Данный метод определяется в терминах того, какая информация будет подвергнута рассмотрению, каким образом и с какой целью. Дальнейшее руководство по проведению методического анализа уязвимостей представлено в приложении В.2.2.2.3.

14.2.4.4 Действие AVA_VAN.4.1E

ИСО/МЭК 15408-3 AVA_VAN.4.1C: *ОО должен быть пригоден для тестирования.*

14.2.4.4.1 Шаг оценивания AVA_VAN.4-1

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, предоставленному разработчиком и идентифицированному в плане для тестирования, следует иметь ту же уникальную маркировку, которая установлена в соответствии с подвидами деятельности семейства ALC_CMC «Возможности УК» и идентифицирована во введении ЗБ.

В ЗБ может быть определено более одной подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию в соответствии с ЗБ. Оценщик верифицирует, что все конфигурации ОО согласованы с ЗБ.

Оценщику следует рассмотреть описанные в ЗБ цели безопасности для среды функционирования ОО, которые могут быть применимы к среде тестирования, и удостовериться, что они достигаются

в среде тестирования. В ЗБ могут быть и другие цели безопасности, которые не применимы для среды тестирования. Например, цель безопасности относительно допусков пользователей не применима к среде тестирования, однако цель безопасности относительно единой точки подключения к сети применима к среде тестирования.

При использовании каких бы то ни было средств тестирования (например измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика.

14.2.4.4.2 Шаг оценивания AVA_VAN.4-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами. Например, предшествующее успешное завершение подвида деятельности AGD_PRE.1 позволит считать удовлетворенным данный шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был правильно установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить и запустить ОО, используя только поставляемое руководство.

Если оценщику приходится выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данный шаг оценивания мог бы удовлетворить шаг оценивания AGD_PRE.1-3.

14.2.4.5 Действие AVA_VAN.4.2E

14.2.4.5.1 Шаг оценивания AVA_VAN.4-3

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

Оценщик исследует общедоступные источники информации в целях поддержки идентификации возможных потенциальных уязвимостей в ОО. Существует много общедоступных источников информации, которые следует рассмотреть оценщику. Например, общедоступные ресурсы в мировой сети, включая:

a) специальные публикации (журналы, книги);

b) исследовательские статьи;

c) материалы конференций.

Оценщику не следует ограничивать рассмотрение общедоступной информации вышеупомянутыми источниками; ему следует рассмотреть любую другую доступную информацию, имеющую отношение к уязвимостям ОО.

В процессе исследования предоставленных разработчиком свидетельств оценщик будет использовать общедоступную информацию для дальнейшего поиска потенциальных уязвимостей. Оценщику также следует особо рассмотреть всю доступную информацию, касающуюся идентифицированных проблемных областей.

Возможность легкого 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 средств нападения позволяет с высокой степенью вероятности предположить, что данная информация будет использоваться при попытках идентифицировать потенциальные уязвимости в ОО и использовать их. Современные средства поиска 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 сделано в терминах «эффективность-стоимость».

Поиск общедоступной информации следует сосредоточить на тех источниках, которые относятся к конкретным технологиям, использованным в разработке продукта ИТ, на основании которого получен ОО. При определении требуемой широты этого поиска следует рассмотреть следующие факторы: тип ОО, опыт оценщика для данного типа ОО, ожидаемый потенциал нападения и уровень доступных свидетельств согласно классу ADV.

Процесс идентификации является итерационным (повторяющимся), т. е. идентификация одной потенциальной уязвимости может привести к идентификации другой проблемной области, которая требует дальнейшего исследования.

Оценщик описывает подход, применяемый для идентификации потенциальных уязвимостей на основании изучения общедоступных источников, детально описывая выполняемый поиск. На этот процесс могут влиять такие факторы, как идентифицированные оценщиком проблемные области, связанные со свидетельствами, которые предположительно могут быть доступны нарушителю. Однако

следует признать, что для этого типа поиска подход может развиться далее в результате полученной во время поиска информации. Поэтому оценщик также приводит в отчете информацию о любых действиях, предпринятых в дополнение к описанным в подходе для дальнейшего исследования проблем, приводящих к потенциальным уязвимостям, и о том, какие свидетельства были исследованы в процессе поиска потенциальных уязвимостей.

14.2.4.6 Действие AVA_VAN.4.3E

14.2.4.6.1 Шаг оценивания AVA_VAN.4-4

Оценщик должен провести методический анализ ЗБ, документации руководств, функциональной спецификации, проекта ОО и описания архитектуры безопасности, чтобы идентифицировать возможные потенциальные уязвимости в ОО.

Руководство по проведению методического анализа представлено в приложении В.2.2.2.3.

Данный подход к идентификации потенциальных уязвимостей предусматривает упорядоченный планируемый подход. Применяется системный подход к исследованию. Оценщик должен описать используемый метод с точки зрения рассматриваемых свидетельств, исследуемой информации этих свидетельств, способа рассмотрения этой информации и выдвигаемых гипотез.

Должна быть использована методология гипотез о недостатках, посредством которой анализируются ЗБ, свидетельства разработки (функциональная спецификация, проект ОО, представление реализации), а также руководства, а после этого делаются предположения о потенциальных уязвимостях в ОО.

Оценщик использует знания проекта ОО и функционирования ОО, полученные от изучения поставляемых материалов ОО, чтобы выдвинуть гипотезу о недостатках и идентифицировать потенциальные недостатки разработки ОО и потенциальные ошибки в специфицированном методе функционирования ОО.

«Описание архитектуры безопасности» предоставляет сведения об анализе уязвимостей, проведенном разработчиком, поскольку в ней документировано, каким образом в ФБО обеспечена собственная защита от вмешательства недоверенных субъектов и предотвращение обхода функциональных возможностей обеспечения безопасности. Таким образом, оценщик базируется на своем понимании защиты ФБО, полученном в результате анализа этих свидетельств и расширенном за счет знаний, полученных из других свидетельств по классу ADV, связанных с разработкой.

Принятый подход при методическом анализе уязвимостей направлен на проблемные области, идентифицированные во время исследования свидетельств разработки и руководств в рамках проведения действий по оценке. Однако оценщику следует также рассмотреть каждый аспект анализа архитектуры безопасности для поиска любых способов, которыми можно нарушить защиту ФБО. Может оказаться полезным структурировать методический анализ на основе материала, представленного в «Описании архитектуры безопасности», учитывая, если это применимо, аспекты из других свидетельств по классу ADV. Анализ может быть в дальнейшем развит в целях предоставления уверенности в том, что рассмотрены все материалы других свидетельств класса ADV.

Ниже приводится несколько примеров гипотез, которые могут быть выдвинуты:

a) рассмотрение возможности ввода нарушителем некорректных исходных данных через интерфейсы на уровне внешних интерфейсов;

b) исследование ключевых механизмов безопасности, приведенных в «Описании архитектуры безопасности», таких как разделение процессов, при котором выдвигается гипотеза о возможном переполнении внутреннего буфера, что может привести к нарушению такого разделения;

c) поиск в целях идентификации любых объектов, созданных в представлении реализации ОО, которые не полностью контролируются ФБО и могут быть использованы нарушителем для компрометации ФТБ.

Например, оценщик может идентифицировать, что интерфейсы являются потенциальной областью слабых мест ОО и определить подход к поиску уязвимостей таким образом, что: «все спецификации интерфейсов, представленные в функциональной спецификации и проекте ОО, будут исследованы для выдвижения гипотезы о потенциальных уязвимостях», а затем продолжить объяснение методов, используемых при выдвижении таких гипотез.

Дополнительно рассматриваются проблемные области, идентифицированные оценщиком во время исследования свидетельств в процессе проведения действий по оценке. Проблемные области также могут быть идентифицированы во время выполнения других шагов оценивания, связанных с данным компонентом, в особенности шагов AVA_VAN.4-7, AVA_VAN.4-5 и AVA_VAN.4-6, при выполнении которых разработка и проведение тестов проникновения могут позволить идентифицировать проблемные области, для которых требуется дальнейшее исследование, или потенциальные уязвимости.

Однако на данном уровне строгости анализ только подмножества свидетельств разработки и руководств и их содержания недопустим. Описанием подхода следует обеспечить демонстрацию того, что используемый методический подход достаточно полон и предоставляет уверенность в том, что при использовании подхода к поиску в поставляемых материалах ОО рассматривалась вся информация, представленная в этих материалах.

Данный подход к идентификации потенциальных уязвимостей предусматривает упорядоченный планируемый подход. Применяется системный подход к исследованию. Оценщик должен описать используемый метод с точки зрения рассматриваемых свидетельств, исследуемой информации этих свидетельств, способа рассмотрения этой информации и выдвигаемых гипотез. Данный подход следует согласовать с органом оценки, а орган оценки может предоставить детализацию любых дополнительных подходов, которые следует предпринять оценщику при проведении анализа уязвимостей и при идентификации любой дополнительной информации, которую следует рассмотреть оценщику.

Хотя системный подход для идентификации потенциальных уязвимостей для данного подхода предопределен, процесс идентификации все еще может быть итерационным (повторяющимся), т.е. идентификация одной потенциальной уязвимости может привести к идентификации другой проблемной области, которая требует дальнейшего исследования.

Исходя из ФТБ, которые должны выполняться для данного ОО в среде функционирования, оценщику при независимом анализе уязвимостей следует рассмотреть характерные потенциальные уязвимости под каждой из следующих рубрик:

a) потенциальные уязвимости, характерные для конкретного типа оцениваемого ОО, которые могут быть указаны органом оценки;

b) обход ФБО;

c) вмешательство;

d) прямое нападение;

e) мониторинг;

f) неправильное применение.

Пункты b) — f) объясняются более детально в приложении В.

«Описание архитектуры безопасности» следует рассматривать в свете каждой из вышеупомянутых рубрик типовых потенциальных уязвимостей. Каждую потенциальную уязвимость следует рассматривать при поиске возможных способов нарушения защиты ФБО и компрометации ФБО.

14.2.4.6.2 Шаг оценивания AVA_VAN.4-5

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

Может быть идентифицировано, 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 эффективно снизить вероятность использования потенциальной уязвимости для несанкционированного вмешательства в ОО.

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.

14.2.4.7 Действие AVA_VAN.4.4E

14.2.4.7.1 Шаг оценивания AVA_VAN.4-6

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

Оценщик готовит к тестированию проникновения то, что необходимо, чтобы сделать заключение о восприимчивости ОО, находящегося в своей среде функционирования, к потенциальным уязвимостям, идентифицированным в процессе поиска по источникам общедоступной информации. Любая текущая информация об известных потенциальных уязвимостях, предоставленная оценщику третьей стороной (например органом оценки), рассматривается оценщиком наряду с любыми обнаруженными в результате выполнения других действий по оценке потенциальными уязвимостями.

Оценщику следует помнить, что при рассмотрении «Описания архитектуры безопасности» для поиска уязвимостей (как детализировано в AVA_VAN.4-3), следует выполнить тестирование в целях подтверждения архитектурных свойств. Если требования ATE_DPT включены в ТДБ, то в свидетельства тестирования разработчика будет включено тестирование, проводимое для подтверждения правильности реализации любых конкретных механизмов, детально описанных в «Описании архитектуры безопасности». Однако проводимое разработчиком тестирование не обязательно должно включать тестирование всех аспектов свойств архитектуры, обеспечивающих защиту ФБО, так как большая часть таких тестов будет являться негативными тестами, которые проводятся, чтобы попытаться опровергнуть эффективность этих свойств. При разработке стратегии тестирования проникновения оценщик обеспечивает, что каждая из основных характеристик в «Описании архитектуры безопасности» протестирована либо при функциональном тестировании (как рассмотрено в главе 13), либо при тестировании проникновения, проведенном оценщиком.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной потенциальной уязвимости.

Не предполагается тестирования оценщиком на предмет наличия потенциальных уязвимостей (в том числе известных из общедоступных источников) помимо тех, для использования которых требуется Умеренный потенциал нападения. Однако в некоторых случаях необходимо будет выполнить некоторый тест прежде, чем может быть определена пригодность к использованию. Когда в результате исследований оценщик обнаруживает некоторую потенциальную уязвимость, для использования которой требуется потенциал нападения выше, чем Умеренный, она приводится в ТОО как остаточная уязвимость.

Руководство по определению необходимого для использования потенциальной уязвимости потенциала нападения представлено в приложении В.4.

Потенциальным уязвимостям, по поводу которых выдвигается гипотеза, что эти уязвимости могут использовать нарушители, обладающие Умеренным (или ниже) потенциалом нападения и использование которых приводит к нарушению целей безопасности, следует быть самыми высокими по приоритету потенциальными уязвимостями, и их следует включать в перечень, который далее будет использоваться для тестирования проникновения.

14.2.4.7.2 Шаг оценивания AVA_VAN.4-7

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на перечне потенциальных уязвимостей, причем детализация этой документации должна быть достаточна для обеспечения воспроизводимости тестов. Тестовая документация должна включать:

a) идентификацию тестируемой потенциальной уязвимости оцениваемого ОО;

b) инструкции по подключению и настройке всего требуемого тестового оборудования, как требуется для проведения конкретного теста проникновения;

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

d) инструкции по инициированию ФБО;

e) инструкции по наблюдению режима выполнения ФБО;

f) описание всех ожидаемых результатов и необходимого анализа, который следует выполнить по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

g) инструкции по завершению теста и установке необходимого послетестового состояния ОО.

Оценщик готовится к тестированию проникновения, основываясь на перечне потенциальных уязвимостей, идентифицированных во время поиска общедоступной информации и анализа свидетельств.

Не предполагается, что оценщик сделает заключение о возможности использования потенциальных уязвимостей помимо тех, для которых требуется Умеренный потенциал нападения, чтобы осуществить нападение. Однако в результате исследований в ходе оценки оценщик может обнаружить потенциальную уязвимость, пригодную для использования только нарушителем с большим, чем Умеренный, потенциалом нападения. Такие уязвимости нужно приводить в ТОО как остаточные уязвимости.

Поняв потенциальную уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. Оценщик особенно внимательно рассматривает:

a) ИФБО или другой интерфейс ОО, который будет использоваться для инициирования выполнения ФБО и наблюдения за реакцией ФБО (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. Следует отметить, что хотя интерфейсы ОО предоставляют средства тестирования свойств ФБО, сами эти интерфейсы не являются предметом тестирования);

b) начальные условия, которые будут необходимы для выполнения теста (т. е. какие-либо конкретные объекты или субъекты, которые необходимы и атрибуты безопасности, которые им необходимо будет иметь);

c) специальное оборудование для тестирования, которое потребуется либо для инициирования ИФБО, либо для наблюдения за ИФБО (хотя маловероятно, что для использования уязвимости, для которой предполагается Базовый потенциал нападения нарушителя, потребуется специальное оборудование);

d) следует ли заменить теоретическим анализом физическое тестирование, в частности в отношении того, когда результаты первоначального теста могут экстраполироваться для демонстрации того, что повторные попытки нападения, вероятно, будут успешными после выполнения некоторого заданного числа попыток.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной потенциальной уязвимости.

Цель определения данного уровня детализации в тестовой документации — предоставить возможность другому оценщику повторить тесты и получить эквивалентный результат.

14.2.4.7.3 Шаг оценивания AVA_VAN.4-8

Оценщик должен провести тестирование проникновения.

Оценщик использует документацию для тестов проникновения, подготовленную на шаге оценивания AVA_VAN.4-6, как основу для выполнения тестов проникновения по отношению к ОО, но это не мешает оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может разработать специальные тесты в результате изучения информации в процессе тестирования проникновения, которые, если были выполнены оценщиком, должны быть внесены в документацию тестов проникновения. Такие тесты могут быть необходимы, чтобы исследовать непредвиденные результаты или наблюдения, а также потенциальные уязвимости, о существовании которых оценщик сделал предположение во время предварительно запланированного тестирования.

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

Не предполагается тестирования оценщиком потенциальных уязвимостей (в том числе известных из общедоступных источников), для использования которых требуется потенциал нападения выше, чем Умеренный. Однако в некоторых случаях необходимо будет выполнить тест прежде, чем может быть определена пригодность к использованию. Если в результате исследований в ходе оценки оценщик обнаружит потенциальную уязвимость, пригодную для использования только нарушителем с большим, чем Умеренный, потенциалом нападения, то она должна быть приведена в ТОО как остаточная уязвимость.

14.2.4.7.4 Шаг оценивания AVA_VAN.4-9

Оценщик должен зафиксировать фактические результаты тестов проникновения.

Хотя некоторые специфические детали фактических результатов выполнения тестов могут отличаться от ожидаемых (например поля времени и даты в записи аудита), общим результатам следует быть идентичными. Следует исследовать любые непредвиденные результаты выполнения тестов. Влияние на оценку следует установить и логически обосновать.

14.2.4.7.5 Шаг оценивания AVA_VAN.4-10

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

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Цель предоставления данной информации состоит в том, чтобы привести содержательный краткий обзор усилий оценщика по тестированию проникновения. Это не означает, что информация в ТОО относительно тестирования проникновения является точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов проникновения. Целью является предоставление достаточных подробностей, чтобы позволить другим оценщикам и сотрудникам органов оценки получить некоторое понимание выбранного подхода к тестированию проникновения, объема выполненного тестирования проникновения, тестируемых конфигураций ОО и общих результатов действий по тестированию проникновения.

Информация об усилиях оценщика по тестированию проникновения, которая обычно представлена в соответствующем разделе ТОО, включает:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые подвергались тестированию проникновения;

b) ИФБО, которые подвергались тестированию проникновения. Краткий перечень ИФБО и других интерфейсов ОО, на которых было сосредоточено тестирование проникновения;

c) вердикт по данному подвиду деятельности. Общий вывод по результатам тестирования проникновения.

Приведенный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы предоставить некоторое представление о типе информации, касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует привести в ТОО.

14.2.4.7.6 Шаг оценивания 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 нарушителю, обладающему 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 оценщиком делается отрицательное заключение.

Руководство из приложения В.4 следует использовать для того, чтобы сделать заключение о потенциале нападения, требуемом для использования конкретной уязвимости, и может ли эта уязвимость быть использована в предполагаемой среде функционирования, Может не быть необходимости вычислять потенциал нападения для каждого случая, а только если есть некоторое сомнение относительно того, может ли уязвимость использоваться нарушителем, обладающим потенциалом нападения меньшим, чем Высокий.

14.2.4.7.7 Шаг оценивания AVA_VAN.4-12

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

a) ее источник (например стала известна при выполнении действий ОМО, известна оценщику, прочитана в публикации);

b) связанные с ней невыполненные ФТБ;

c) описание;

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

e) количество времени, уровень компетенции, уровень знаний об ОО, уровень возможности доступа и оборудование, требуемые для использования идентифицированных уязвимостей, а также соответствующие значения с использованием таблиц В.2 и В.3 приложения В.4.

14.2.5 Подвид деятельности по оценке (AVA_VAN.5)

Общее руководство отсутствует; за консультациями по выполнению данного подвида деятельности следует обращаться в конкретную систему оценки.

15 Класс ACO: Композиция

15.1 Введение

Вид деятельности «Композиция» предназначен для того, чтобы сделать заключение, могут ли компоненты ОО быть объединены безопасным образом, как определено в ЗБ составного ОО. Это достигается посредством исследования и тестирования взаимодействий между компонентами, поддержанными исследованием проекта компонентов и проведением анализа уязвимостей.

15.2 Замечания по применению

Семейство «Зависимости зависимых компонентов» (ACO_REL) идентифицирует случай, когда зависимый компонент полагается на продукт ИТ в среде функционирования (удовлетворенной базовым компонентом при оценке составного ОО) для предоставления своих сервисов безопасности. Эта зависимость идентифицируется в терминах интерфейсов, которые зависимый компонент ожидает получить от базового. Затем в классе «Свидетельство разработки» (ACO_DEV) определяется, какие интерфейсы базового компонента рассматривались (как ИФБО) во время оценки базового компонента.

Следует отметить, что семейство «Зависимости зависимых компонентов» не охватывает другие свидетельства, которые могут быть необходимы для рассмотрения технических проблем интеграции компонентов (например описания не относящихся к ФБО интерфейсов операционной системы, правил интеграции и т.д.). Эти вопросы находятся вне проблемной области оценки безопасности композиции и рассматриваются как проблема функциональной композиции.

В части «Тестирование составного ОО» (ACO_CTT) оценщик выполняет тестирование ФТБ составного ОО для интерфейсов составного ОО и интерфейсов базового компонента, на функционирование которого полагается зависимый компонент, чтобы подтвердить, что эти интерфейсы работают определенным образом. В выборке рассматриваются возможные эффекты от изменения конфигурации/использования базового компонента таким же образом, как в составном ОО. Эти изменения идентифицируются на основе конфигурации базового компонента, определенного во время оценки базового компонента. Разработчик предоставит тестовые свидетельства для каждого интерфейса базовых компонентов (требования охвата согласуются с теми, которые применяются для оценки базового компонента).

Семейством «Обоснование композиции» (ACO_COR) требуется, чтобы оценщик сделал заключение о том, были ли соответствующие меры доверия применены к базовому компоненту и используется ли базовый компонент в его оцененной конфигурации. Это включает определение того, включены ли все функции безопасности, требуемые зависимыми компонентами, в ФБО базового компонента. Требование семейства «Обоснование композиции» (ACO_COR) может быть удовлетворено посредством производства свидетельств, где для каждой функции демонстрируется, что функция поддерживается. Такие свидетельства могут быть представлены в виде целей безопасности или открытого отчета об оценке компонента (например отчет о сертификации).

Если, с другой стороны, что-то из вышеупомянутого не поддерживается, то существует вероятность возникновения разногласий по поводу того, почему на доверие, полученное во время проведения исходной оценки, не было оказано влияние впоследствии. Если это не представляется возможным, тогда может потребоваться предоставление дополнительных свидетельств оценки для неохваченных аспектов базового компонента. В этом случае такие материалы оцениваются в рамках семейства «Свидетельство разработки» (ACO_DEV).

Например, может иметь место случай, описанный в подразделе «Взаимодействия между объединенными сущностями ИТ» (см. приложение В.3 «Взаимодействия между объединенными сущностями ИТ» в ИСО/МЭК 15408-3), когда зависимому компоненту требуется, чтобы базовый компонент обеспечил больше функций безопасности в составном ОО, чем включено в оценку базового компонента. Это возможно определить во время применения семейств «Зависимости зависимых компонентов» (ACO_REL) и «Свидетельство разработки» (ACO_DEV). В этом случае свидетельства обоснования композиции, предоставленные для семейства «Обоснование композиции» (ACO_COR), продемонстрируют, что доверие, приобретенное при оценке базового компонента, не было затронуто тем или иным образом. Это может быть достигнуто различными средствами, включая:

a) выполнение повторной оценки базового компонента, направленной на исследование свидетельств, касающихся расширенной части ФБО;

b) демонстрацию того, что расширенная часть ФБО не затрагивает другие части ФБО, и представление свидетельств того, что расширенная часть ФБО обеспечивает выполнение необходимых функций безопасности.

15.3 Обоснование композиции (ACO_COR)

15.3.1 Подвид деятельности по оценке (ACO_COR.1)

15.3.1.1 Исходные данные

Свидетельства оценки этого подвида деятельности:

a) составное ЗБ;

b) обоснование композиции;

c) информация о зависимостях;

d) информация о разработке;

e) уникальный идентификатор.

15.3.1.2 Действие ACO_COR.1.1E

ИСО/МЭК 15408-3 ACO_COR.1.1C: *Обоснование композиции должно продемонстрировать, что уровень доверия, приобретенный для поддержки функциональных возможностей базового компонента, является таким же высоким или выше, чем уровень доверия к зависимому компоненту, при условии, что конфигурация базового компонента соответствует требованиям для поддержки ФБО зависимого компонента.*

15.3.1.2.1 Шаг оценивания ACO_COR.1-1

Оценщик должен исследовать анализ соответствия информации о разработке и информации о зависимостях для идентификации интерфейсов, на которые полагается зависимый компонент и которые не детализированы в информации о разработке.

Для данного шага оценивания у оценщика две цели:

a) сделать заключение о том, к каким интерфейсам, на которые полагается зависимый компонент, были применены соответствующие меры доверия;

b) сделать заключение о том, что пакет доверия, применявшийся к базовому компоненту во время его оценивания, содержал те же требования доверия, что в пакете доверия, применяемом к зависимому компоненту во время его оценки, или иерархически более высокие требования доверия.

Оценщик может использовать прослеживание соответствия в информации о разработке, разработанной в процессе выполнения действий семейства ACO_DEV «Свидетельство разработки» (например: ACO_DEV.1-2, ACO_DEV.2-4, ACO_DEV.3-6, чтобы помочь выявить интерфейсы, идентифицированные в информации о зависимостях, но не рассмотренные в информации о разработке.

Оценщик приводит в отчете описанные в информации о зависимостях осуществляющие выполнение ФТБ интерфейсы, которые не включены в информацию о разработке. Это предоставит исходные данные для шага оценивания ACO_COR.1-3, помогая идентифицировать части базового компонента, для которых требуется приобретение большего уровня доверия.

Если и базовый и зависимые компоненты оценивались относительно одного и того же пакета доверия, то вынесение заключения о том, является ли уровень доверия в частях оценки базового компонента по крайней мере таким же, как уровень доверия зависимого компонента, не представляет особого труда. Однако, если к компонентам во время их оценки применялись различные пакеты доверия, оценщику необходимо сделать заключение о том, что все требования доверия, относящиеся к базовому компоненту, иерархически выше требований доверия, относящихся к зависимому компоненту.

15.3.1.2.2 Шаг оценивания ACO_COR.1-2

Оценщик должен исследовать обоснование композиции, чтобы сделать заключение о том, были ли рассмотрены во время оценки базового компонента включенные в базовый компонент интерфейсы, на которые полагается зависимый компонент.

Информация об области охвата и границах базового компонента содержится в ЗБ, открытом отчете об оценке компонентов (например отчете о сертификации) и руководствах для базового компонента. В ЗБ предоставляется детальное описание области логического охвата и границ составного ОО, что позволяет оценщику сделать заключение о том, относится ли интерфейс к той части продукта, которая находилась в области проведения оценки. В документации руководств предоставлено детальное описание использования всех интерфейсов составного ОО. Хотя документация руководств может включать детальное описание интерфейсов продукта, который не включен в область оценивания, любым таким интерфейсам следует быть идентифицируемыми или из информации по области в ЗБ или через некоторую часть руководств, которая относится к оцененной конфигурации. В открытом отчете об оценке могут быть предоставлены дополнительные необходимые ограничения на использование составного ОО.

Таким образом, совокупность этих исходных данных позволяет оценщику сделать заключение о том, имеется ли у интерфейса, описанного в обосновании композиции, необходимый связанный с ним уровень доверия или требуется больший уровень доверия. Оценщик приводит в отчете интерфейсы базового компонента, для которых требуется приобретение дополнительного доверия в целях их дальнейшего рассмотрения во время шага оценивания ACO_COR.1-3.

15.3.1.2.3 Шаг оценивания ACO_COR.1-3

Оценщик должен исследовать обоснование композиции, чтобы сделать заключение о том, что необходимые меры доверия были применены к базовому компоненту.

Вердикты по оценке и результирующее доверие к базовому компоненту могут быть использованы повторно, если эти же части уже оцененного базового компонента используются в составном ОО совместимым образом.

Чтобы сделать заключение о том, были ли необходимые меры доверия применены к компоненту и к частям компонента, к которым еще должны быть применены меры доверия, оценщику следует использовать данные, полученные в результате проведения действия ACO_DEV.*.2E и шагов оценивания ACO_COR.1-1 и ACO_COR.1-2:

a) Для интерфейсов, идентифицированных в информации о зависимостях (семейство ACO_REL «Зависимости зависимых компонентов»), но не рассматривающихся в информации о разработке (семейство ACO_DEV «Свидетельство разработки»), требуется дополнительная информация (идентифицированная в ACO_COR.1-1.).

b) Для интерфейсов базового компонента, используемых несовместимым образом в составном ОО (когда имеется различие между информацией, предоставленной в семействах ACO_DEV «Свидетельство разработки» и ACO_REL «Зависимости зависимых компонентов», необходимо рассмотреть воздействие этих различий на использование ОО (как идентифицировано в ACO_DEV.*.2E.)).

c) Для интерфейсов, идентифицированных в обосновании композиции, для которых ранее не было приобретено доверие, требуется дополнительная информация (идентифицированная в ACO_COR.1-1.)

d) Для интерфейсов, согласованно описанных в информации о зависимостях, обосновании композиции и информации о разработке, не требуется проведение каких-либо дальнейших действий оценщика, поскольку можно повторно использовать результаты оценки базового компонента.

Интерфейсы базового компонента, о которых оценщиком приводится в отчете, что они требуются в информации о зависимостях, но не включаются в информацию о разработке, указывают на части базового компонента, где требуется приобретение большего доверия. Интерфейсы идентифицируют точки входа в базовый компонент.

Для интерфейсов, включенных в информацию и о разработке и о доверии, оценщик должен сделать заключение о том, используются ли интерфейсы составного ОО в манере, которая совместима с оценкой базового компонента. Метод использования интерфейса рассматривается в действиях семейства «Свидетельство разработки» (ACO_DEV), чтобы сделать заключение, используется ли интерфейс совместимым образом и в базовом компоненте и в составном ОО. Остается только вынести заключение, согласованы ли конфигурации базового компонента и составного ОО. Чтобы сделать об этом заключение, оценщик рассматривает документацию руководств для них, чтобы удостовериться, что они согласованы (см. ниже дальнейшее руководство по оценке согласованности документации руководств). Любое отклонение в документации будет далее проанализировано при оценке, чтобы сделать заключение о возможном влиянии подобной несогласованности.

Для тех интерфейсов, которые согласованно описаны в информации о зависимостях и информации о разработке, и для которых руководства базового компонента и составного ОО являются согласованными, обеспечен необходимый уровень доверия.

Следующие подразделы дают представление о том, как сделать заключение о согласованности между доверием, приобретенным для базового компонента, свидетельствами, предусмотренными для составного ОО, и анализом, проведенным оценщиком в тех случаях, когда выявлены несоответствия.

15.3.1.2.3.1 Разработка

В информации о зависимостях идентифицируются интерфейсы зависимого компонента, которые должны соответствовать интерфейсам базового компонента. Если интерфейс, идентифицированный в информации о зависимостях, не идентифицирован в информации о разработке, то в обосновании композиции должно быть обеспечено обоснование того, каким образом базовый компонент обеспечивает зависимый необходимыми интерфейсами.

Если интерфейс, идентифицированный в информации о зависимостях, идентифицирован в информации о разработке, но между описаниями есть несоответствия, требуется дальнейший анализ. Оценщик идентифицирует различия в использовании базового компонента в соответствии с тем, как он рассматривается при оценке базового компонента и при оценке составного ОО. Оценщик разрабатывает тестирование, которое будет проведено (во время проведения оценки по семейству ACO_CTT «Тестирование составного ОО») для проверки интерфейса.

Следует, чтобы состояние исправлений (патчей) базовых и зависимых компонентов, использующихся в составном ОО, было сравнимо с состоянием исправлений компонентов во время проведения их оценивания. Если какие-либо исправления были применены к компонентам, обоснование композиции должно включать детальное описание таких исправлений, включая любое потенциальное влияние на ФТБ оцениваемого компонента. Оценщику следует рассмотреть предоставленную ему информацию по поводу исправлений и проверить точность определения потенциального влияния исправления на составные ФТБ. Затем оценщику следует оценить, должны ли изменения, внесенные данным исправлением, быть проверены посредством тестирования, и идентифицирует необходимый подход к тестированию. Тестирование может принять форму повторения применимого тестирования оценщика/разработчика, выполненного для оценки компонента, или же от оценщика может потребоваться разработать новые тесты для подтверждения правильности исправленной версии компонента.

Если над каким-либо из отдельных компонентов проводились действия по обеспечению непрерывности доверия с момента завершения оценки компонента, оценщик может считать изменения уже оцененными в рамках данных действий во время осуществления деятельности по независимому анализу уязвимостей составного ОО (в рамках семейства ACO_VUL «Анализ уязвимостей композиции»).

15.3.1.2.3.2 Руководство

Руководство для составного ОО, вероятно, будет в значительной степени ссылаться на руководства для отдельных компонентов. Минимальное требуемое руководство — идентификация любых иерархических зависимостей при применении руководств для зависимых и базовых компонентов, особенно во время подготовки (установки) составного ОО.

В дополнение к применению к руководству составного ОО требований семейств «Подготовительные процедуры» (AGD_PRE) и «Руководство пользователя по эксплуатации» (AGD_OPE) необходимо проанализировать согласованность между руководством для компонентов и составным ОО, выявить любые несоответствия.

Если руководство составного ОО ссылается на руководство базового и зависимого компонента, тогда рассмотрение согласованности ограничивается вопросом согласованности документации руководств, предусмотренной для каждого из компонентов (то есть согласованность между руководствами базового и зависимого компонентов). Однако, если для составного ОО имеется дополнительное руководство помимо того, которое предоставляется для его компонентов, требуется провести больший объем анализа согласованности, так как дополнительно требуется оценить согласованность между документацией руководств для компонентов и документацией руководств для составного ОО.

Под согласованностью в данном случае понимают, что руководства являются идентичными или их совокупность налагает дополнительные ограничения на функционирование отдельных компонентов, как при *усилении функциональных* компонентов/компонентов доверия.

Оценщик может на основании доступной ему информации (которая используется как исходные данные для семейства «Свидетельство разработки» (ACO_DEV) или для аспектов разработки, рассмотренных выше) сделать заключение о том, что все возможные влияния отклонений от конфигурации базового компонента определены при оценке компонентов. Однако для высоких ОУД (где оценка базового компонента включает требования семейства ADV_TDS «Проект ОО») возможна ситуация, когда потенциально возможные воздействия в результате изменения руководств не могут быть полностью определены, поскольку не известны все свойства, если только представления детальной информации по проектированию базового компонента не предоставлены оценщику как часть информации о разработке составного ОО. В этом случае оценщик приводит в отчете информацию об остаточном риске после проведения анализа.

Эти остаточные риски должны быть включены в открытый отчет об оценке составного ОО.

Оценщик отмечает различия в руководствах для дальнейшего использования этих сведений в качестве исходных данных для проведения независимых действий оценщика по тестированию (семейство ACO_CTT «Тестирование составного ОО»).

Руководство для составного ОО может добавляться к руководству для компонентов, особенно с точки зрения установки и порядка проведения этапов установки базового компонента относительно этапов установки зависимого компонента. Не следует изменять порядок установки отдельных компонентов, однако они, возможно, должны чередоваться. Оценщик исследует руководство составного ОО, чтобы удостовериться, что оно все еще отвечает требованиям деятельности по AGD_PRE, выполняемой во время оценивания компонентов.

Может иметь место случай, когда информация о зависимостях идентифицирует, что на интерфейсы базового компонента, помимо идентифицированных как ИФБО, полагается зависимый компонент, идентифицированный в информации о зависимостях. Может потребоваться, чтобы было предоставлено руководство по использованию любых таких дополнительных интерфейсов базового компонента. Если пользователь составного ОО должен получить документацию руководств для базового компонента, тогда результаты оценивания AGD_PRE и вердиктов по AGD_OPE базового компонента могут быть повторно использованы для тех интерфейсов, которые рассматриваются при оценке базового компонента. Однако для дополнительных интерфейсов, на которые полагается зависимый компонент, оценщик должен будет сделать заключение о том, что документация руководств для базового компонента отвечает требованиям AGD_PRE и AGD_OPE, как применимо для оценки базовых компонентов.

Для интерфейсов, которые были рассмотрены во время оценки базового компонента и для которых уже было приобретено доверие, оценщик удостоверяется, что руководство для использования каждого интерфейса составного ОО согласуется с тем, которое предусмотрено базовым компонентом. В целях вынесения заключения о том, что руководство составного ОО согласуется с руководством базового компонента, оценщику следует выполнить прослеживание каждого интерфейса к руководству, предусмотренному и для составного ОО и для базового компонента. Затем оценщик сравнивает руководства, чтобы сделать заключение о том, что они согласованы.

Примеры дополнительных ограничений, предоставленных в руководстве составного ОО, которое предположительно совместимо с руководством компонента (руководства компонента сопровождаются примером руководства для составного ОО, которое предположительно обеспечивает введение дополнительных ограничений):

Компонент: «Длина пароля должна быть минимум 8 символов, включая буквенные символы и цифры».

Составной ОО: «Длина пароля должна быть минимум 10 символов, включая буквенные символы и цифры *и по крайней мере один из следующих специальных символов: ( ) { } ^ < > - _».*

Примечание — было бы приемлемо просто увеличить длину пароля до значения [*целое число> 8*], с удалением мандата по включению буквенных символов и цифр для составного ОО, если бы та же или более высокая метрика достигалась для оценивания стойкости пароля (с учетом предполагаемой вероятности того или иного сочетания символов в качестве пароля).

Компонент: «Следующие службы должны быть отключены в настройках реестра: служба публикации в WWW и служба ICDBReporter».

Составной ОО: «Следующие службы должны быть отключены в настройках реестра: *служба публикации, служба ICDBReporter, локатор удаленного вызова процедур (RPC) и служба вызова процедур (RPC)».*

Компонент: «Выберите следующие атрибуты для включения в системный журнал регистрации событий: дата, время, тип события, сведения об инициировавшем событие пользователе и результат события (успех/провал)».

Составной ОО: «Выберите следующие атрибуты для включения в системный журнал регистрации событий: дата, время, тип события, сведения об инициировавшем событие пользователе и результат события (успех/провал), *сообщение о событии и нить (последовательность инструкций на выполнение) процесса.*

Если руководство для составного ОО отклоняется от предусмотренного для базового компонента (т. е. не усиливает его требования), оценщик оценивает потенциальные риски модификации руководств. Оценщик использует доступную информацию (в том числе из общедоступных источников, а также описание архитектуры базового компонента в открытом отчете об оценке (например отчете о сертификации) и содержание руководств в другой документации руководств) для того, чтобы идентифицировать вероятное воздействие модификации руководств на ФТБ составного ОО.

Если во время оценки зависимого компонента для пробной установки использовался базовый компонент для удовлетворения требований среды функционирования зависимого компонента, данный шаг оценивания составного ОО считается удовлетворенным. Если базовый компонент не использовался при удовлетворении требований шага оценивания AGD_PRE.1-3 во время оценки зависимого компонента, оценщик обращается к пользовательским процедурам, предусматриваемым для подготовки составного ОО к функционированию в соответствии с руководством, определенным в AGD_PRE.1-3. Это позволит оценщику сделать заключение о том, что в подготовительном руководстве рассматривается сборка составного ОО в достаточной мере для того, чтобы надежно подготовить к эксплуатации составной ОО и среду его функционирования.

15.3.1.2.3.3 Жизненный цикл

Поставка

Если существуют различные механизмы, используемые для поставки составного ОО (то есть компоненты не поставляются пользователю в соответствии с безопасными процедурами поставки, определенными и оцененными во время оценки компонентов), для процедур поставки составного ОО требуется оценка выполнения требований семейства «Поставка» (ALC_DEL), применяемых во время оценивания компонентов.

Составной ОО может быть поставлен как интегрированный продукт или же может потребоваться осуществить поставку его компонентов отдельно для последующей сборки.

Если компоненты поставляются отдельно, возможно повторное использование результатов поставки базового и зависимого компонента. Поставка базового компонента проверяется во время проведения оценщиком пробной установки зависимого компонента с использованием указанного руководства и с проверкой аспектов поставки, ответственность за проведение которых, согласно документации руководств для базового компонента, несет сам пользователь.

Если составной ОО поставляется в качестве новой сущности, то метод поставки этой сущности нужно рассмотреть в рамках осуществления действий по оценке составного ОО.

Оценка процедур поставки компонентов составного ОО должна выполняться в соответствии с методологией оценки семейства «Поставка» (ALC_DEL), как и оценка поставки любого другого ОО [ОО-компонента], с обеспечением того, что любые расширенные элементы (например дополнительные руководства для составного ОО) рассматриваются в процедурах поставки.

Возможности УК

Уникальную идентификацию составного ОО рассматривают во время применения «Подвида деятельности по оценке ALC_CMC.1», а компоненты данного составного ОО рассматриваются во время применения «Подвида деятельности по оценке ALC_CMS.2».

Хотя для составного ОО, возможно, потребуется составить дополнительное руководство, уникальная идентификация данного руководства (рассматриваемая как часть уникальной идентификации

составного ОО во время «Подвида деятельности по оценке ALC_CMC.1») считается достаточным контролем руководства.

Вердикты оценщика по остальным (не рассмотренным выше) мероприятиям класса ALC: «Поддержка жизненного цикла», вынесенные во время оценки базового компонента, могут быть повторно использованы, поскольку во время интеграции составного ОО не производится дальнейшая разработка.

Не имеется дополнительных вопросов по безопасности разработки, требующих рассмотрения, поскольку предполагается, что интеграция компонентов ОО в составной ОО происходит или на месте у пользователя или, в случае, если составной ОО поставляется в виде интегрированного продукта, на месте у разработчика зависимых компонентов. Контроль за местом сборки у пользователя находится вне рассмотрения стандарта ИСО/МЭК 15408. Не требуется дополнительных требований или руководств, если интеграция зависимых компонентов ОО в составной ОО происходит там же, где и интеграция всех прочих компонентов, так как все компоненты считаются элементами конфигурации составного ОО и их поэтому следует рассматривать при осуществлении разработчиком зависимого компонента мер безопасности.

Инструменты и методы, принятые во время интеграции, рассматриваются в свидетельствах, предоставленных разработчиком зависимого компонента. Любые инструменты/методы, относящиеся к базовому компоненту, рассматриваются во время оценки базового компонента. Например, если базовый компонент поставлен в виде исходного кода и требует компиляции пользователем (например разработчиком зависимого компонента, который осуществляет интеграцию), компилятор должен быть определен и оценен наряду с соответствующими аргументами во время оценивания базового компонента.

К составному ОО не применяется определение жизненного цикла, поскольку не происходит дальнейшей разработки элементов.

Результаты исправления недостатков компонента не применимы к составному ОО. Если устранение недостатков включается в пакет доверия для составного ОО, то во время проведения оценки составного ОО к нему должны быть применены и требования семейства «Устранение недостатков» (то же касается любого усиления).

15.3.1.2.3.4 Тесты

Составной ОО будет тестироваться во время проведения действий оценки зависимого компонента по классу ATE: «Тестирование», поскольку в конфигурации, используемые для тестирования зависимого компонента, следует включать и базовый компонент в целях удовлетворения требований, предъявляемых к продуктам ИТ в среде функционирования ОО. Если базовый компонент не используется при тестировании зависимого компонента для оценки зависимого компонента или если конфигурация компонентов отличается от их оцененной конфигурации, то тесты разработчика, выполняемые для оценки зависимого компонента в целях удовлетворения требований класса ATE: «Тестирование», должны быть выполнены повторно для составного ОО.

15.4 Свидетельство разработки (ACO_DEV)

15.4.1 Подвид деятельности по оценке (ACO_DEV.1)

15.4.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение, что базовым компонентом для поддержания зависимого компонента обеспечивается выполнение определенных функций безопасности. Это заключение достигается посредством анализа интерфейсов базового компонента для вынесения заключения о том, что они совместимы с интерфейсами, определенными в информации о зависимостях; эти интерфейсы требуются зависимым компонентом.

Описание интерфейсов в базовом компоненте должно быть представлено с уровнем детализации, совместимым с «Подвидом деятельности по оценке ADV_FSP.2», хотя не все аспекты, необходимые для удовлетворения «Подвида деятельности по оценке ADV_FSP.2», требуются для «Подвида деятельности по оценке ACO_DEV.1», так как после идентификации интерфейса и описания остальных деталей интерфейса в его назначении, спецификация, использованная при оценке базового компонента, может быть использована повторно.

15.4.1.2 Исходные данные

Свидетельствами оценки этого подвида деятельности являются:

a) составное ЗБ;

b) информация о разработке;

c) информация о зависимостях.

15.4.1.3 Действие ACO_DEV.1.1E

ИСО/МЭК 15408-3 ACO_DEV.1.1C: *Информация по разработке должна описывать назначение каждого интерфейса базового компонента, используемого в составном ОО.*

15.4.1.3.1 Шаг оценивания ACO_DEV.1-1

Оценщик должен исследовать информацию о разработке, чтобы сделать заключение о том, что в ней описано назначение каждого интерфейса.

Базовый компонент предоставляет интерфейсы для поддержания взаимодействия с зависимым компонентом при предоставлении зависимых ФБО. Назначение каждого интерфейса должно быть описано с тем же уровнем детализации, что и описание интерфейсов в функциях, относящихся к ФБО зависимого компонента, как обеспечивается между подсистемами проекта ОО (см. «Подвид деятельности по оценке ADV_TDS.1»). Это описание должно предоставить читателю понимание того, каким образом базовый компонент предоставляет сервисы, требуемые ФБО зависимого компонента.

Этот шаг оценивания может быть удовлетворен посредством предоставления функциональной спецификации базового компонента для тех интерфейсов, которые являются интерфейсами ФБО базового компонента.

ИСО/МЭК 15408-3 ACO_DEV.1.2C: *Информация по разработке должна показывать соответствие между интерфейсами базового и зависимого компонентов, используемыми в составном ОО для поддержки ФБО зависимого компонента.*

15.4.1.3.2 Шаг оценивания ACO_DEV.1-2

Оценщик должен исследовать информацию о разработке, чтобы сделать заключение о том, что между интерфейсами базового компонента и интерфейсами, на которые полагается зависимый компонент, имеется точное соответствие.

Демонстрация соответствия между интерфейсами базового компонента и интерфейсами, на которые полагается зависимый компонент, может производиться в виде матрицы или таблицы. Интерфейсы, на которые полагается зависимый компонент, идентифицированы в информации о зависимостях (как исследуется во время деятельности по оценке семейства ACO_REL «Зависимости зависимых компонентов»).

Во время выполнения этой деятельности не предъявляется никаких требований по необходимости вынесения заключения о полноте охвата интерфейсов, на которые полагается зависимый компонент; заключение необходимо сделать только о том, что имеется точное соответствие и прослеживание между интерфейсами базового компонента и интерфейсами, требуемыми зависимым компонентом везде, где это представляется возможным. Полнота охвата рассматривается в действиях по оценке семейства «Обоснование композиции» (ACO_COR).

15.4.1.4 Действие ACO_DEV.1.2E

15.4.1.4.1 Шаг оценивания ACO_DEV.1-3

Оценщик должен исследовать информацию о разработке и информацию о зависимостях, чтобы сделать заключение о том, что интерфейсы описаны согласованным и последовательным образом.

Цель оценщика на данном шаге оценивания состоит в том, чтобы сделать заключение, согласуются ли описания интерфейсов в информации о разработке для базового компонента и информации о зависимостях для зависимого компонента.

15.4.2 Подвид деятельности по оценке (ACO_DEV.2)

15.4.2.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение, что базовым компонентом для поддержания зависимого компонента обеспечивается выполнение определенных функций безопасности. Это заключение достигается посредством анализа интерфейсов базового компонента и связанных с ними режимов функционирования базового компонента для вынесения заключения о том, что они совместимы с интерфейсами, определенными в информации о зависимостях; эти интерфейсы требуются зависимым компонентом.

15.4.2.2 Исходные данные

Свидетельствами оценки этого подвида деятельности являются:

a) составное ЗБ;

b) информация о разработке;

c) информация о зависимостях.

15.4.2.3 Действие ACO_DEV.2.1E

ИСО/МЭК 15408-3 ACO_DEV.2.1C: *Информация по разработке должна описывать назначение и метод использования каждого интерфейса базового компонента, используемого в составном ОО.*

15.4.2.3.1 Шаг оценивания ACO_DEV.2-1

Оценщик должен исследовать информацию о разработке, чтобы сделать заключение о том, что в ней описано назначение каждого интерфейса.

Базовый компонент предоставляет интерфейсы для поддержания взаимодействия с зависимым компонентом при предоставлении зависимых ФБО. Назначение каждого интерфейса должно быть описано с тем же уровнем детализации, что и описание интерфейсов в функциях, относящихся к ФБО зависимого компонента, как обеспечивается между подсистемами проекта ОО (см. «Подвид деятельности по оценке ADV_TDS.1»). Это описание должно предоставить читателю понимание того, каким образом базовый компонент предоставляет сервисы, требуемые ФБО зависимого компонента.

Этот шаг оценивания может быть удовлетворен посредством предоставления функциональной спецификации базового компонента для тех интерфейсов, которые являются интерфейсами ФБО базового компонента.

15.4.2.3.2 Шаг оценивания ACO_DEV.2-2

Оценщик должен исследовать информацию о разработке, чтобы сделать заключение о том, что в ней описан метод использования каждого интерфейса.

Метод использования для интерфейса предоставляет краткую информацию по поводу того, каким образом интерфейсом управляют в целях вызова некоторых операций и получения некоторых связанных с интерфейсом результатов. Оценщику следует быть в состоянии сделать заключение о том, что при прочтении этого материала в информации о разработке становится ясно, каким образом следует использовать каждый из интерфейсов. Это не обязательно означает, что для каждого интерфейса должен быть отдельный метод использования, поскольку может не быть возможности описать методы вызова, например интерфейса программирования приложений и затем идентифицировать каждый интерфейс, используя общий стиль описания.

Этот шаг оценивания может быть удовлетворен посредством предоставления функциональной спецификации базового компонента для тех интерфейсов, которые являются интерфейсами ФБО базового компонента.

ИСО/МЭК 15408-3 ACO_DEV.2.2C: *В информации по разработке должно быть представлено описание верхнего уровня для режима функционирования базового компонента, который поддерживает осуществление ФТБ зависимого компонента.*

15.4.2.3.3 Шаг оценивания ACO_DEV.2-3

Оценщик должен исследовать информацию о разработке, чтобы сделать заключение о том, что в ней описан режим функционирования базового компонента, который поддерживает выполнение ФТБ для зависимого компонента.

Зависимый компонент вызывает интерфейсы базового компонента для предоставления базовым компонентом зависимому некоторых сервисов. В информации о разработке должно приводиться описание верхнего уровня режима функционирования базового компонента для вызываемых интерфейсов базового компонента. Описание безопасного режима функционирования базового компонента обрисовывает в общих чертах, каким образом базовый компонент предоставляет необходимый сервис при вызове интерфейса. Это описание должно быть осуществлено на уровне, сходном с предусматриваемым по ADV_TDS.1.4C. Поэтому предоставление свидетельств оценки базового компонента по проекту ОО, когда интерфейсы, вызываемые зависимым компонентом, являются интерфейсами ФБО базового компонента, удовлетворяет требованиям данного шага оценивания. Если интерфейсы, вызываемые зависимым компонентом, не являются ИФБО базового компонента, связанный с такими интерфейсами безопасный режим функционирования не обязательно должен быть описан в свидетельствах проекта ОО базового компонента.

ИСО/МЭК 15408-3 ACO_DEV.2.3C: *Информация по разработке должна показывать соответствие между интерфейсами базового и зависимого компонентов, используемыми в составном ОО для поддержки ФБО зависимого компонента.*

15.4.2.3.4 Шаг оценивания ACO_DEV.2-4

Оценщик должен исследовать информацию о разработке, чтобы сделать заключение о том, что между интерфейсами базового компонента и интерфейсами, на которые полагается зависимый компонент, имеется точное соответствие.

Демонстрация соответствия между интерфейсами базового компонента и интерфейсами, на которые полагается зависимый компонент, может производиться в виде матрицы или таблицы. Интерфейсы, на которые полагается зависимый компонент, идентифицированы в информации о зависимостях (как исследуется во время деятельности по оценке семейства ACO_REL «Зависимости зависимых компонентов»).

Во время проведения этой деятельности не предъявляется никаких требований о необходимости вынесения заключения о полноте охвата интерфейсов, на которые полагается зависимый компонент; заключение необходимо сделать только о том, что имеется точное соответствие и прослеживание между интерфейсами базового компонента и интерфейсами, требуемыми зависимым компонентом везде, где это представляется возможным. Полнота охвата рассматривается в действиях по оценке семейства «Обоснование композиции» (ACO_COR).

15.4.2.4 Действие ACO_DEV.2.2E

15.4.2.4.1 Шаг оценивания ACO_DEV.2-5

Оценщик должен исследовать информацию о разработке и информацию о зависимостях, чтобы сделать заключение о том, что интерфейсы описаны согласованным и последовательным образом.

Цель оценщика на данном шаге оценивания состоит в том, чтобы сделать заключение о том, согласуются ли описания интерфейсов в информации о разработке для базового компонента и информации о зависимостях для зависимого компонента.

15.4.3 Подвид деятельности по оценке (ACO_DEV.3)

15.4.3.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение, что базовым компонентом для поддержания зависимого компонента обеспечивается выполнение определенных функций безопасности. Это заключение достигается посредством анализа интерфейсов базового компонента и связанных с ними режимов функционирования базового компонента для вынесения заключения о том, что они совместимы с интерфейсами, определенными в информации о зависимостях; эти интерфейсы требуются зависимым компонентом.

В дополнение к описанию интерфейса необходимо описать подсистемы базового компонента, которые обеспечивают выполнение функций безопасности, требуемых зависимым компонентом, чтобы позволить оценщику сделать заключение о том, является ли данный интерфейс частью ФБО базового компонента.

15.4.3.2 Исходные данные

Свидетельствами оценки этого подвида деятельности являются:

a) составное ЗБ;

b) информация о разработке;

c) информация о зависимостях.

15.4.3.3 Действие ACO_DEV.3.1E

ИСО/МЭК 15408-3 ACO_DEV.3.1C: *Информация по разработке должна описывать назначение и метод использования каждого интерфейса базового компонента, используемого в составном ОО.*

15.4.3.3.1 Шаг оценивания ACO_DEV.3-1

Оценщик должен исследовать информацию о разработке, чтобы сделать заключение о том, что в ней описано назначение каждого интерфейса.

Базовый компонент предоставляет интерфейсы для поддержания взаимодействия с зависимым компонентом при предоставлении зависимых ФБО. Назначение каждого интерфейса должно быть описано с тем же уровнем детализации, что и описание интерфейсов в функциях, относящихся к ФБО зависимого компонента, как обеспечивается между подсистемами проекта ОО (см. «Подвид деятельности по оценке ADV_TDS.1»). Это описание должно предоставить читателю понимание того, каким образом базовый компонент предоставляет сервисы, требуемые ФБО зависимого компонента.

Этот шаг оценивания может быть удовлетворен посредством предоставления функциональной спецификации базового компонента для тех интерфейсов, которые являются интерфейсами ФБО базового компонента.

15.4.3.3.2 Шаг оценивания ACO_DEV.3-2

Оценщик должен исследовать информацию о разработке, чтобы сделать заключение о том, что в ней описан метод использования каждого интерфейса.

Метод использования для интерфейса предоставляет краткую информацию по поводу того, каким образом интерфейсом управляют в целях вызова некоторых операций и получения некоторых связанных с интерфейсом результатов. Оценщику следует быть в состоянии сделать заключение о том, что при прочтении этого материала в информации о разработке становится ясно, каким образом следует использовать каждый из интерфейсов. Это не обязательно означает, что для каждого интерфейса должен быть отдельный метод использования, поскольку может не быть возможности описать методы вызова, например интерфейса программирования приложений и затем идентифицировать каждый интерфейс, используя общий стиль описания.

Этот шаг оценивания может быть удовлетворен посредством предоставления функциональной спецификации базового компонента для тех интерфейсов, которые являются интерфейсами ФБО базового компонента.

ИСО/МЭК 15408-3 ACO_DEV.3.2C: *В информации по разработке должны быть идентифицированы подсистемы базового компонента, которые предоставляют интерфейсы базового компонента, используемого в составном ОО.*

15.4.3.3.3 Шаг оценивания ACO_DEV.3-3

Оценщик должен исследовать информацию о разработке, чтобы сделать заключение о том, что идентифицированы все подсистемы базового компонента, которые предоставляют интерфейсы базового компонента зависимому.

Для тех интерфейсов, которые считаются частью ИФБО базового компонента, подсистемы, связанные с интерфейсами, будут рассматриваться во время деятельности по оценке семейства «Проект ОО» (ADV_TDS) для базового компонента. Интерфейсы, на которые полагается зависимый компонент, и которые при этом не являются частью ИФБО базового компонента, прослеживаются к подсистемам, находящимся вне ФБО базового компонента.

ИСО/МЭК 15408-3 ACO_DEV.3.3C: *В информации по разработке должно быть представлено высокоуровневое описание режима функционирования подсистем базового компонента, которые поддерживают выполнение ФТБ зависимого компонента.*

15.4.3.3.4 Шаг оценивания ACO_DEV.3-4

Оценщик должен исследовать информацию о разработке, чтобы сделать заключение о том, что в ней описан режим функционирования подсистем базового компонента, которые поддерживают выполнение ФТБ для зависимого компонента.

Зависимый компонент вызывает интерфейсы базового компонента для предоставления базовым компонентом зависимому некоторых сервисов. В информации о разработке должно приводиться описание верхнего уровня для соответствующего вызываемым интерфейсам режима функционирования базового компонента. Описание безопасного режима функционирования базового компонента обрисовывает в общих чертах, каким образом базовый компонент предоставляет необходимый сервис при вызове интерфейса. Это описание должно быть осуществлено на уровне, сходном с предусматриваемым по ADV_TDS.1.4C. Поэтому предоставление свидетельств оценки базового компонента по проекту ОО, когда интерфейсы, вызываемые зависимым компонентом, являются интерфейсами ФБО базового компонента, удовлетворяет требованиям данного шага оценивания. Если интерфейсы, вызываемые зависимым компонентом, не являются ИФБО базового компонента, связанный с такими интерфейсами безопасный режим функционирования не обязательно должен быть описан в свидетельствах проекта ОО базового компонента.

ИСО/МЭК 15408-3 ACO_DEV.3.4C: *В информации о разработке должно быть обеспечено прослеживание интерфейсов к подсистемам базового компонента.*

15.4.3.3.5 Шаг оценивания ACO_DEV.3-5

Оценщик должен исследовать информацию о разработке, чтобы сделать заключение о том, что между интерфейсами и подсистемами базового компонента имеется точное соответствие.

В случае, если оценщику доступны проект ОО и свидетельства функциональной спецификации базового компонента, он может использовать эти свидетельства для проверки точности соответствия между интерфейсами и подсистемами базового компонента как использующегося в составном ОО. Те интерфейсы базового компонента, которые являются частью ИФБО базового компонента, будут описаны в функциональной спецификации базового компонента, а связанные с этими интерфейсами подсистемы будут описаны в свидетельствах по проекту ОО базового компонента. Прослеживание между этими подсистемами и интерфейсами представлено в свидетельствах проекта ОО для базового компонента.

Если же интерфейс базового компонента не является частью ИФБО базового компонента, для верификации точности соответствия будет использоваться описание режима функционирования подсистемы, предоставленное в информации о разработке.

ИСО/МЭК 15408-3 ACO_DEV.3.5C: *Информация по разработке должна показывать соответствие между используемыми в составном ОО интерфейсами базового и зависимого компонентов для поддержки ФБО зависимого компонента.*

15.4.3.3.6 Шаг оценивания ACO_DEV.3-6

Оценщик должен исследовать информацию о разработке, чтобы сделать заключение о том, что между интерфейсами базового компонента и интерфейсами, на которые полагается зависимый компонент, имеется точное соответствие.

Демонстрация соответствия между интерфейсами базового компонента и интерфейсами, на которые полагается зависимый компонент, может производиться в виде матрицы или таблицы. Интерфейсы, на которые полагается зависимый компонент, идентифицированы в информации о зависимостях (как исследуется во время деятельности по оценке семейства ACO_REL «Зависимости зависимых компонентов»).

Во время проведения этой деятельности не предъявляется никаких требований по необходимости вынесения заключения о полноте охвата интерфейсов, на которые полагается зависимый компонент; заключение необходимо сделать только о том, что имеется точное соответствие и прослеживание между интерфейсами базового компонента и интерфейсами, требуемыми зависимым компонентом везде, где это представляется возможным. Полнота охвата рассматривается в действиях по оценке семейства «Обоснование композиции» (ACO_COR).

15.4.3.4 Действие ACO_DEV.3.2E

15.4.3.4.1 Шаг оценивания ACO_DEV.3-7

Оценщик должен исследовать информацию о разработке и информацию о зависимостях, чтобы сделать заключение о том, что интерфейсы описаны согласованным и последовательным образом.

Цель оценщика на данном шаге оценивания состоит в том, чтобы сделать заключение о том, согласуются ли описания интерфейсов в информации о разработке для базового компонента и информации о зависимостях для зависимого компонента.

15.5 Зависимости зависимых компонентов (ACO_REL)

15.5.1 Подвид деятельности по оценке (ACO_REL.1)

15.5.1.1 Цели

Цель этого подвида деятельности — сделать заключение о том, предоставлена ли в полученных от разработчика свидетельствах доверия достаточная информация для того, чтобы определить, что необходимые функции доступны в базовом компоненте, а также определить средства и способы вызова этих функций. Вся эта информация должна быть представлена в виде описаний верхнего уровня.

15.5.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) составное ЗБ;
b) функциональная спецификация зависимого компонента;
c) проект зависимого компонента;
d) проект архитектуры зависимого компонента;
e) информация о зависимостях.

15.5.1.3 Замечания по применению

Для зависимого компонента, ФБО которого взаимодействуют с базовым компонентом, требуются функции, обеспеченные этим базовым компонентом (например удаленная аутентификация, удаленное хранение данных аудита). В таких случаях вызываемые сервисы должны быть описаны вместе с теми, которые требуются для формирования составного ОО конечными пользователями. Обоснование необходимости такой документации заключается в том, что эти сведения должны помочь интеграторам составного ОО определить, какие сервисы базового компонента могут оказывать отрицательное воздействие на зависимый компонент, а также они предоставляют информацию, на основании которой можно сделать заключение о совместимости компонентов при применении требований семейства «Свидетельство разработки» (ACO_DEV).

15.5.1.4 Действие ACO_REL.1.1E

ИСО/МЭК 15408-3 ACO_REL.1.1C: *В информации о зависимостях должны быть описаны функции аппаратного, программного и программно-аппаратного обеспечения базового компонента, на которые полагаются ФБО зависимого компонента.*

15.5.1.4.1 Шаг оценивания ACO_REL.1-1

Оценщик должен проверить информацию о зависимостях, чтобы сделать заключение о том, что в ней описаны функции аппаратного, программного и программно-аппаратного обеспечения базового компонента, на которые полагаются ФБО зависимого компонента.

Оценщик оценивает описание функций безопасности аппаратного, программного и программно-аппаратного обеспечения базового компонента, которые требуются ФБО зависимого компонента. Особое внимание при выполнении данного шага оценивания уделяется уровню детализации этого описания, а не оценке точности информации (оценка точности информации проводится при выполнении следующего шага оценивания).

Описание функциональных возможностей базового компонента должно быть выполнено с уровнем детализации не выше, чем при описании компонента ФБО, предоставленного в проекте ОО (семейство ADV_TDS «Проект ОО»).

15.5.1.4.2 Шаг оценивания ACO_REL.1-2

Оценщик должен исследовать информацию о зависимостях, чтобы сделать заключение о том, что в ней точно отражены цели безопасности, определенные для среды функционирования зависимого компонента.

Информация о зависимостях содержит описание функций безопасности базового компонента, на которые полагается зависимый компонент. Чтобы удостовериться, что информация о зависимостях согласуется с ожиданиями, предъявляемыми к среде функционирования зависимого компонента, оценщик сравнивает информацию о зависимостях с заявленными в ЗБ целями безопасности среды функционирования для зависимого компонента.

Например, если в информации о зависимостях утверждается, что ФБО зависимого компонента полагаются на базовый компонент для хранения и защиты контрольных данных, а из других свидетельств оценки (например из проекта зависимого компонента) следовало бы, что ФБО зависимого компонента самостоятельно хранят и защищают контрольные данные, это указывало бы на несоответствие.

Следует отметить, что цели среды функционирования могут включать в себя цели, достигающиеся без применения средств ИТ. Хотя сервисы, которые предположительно должны быть обеспечены средой функционирования, могут быть описаны в рамках описания в ЗБ целей ИТ для среды функционирования зависимого компонента, не требуется, чтобы все такие ожидания от среды функционирования были описаны в информации о зависимостях.

ИСО/МЭК 15408-3 ACO_REL.1.2C: *В информации о зависимостях должны быть описаны все взаимодействия, через которые ФБО зависимого компонента запрашивают сервисы базового компонента.*

15.5.1.4.3 Шаг оценивания ACO_REL.1-3

Оценщик должен исследовать информацию о зависимостях, чтобы сделать заключение о том, что в ней описаны все взаимодействия между зависимым компонентом и базовым, через которые ФБО зависимого компонента запрашивает сервисы базового компонента.

ФБО зависимого компонента могут запросить сервисы базового компонента, не принадлежащие к ФБО базового компонента (см. ИСО/МЭК 15408-3, приложение В.3 «Взаимодействия между объединенными сущностями ИТ»).

Интерфейсы функций базового компонента описываются на таком же уровне представления, как и при описании интерфейсов функций ФБО зависимого компонента, как предоставляется между подсистемами в проекте ОО (см. Подвид деятельности по оценке (ADV_TDS.1)).

Цель описания взаимодействий между зависимым компонентом и базовым состоит в том, чтобы обеспечить понимание того, каким образом ФБО зависимого компонента полагаются на базовый компонент для предоставления сервисов, поддерживающих выполнение функций безопасности зависимого компонента. Эти взаимодействия не должны характеризоваться на уровне реализации (например передача параметров от принятого метода одного компонента до такого же принятого метода другого компонента), но элементы данных, идентифицированных для конкретного компонента, которые будут использоваться в другом компоненте, следует охватить этим описанием. Следует, чтобы такое утверждение помогло читателю понять, зачем вообще необходимо взаимодействие.

Точность и полнота интерфейсов основывается на функциях безопасности, которые требуются ФБО зависимого компонента от базового компонента, что оценивается при выполнении шагов оценивания ACO_REL.1-1 и ACO_REL.1-2. Следует иметь возможность прослеживания всех функций, описанных на более ранних шагах оценивания, к интерфейсам, идентифицированным на этом шаге оценивания, и возможность обратного прослеживания. Наличие интерфейса, который не соответствует описанным функциям, также указало бы на несоответствие.

ИСО/МЭК 15408-3 ACO_REL.1.3C: *В информации о зависимостях должно быть описание того, каким образом ФБО зависимого компонента обеспечивают собственную защиту от вмешательства со стороны базового компонента.*

15.5.1.4.4 Шаг оценивания ACO_REL.1-4

Оценщик должен исследовать информацию о зависимостях, чтобы сделать заключение о том, что в ней описано, каким образом ФБО зависимого компонента обеспечивают собственную защиту от вмешательства со стороны базового компонента.

Описание того, каким образом зависимый компонент защищает себя от вмешательства базового компонента, должно быть представлено с тем же уровнем детализации, что необходим для ADV_ARC.1-4.

15.5.2 Подвид деятельности по оценке (ACO_REL.2)

15.5.2.1 Цели

Цель этого подвида деятельности — сделать заключение о том, предоставлена ли в полученных от разработчика свидетельствах доверия достаточная информация для того, чтобы определить, что необходимые функции доступны в базовом компоненте, а также определить средства и способы вызова этих функций. Это обеспечивается в терминах взаимодействий между зависимым и основным компонентом, а также возвращаемых значений от интерфейсов, вызываемых зависимым компонентом.

15.5.2.2 Исходные данные

Свидетельствами оценки этого подвида деятельности являются:

a) составное ЗБ;

b) функциональная спецификация зависимого компонента;

c) проект зависимого компонента;

d) представление реализации зависимого компонента;

e) проект архитектуры зависимого компонента;

f) информация о зависимостях.

15.5.2.3 Замечания по применению

Для зависимого компонента, ФБО которого взаимодействуют с базовым компонентом, требуются функции, обеспеченные этим базовым компонентом (например удаленная аутентификация, удаленное хранение данных аудита). В таких случаях вызываемые сервисы должны быть описаны вместе с теми, которые требуются для формирования составного ОО конечными пользователями. Обоснование необходимости такой документации заключается в том, что эти сведения должны помочь интеграторам составного ОО определить, какие сервисы базового компонента могут оказывать отрицательное воздействие на зависимый компонент, а также они предоставляют информацию, на основании которой можно сделать заключение о совместимости компонентов при применении требований семейства «Свидетельство разработки» (ACO_DEV).

15.5.2.4 Действие ACO_REL.2.1E

ИСО/МЭК 15408-3 ACO_REL.2.1C: *В информации о зависимостях должны быть описаны функции аппаратного, программного и программно-аппаратного обеспечения базового компонента, на которые полагаются ФБО зависимого компонента.*

15.5.2.4.1 Шаг оценивания ACO_REL.2-1

Оценщик должен проверить информацию о зависимостях, чтобы сделать заключение о том, что в ней описаны функции аппаратного, программного и программно-аппаратного обеспечения базового компонента, на которые полагаются ФБО зависимого компонента.

Оценщик оценивает описание функций безопасности аппаратного, программного и программно-аппаратного обеспечения базового компонента, которые требуются ФБО зависимого компонента. Особое внимание при выполнении данного шага оценивания уделяется уровню детализации этого описания, а не оценке точности информации (оценка точности информации проводится при выполнении следующего шага оценивания).

Описание функциональных возможностей базового компонента должно быть выполнено с уровнем детализации не выше, чем при описании компонента ФБО, предоставленного в проекте ОО (семейство ADV_TDS «Проект ОО»).

15.5.2.4.2 Шаг оценивания ACO_REL.2-2

Оценщик должен исследовать информацию о зависимостях, чтобы сделать заключение о том, что в ней точно отражены цели безопасности, определенные для среды функционирования зависимого компонента.

Информация о зависимостях содержит описание функций безопасности базового компонента, на которые полагается зависимый компонент. Чтобы удостовериться, что информация о зависимостях согласуется с ожиданиями, предъявляемыми к среде функционирования зависимого компонента, оценщик сравнивает информацию о зависимостях с заявленными в ЗБ целями безопасности среды функционирования для зависимого компонента.

Например, если в информации о зависимостях утверждается, что ФБО зависимого компонента полагаются на базовый компонент для хранения и защиты контрольных данных, а из других свидетельств оценки (например из проекта зависимого компонента) следовало бы, что ФБО зависимого компонента самостоятельно хранят и защищают контрольные данные, это указывало бы на несоответствие.

Следует отметить, что цели среды функционирования могут включать в себя цели, достигающиеся без применения средств ИТ. Хотя сервисы, которые предположительно должны быть обеспечены средой функционирования, могут быть описаны в рамках описания в ЗБ целей ИТ для среды функцио-

нирования зависимого компонента, не требуется, чтобы все такие ожидания от среды функционирования были описаны в информации о зависимостях.

ИСО/МЭК 15408-3 ACO_REL.2.2C: *В информации о зависимостях должны быть описаны все взаимодействия, через которые ФБО зависимого компонента запрашивают сервисы базового компонента.*

15.5.2.4.3 Шаг оценивания ACO_REL.2-3

Оценщик должен исследовать информацию о зависимостях, чтобы сделать заключение о том, что в ней описаны все взаимодействия между зависимым компонентом и базовым, через которые ФБО зависимого компонента запрашивает сервисы базового компонента.

ФБО зависимого компонента могут запросить сервисы базового компонента, не принадлежащие к ФБО базового компонента (см. ИСО/МЭК 15408-3, приложение В.3 «Взаимодействия между объединенными сущностями ИТ»).

Интерфейсы функций базового компонента описываются на таком же уровне представления, как и при описании интерфейсов функций ФБО зависимого компонента, как предоставляется между подсистемами в проекте ОО (см. Подвид деятельности по оценке (ADV_TDS.1)).

Цель описания взаимодействий между зависимым компонентом и базовым состоит в том, чтобы обеспечить понимание того, каким образом ФБО зависимого компонента полагаются на базовый компонент для предоставления сервисов, поддерживающих выполнение функций безопасности зависимого компонента. Эти взаимодействия не должны характеризоваться на уровне реализации (например передача параметров от принятого метода одного компонента до такого же принятого метода другого компонента), но элементы данных, идентифицированных для конкретного компонента, которые будут использоваться в другом компоненте, следует охватить этим описанием. Следует, чтобы такое утверждение помогло читателю понять, зачем вообще необходимо взаимодействие.

Точность и полнота интерфейсов основывается на функциях безопасности, которые требуются ФБО зависимого компонента от базового компонента, что оценивается при выполнении шагов оценивания ACO_REL.2-1 и ACO_REL.2-2. Должна быть возможность прослеживания всех функций, описанных на более ранних шагах оценивания, к интерфейсам, идентифицированным на этом шаге оценивания, и возможность обратного прослеживания. Наличие интерфейса, который не соответствует описанным функциям, также указало бы на несоответствие.

ИСО/МЭК 15408-3 ACO_REL.2.3C: *В информации о зависимостях каждое взаимодействие должно быть описано в терминах используемых для этого интерфейсов и возвращаемых этими интерфейсами значений.*

15.5.2.4.4 Шаг оценивания ACO_REL.2-4

В информации о зависимостях должно быть описано каждое взаимодействие в терминах используемых для этого интерфейсов и возвращаемых этими интерфейсами значений.

Идентификация интерфейсов, используемых ФБО зависимого компонента при отправке запросов к сервисам базового компонента, позволяет лицу, осуществляющему интегрирование, определить, предоставляет ли базовый компонент все необходимые интерфейсы. Это понимание в дальнейшем получается путем спецификации возвращаемых интерфейсом значений, ожидаемых зависимым компонентом. Оценщик удостоверяется, что интерфейсы описаны для каждого идентифицированного взаимодействия (как анализируется в ACO_REL.2-3).

ИСО/МЭК 15408-3 ACO_REL.2.4C: *В информации о зависимостях должно быть описание того, каким образом ФБО зависимого компонента обеспечивают собственную защиту от вмешательства со стороны базового компонента.*

15.5.2.4.5 Шаг оценивания ACO_REL.2-5

Оценщик должен исследовать информацию о зависимостях, чтобы сделать заключение о том, что в ней описано, каким образом ФБО зависимого компонента обеспечивают собственную защиту от вмешательства со стороны базового компонента.

Описание того, каким образом зависимый компонент защищает себя от вмешательства базового компонента, должно быть представлено с тем же уровнем детализации, что необходим для ADV_ARC.1-4.

15.6 Тестирование составного ОО (ACO_CTT)

15.6.1 Подвид деятельности по оценке (ACO_CTT.1)

15.6.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, верным ли образом разработчик провел и зафиксировал тесты каждого из интерфейсов базового компонента, на которые полагается зависимый компонент. Как часть этого заключения оценщик повторно проводит выборочно не-

которые тесты, выполненные разработчиком, а также проводит любые дополнительные тесты, требуемые для того, чтобы удостовериться в том, что продемонстрирован ожидаемый режим функционирования всего составного ОО, ФТБ и интерфейсов базового компонента, на которые полагается зависимый компонент.

15.6.1.2 Исходные данные

Свидетельствами оценки этого подвида деятельности являются:

a) составной ОО, пригодный для тестирования;

b) составленные свидетельства тестирования ОО;

c) информация о зависимостях;

d) информация о разработке.

15.6.1.3 Действие ACO_CTT.1.1E

ИСО/МЭК 15408-3 ACO_CTT.1.1C: *Тестовая документация для составного ОО и интерфейсов базового компонента должна содержать планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.*

15.6.1.3.1 Шаг оценивания ACO_CTT.1-1

Оценщик должен исследовать тестовую документацию составного ОО, чтобы сделать заключение о том, что в нее включены планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.

Этот шаг оценивания может быть удовлетворен путем предоставления свидетельств тестирования оценки зависимого компонента, если базовый компонент использовался для удовлетворения требований к ИТ в среде функционирования зависимого компонента.

Все шаги оценивания, необходимые для удовлетворения ATE_FUN.1.1E, будут проведены для того, чтобы определить:

a) что тестовая документация содержит планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования;

b) что тестовая документация содержит информацию, необходимую для обеспечения воспроизводимости проведенных тестов;

c) уровень усилий разработчика, который применялся при тестировании базового компонента.

15.6.1.3.2 Шаг оценивания ACO_CTT.1-2

Оценщик должен исследовать тестовую документацию интерфейса базового компонента, чтобы сделать заключение о том, что в нее включены планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.

Этот шаг оценивания может быть удовлетворен путем предоставления свидетельств тестирования оценки базового компонента для интерфейсов, на которые полагается зависимый компонент составного ОО, которые являются ИФБО успешно оцененного базового компонента. Заключение о том, являются ли интерфейсы базового компонента, на которые ссылается зависимый компонент, интерфейсами ФБО оцененного базового компонента, выносится в рамках действия ACO_COR.

Все шаги оценивания, необходимые для удовлетворения ATE_FUN.1.1E, будут проведены для того, чтобы определить:

a) что тестовая документация содержит планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования;

b) что тестовая документация содержит информацию, необходимую для обеспечения воспроизводимости проведенных тестов;

c) уровень усилий разработчика, который применялся при тестировании базового компонента.

ИСО/МЭК 15408-3 ACO_CTT.1.2C: *Тестовая документация разработчика по результатам выполнения тестов по отношению к составному ОО должна демонстрировать, что режим функционирования ФБО соответствует спецификации.*

15.6.1.3.3 Шаг оценивания ACO_CTT.1-3

Оценщик должен исследовать тестовую документацию, чтобы сделать заключение о том, что выполнение разработчиком тестов составного ОО демонстрирует выполнение ФБО.

Оценщику следует проследить тесты, описанные в плане тестирования к ФТБ, определенным для составного ОО, чтобы идентифицировать, какие ФТБ были протестированы разработчиком.

Руководство по этому шагу оценивания представлено в:

a) пункте 13.2.1,

b) пункте 13.2.2.

Выходные данные успешного выполнения тестов согласно оценке ATE_FUN.1.3C можно сравнить с прослеживанием для того, чтобы сделать заключение, что ФТБ составного ОО, как проверено разработчиком, выполняются ожидаемым образом.

ИСО/МЭК 15408-3 ACO_CTT.1.3C: *Тестовая документация по результатам выполнения разработчиком тестирования интерфейсов базового компонента должна продемонстрировать, что режим функционирования конкретного интерфейса базового компонента, на который полагается зависимый компонент, соответствует спецификации.*

15.6.1.3.4 Шаг оценивания ACO_CTT.1-4

Оценщик должен исследовать тестовую документацию, чтобы сделать заключение о том, что выполнение разработчиком тестирования интерфейсов базового компонента демонстрирует, что интерфейсы базового компонента, на которые полагается зависимый компонент, выполняются согласно спецификации.

Оценщику следует провести прослеживание между тестами, описанными в плане тестирования и интерфейсами базового компонента, на которые полагается зависимый компонент (как определено в информации о зависимостях и исследуется в рамках ACO_REL), чтобы идентифицировать, какие интерфейсы базового компонента были протестированы разработчиком.

Руководство по этому шагу оценивания представлено в:

a) пункте 13.2.1,

b) пункте 13.2.2.

Выходные данные успешного выполнения тестов согласно оценке ATE_FUN.1.3C можно сравнить с прослеживанием для того, чтобы сделать заключение, что ФТБ составного ОО, как проверено разработчиком, выполняются согласно спецификации.

ИСО/МЭК 15408-3 ACO_CTT.1.4C: *Базовый компонент должен быть пригоден для тестирования.*

15.6.1.3.5 Шаг оценивания ACO_CTT.1-5

Оценщик должен исследовать составной ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Чтобы сделать заключение, что составной ОО был установлен правильно и находится в известном состоянии, к ОО, предоставленному разработчиком для тестирования, применяются шаги оценивания ATE_IND.2-1 и ATE_IND.2-2.

15.6.2 Шаг оценивания ACO_CTT.1-6

Оценщик должен исследовать набор полученных от разработчика ресурсов, чтобы сделать заключение о том, что этот набор эквивалентен набору ресурсов, используемому разработчиком базового компонента для проведения функционального тестирования базового компонента.

Для вынесения заключения о том, что набор обеспеченных ресурсов эквивалентен используемым для проведения функционального тестирования базового компонента, используемого в составном ОО, применяется шаг оценивания ATE_IND.2-3.

15.6.2.1 Действие ACO_CTT.1.2E

15.6.2.1.1 Шаг оценивания ACO_CTT.1-7

Оценщик должен выполнить тестирование в соответствии с ATE_IND.2.2E для подмножества ФТБ, определенного в составном ЗБ, чтобы проверить результаты тестирования, проведенного разработчиком.

Оценщик применяет все шаги оценивания, необходимые для удовлетворения ATE_IND.2.2E, а также приводит в ТОО для составного ОО весь проведенный им анализ, его результаты и вердикты, продиктованные выполнением соответствующих шагов оценивания.

15.6.2.2 Действие ACO_CTT.1.3E

15.6.2.2.1 Шаг оценивания ACO_CTT.1-8

Оценщик должен выполнить тестирование в соответствии с ATE_IND.2.3E для подмножества ФТБ, определенного в составном ЗБ, чтобы подтвердить, что ФБО выполняются согласно спецификации.

Оценщик применяет все шаги оценивания, необходимые для удовлетворения ATE_IND.2.3E, а также приводит в ТОО для составного ОО весь проведенный им анализ, его результаты и вердикты, продиктованные выполнением соответствующих шагов оценивания.

При выборе для тестирования интерфейсов ФБО составного ОО, оценщику следует принимать во внимание любые модификации компонентов оцененной версии или конфигурации. Примерами модификаций компонентов оцененной версии или конфигурации могут быть примененные исправления, изменение конфигурации в результате внесения изменений в документацию руководств, доверие к дополнительной части компонента, которая относится к ФБО компонента. Эти модификации будут идентифицированы во время деятельности по оценке семейства «Обоснование композиции» (ACO_COR).

15.6.3 Подвид деятельности по оценке (ACO_CTT.2)

15.6.3.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение, верным ли образом разработчик провел и зафиксировал тесты каждого из интерфейсов базового компонента, на которые по-

лагается зависимый компонент. Как часть этого заключения оценщик повторно проводит выборочно некоторые тесты, выполненные разработчиком, а также проводит любые дополнительные тесты, требуемые для того, чтобы удостовериться в том, что продемонстрирован ожидаемый режим функционирования всего составного ОО и интерфейсов базового компонента, на которые полагается зависимый компонент.

15.6.3.2 Исходные данные

Свидетельствами оценки этого подвида деятельности являются:

a) составной ОО, пригодный для тестирования;

b) свидетельства тестирования составного ОО;

c) информация о зависимостях;

d) информация о разработке.

15.6.3.3 Действие ACO_CTT.2.1E

ИСО/МЭК 15408-3 ACO_CTT.2.1C: *Тестовая документация для составного ОО и интерфейсов базового компонента должна содержать планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.*

15.6.3.3.1 Шаг оценивания ACO_CTT.2-1

Оценщик должен исследовать тестовую документацию составного ОО, чтобы сделать заключение о том, что в нее включены планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.

Этот шаг оценивания может быть удовлетворен путем предоставления свидетельств тестирования оценки зависимого компонента, если базовый компонент использовался для удовлетворения требований к ИТ в среде функционирования зависимого компонента.

Все шаги оценивания, необходимые для удовлетворения ATE_FUN.1.1E, будут проведены для того, чтобы определить:

a) что тестовая документация содержит планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования;

b) что тестовая документация содержит информацию, необходимую для обеспечения воспроизводимости проведенных тестов;

c) уровень усилий разработчика, который применялся при тестировании базового компонента.

15.6.3.3.2 Шаг оценивания ACO_CTT.2-2

Оценщик должен исследовать тестовую документацию интерфейса базового компонента, чтобы сделать заключение о том, что в нее включены планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.

Этот шаг оценивания может быть удовлетворен путем предоставления свидетельств тестирования оценки базового компонента для интерфейсов, на которые полагается зависимый компонент составного ОО, которые являются ИФБО успешно оцененного базового компонента. Заключение о том, являются ли интерфейсы базового компонента, на которые ссылается зависимый компонент, интерфейсами ФБО оцененного базового компонента, выносится в рамках действия ACO_COR.

Все шаги оценивания, необходимые для удовлетворения ATE_FUN.1.1E, будут проведены для того, чтобы определить:

a) что тестовая документация содержит планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования;

b) что тестовая документация содержит информацию, необходимую для обеспечения воспроизводимости проведенных тестов;

c) уровень усилий разработчика, который применялся при тестировании базового компонента.

ИСО/МЭК 15408-3 ACO_CTT.2.2C: *Тестовая документация разработчика по результатам выполнения тестов по отношению к составному ОО должна демонстрировать, что режим функционирования ФБО соответствует спецификации и ФБО являются полными.*

15.6.3.3.3 Шаг оценивания ACO_CTT.2-3

Оценщик должен исследовать тестовую документацию, чтобы сделать заключение о том, что в ней представлено точное соответствие между тестами в тестовой документации, касающейся тестирования составного ОО, и ФТБ составного ОО в ЗБ составного ОО.

Простой перекрестной таблицы может быть достаточно для того, чтобы продемонстрировать соответствие тестирований. Идентификация соответствия между тестами и ФТБ, представленными в тестовой документации, должна быть однозначной.

15.6.3.3.4 Шаг оценивания ACO_CTT.2-4

Оценщик должен исследовать тестовую документацию, чтобы вынести заключение о том, что выполнение разработчиком тестирования составного ОО должно продемонстрировать, что ФБО ведет себя согласно спецификации.

Руководство по этому шагу оценивания представлено в:

a) пункте 13.2.1,

b) пункте 13.2.2.

Выходные данные успешного выполнения тестов согласно оценке ATE_FUN.1.3C можно сравнить с прослеживанием для того, чтобы сделать заключение, что ФТБ составного ОО, как проверено разработчиком, выполняются согласно спецификации.

ИСО/МЭК 15408-3 ACO_CTT.2.3C: *Тестовая документация по результатам выполнения разработчиком тестирования интерфейсов базового компонента должна продемонстрировать, что режим функционирования конкретного интерфейса базового компонента, на который полагается зависимый компонент, соответствует спецификации и этот интерфейс является полным.*

15.6.3.3.5 Шаг оценивания ACO_CTT.2-5

Оценщик должен исследовать тестовую документацию, чтобы сделать заключение о том, что в ней представлено точное соответствие между тестами в тестовой документации, касающейся тестирования интерфейсов базового компонента, на которые полагается зависимый компонент, и интерфейсами, определенными в информации о зависимостях.

Простой перекрестной таблицы может быть достаточно для того, чтобы продемонстрировать соответствие тестирований. Идентификация соответствия между тестами и ФТБ, представленными в тестовой документации, должна быть однозначной.

15.6.3.3.6 Шаг оценивания ACO_CTT.2-6

Оценщик должен исследовать тестовую документацию, чтобы сделать заключение о том, что выполнение разработчиком тестирования интерфейсов базового компонента демонстрирует, что интерфейсы базового компонента, на которые полагается зависимый компонент, выполняются согласно спецификации.

Оценщик должен провести прослеживание между тестами, описанными в плане тестирования и интерфейсами базового компонента, на которые полагается зависимый компонент (как определено в информации о зависимостях и исследуется в рамках ACO_REL), чтобы идентифицировать, какие интерфейсы базового компонента были протестированы разработчиком.

Руководство по этому шагу оценивания представлено в:

a) пункте 13.2.1,

b) пункте 13.2.2.

Выходные данные успешного выполнения тестов согласно оценке ATE_FUN.1.3C можно сравнить с прослеживанием для того, чтобы сделать заключение, что ФТБ составного ОО, как проверено разработчиком, выполняются согласно спецификации.

ИСО/МЭК 15408-3 ACO_CTT.2.4C: *Базовый компонент должен быть пригоден для тестирования.*

15.6.3.3.7 Шаг оценивания ACO_CTT.2-7

Оценщик должен исследовать составной ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Чтобы сделать заключение, что составной ОО был установлен правильно и находится в известном состоянии, к ОО, предоставленному разработчиком для тестирования, применяются шаги оценивания ATE_IND.2-1 и ATE_IND.2-2.

15.6.3.3.8 Шаг оценивания ACO_CTT.2-8

Оценщик должен исследовать набор полученных от разработчика ресурсов, чтобы сделать заключение о том, что этот набор эквивалентен набору ресурсов, используемому разработчиком базового компонента для проведения функционального тестирования базового компонента.

Чтобы сделать заключение о том, что набор обеспеченных ресурсов эквивалентен используемым для проведения функционального тестирования базового компонента, используемого в составном ОО, применяется шаг оценивания ATE_IND.2-3.

15.6.3.4 Действие ACO_CTT.2.2E

15.6.3.4.1 Шаг оценивания ACO_CTT.2-9

Тесты должны быть отобраны и выполнены в соответствии с ATE_IND.2.2E для того, чтобы продемонстрировать правильный режим выполнения ФТБ, определенных в ЗБ составного ОО.

Оценщик применяет все шаги оценивания, необходимые для удовлетворения ATE_IND.2.3E, а также приводит в ТОО для составного ОО весь проведенный им анализ, его результаты и вердикты, продиктованные выполнением соответствующих шагов оценивания.

15.6.3.5 Действие ACO_CTT.2.3E

15.6.3.5.1 Шаг оценивания ACO_CTT.2-10

Оценщик должен выполнить тестирование в соответствии с ATE_IND.2.3E для подмножества ФТБ, определенного в составном ЗБ, чтобы подтвердить, что ФБО выполняются согласно спецификации.

Оценщик применяет все шаги оценивания, необходимые для удовлетворения ATE_IND.2.3E, а также приводит в ТОО для составного ОО весь проведенный им анализ, его результаты и вердикты, продиктованные выполнением соответствующих шагов оценивания.

При выборе для тестирования интерфейсов ФБО составного ОО, оценщику следует принимать во внимание любые модификации компонентов оцененной версии или конфигурации. Примерами модификаций компонентов оцененной версии или конфигурации могут быть примененные исправления, изменение конфигурации в результате внесения изменений в документацию руководств, доверие к дополнительной части компонента, которая относится к ФБО компонента. Эти модификации будут идентифицированы во время деятельности по оценке семейства «Обоснование композиции» (ACO_COR).

15.6.3.5.2 Шаг оценивания ACO_CTT.2-11

Оценщик должен провести тестирование в соответствии с «Подвидом деятельности по оценке ATE_IND.2» для подмножества интерфейсов базового компонента, чтобы подтвердить, что они выполняются согласно спецификации.

Оценщик применяет все шаги оценивания, необходимые для удовлетворения ATE_IND.2.3E, а также приводит в ТОО для составного ОО весь проведенный им анализ, его результаты и вердикты, продиктованные выполнением соответствующих шагов оценивания.

При выборе для тестирования интерфейсов ФБО составного ОО, оценщику следует принимать во внимание любые модификации компонентов оцененной версии или конфигурации. Примерами модификаций компонентов оцененной версии или конфигурации могут быть примененные исправления, изменение конфигурации в результате внесения изменений в документацию руководств, доверие к дополнительной части компонента, которая относится к ФБО компонента. Эти модификации будут идентифицированы во время деятельности по оценке семейства «Обоснование композиции» (ACO_COR).

15.7 Анализ уязвимостей композиции (ACO_VUL)

15.7.1 Подвид деятельности по оценке (ACO_VUL.1)

15.7.1.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, имеются ли в составном ОО в его среде функционирования легко пригодные для использования уязвимости.

Разработчик предоставляет детальное описание любых остаточных уязвимостей для компонентов, которые приводятся в отчете при оценке. Оценщик выполняет анализ расположения остаточных уязвимостей, информация о которых приводилась в отчете, а также выполняет поиск в общедоступных источниках информации для идентификации любых новых потенциальных уязвимостей в компонентах (то есть тех проблем, о которых сообщалось в общедоступных источниках после проведения оценивания базового компонента). Затем оценщик выполняет тестирование проникновения в целях демонстрации того, что потенциальные уязвимости не могут использоваться в ОО в его среде функционирования нарушителем с Базовым потенциалом нападения.

15.7.1.2 Исходные данные

Свидетельствами оценки этого подвида деятельности являются:

a) пригодный для тестирования составной ОО;

b) составное ЗБ;

c) обоснование композиции;

d) документация руководств;

e) общедоступная информация для поддержки идентификации возможных уязвимостей безопасности;

f) остаточные уязвимости, которые приводятся в отчете во время оценивания каждого компонента.

15.7.1.3 Замечания по применению

См. Замечания по применению для «Подвида деятельности по оценке (AVA_VAN.1)».

15.7.1.4 Действие ACO_VUL.1.1E

ИСО/МЭК 15408-3 ACO_VUL.1.1C: *Составной ОО должен быть пригодным для тестирования.*

15.7.1.4.1 Шаг оценивания ACO_VUL.1-1

Оценщик должен исследовать составной ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Чтобы сделать заключение, правильно ли установлен составной ОО и находится ли в известном состоянии, к составному ОО применяются шаги оценивания ATE_IND.2-1 и ATE_IND.2-2.

Если в пакет доверия включены компоненты семейства ACO_CTT, то оценщик может обратиться к результату шага оценивания ACO_CTT*-1, чтобы продемонстрировать, что эти требования были удовлетворены.

15.7.1.4.2 Шаг оценивания ACO_VUL.1-2

Оценщик должен исследовать конфигурацию составного ОО, чтобы сделать заключение о том, что любые предположения и цели в ЗБ для компонентов, относящимся к сущностям ИТ, выполняются другими компонентами.

В ЗБ для компонентов могут быть включены предположения о других компонентах, которые могут использовать тот компонент, к которому ЗБ имеет отношение, например ЗБ для операционной системы, используемой в качестве базового компонента, может включать предположение, что любые приложения, загруженные в операционной системе, не запускаются привилегированным образом. Эти предположения и цели должны выполняться другими компонентами составного ОО.

15.7.1.5 Действие ACO_VUL.1.2E

15.7.1.5.1 Шаг оценивания ACO_VUL.1-3

Оценщик должен исследовать остаточные уязвимости после оценки базового компонента, чтобы сделать заключение о том, что они не пригодны для использования в составном ОО в его среде функционирования.

Перечень уязвимостей данного продукта, идентифицированных во время оценки базового компонента, для которых было продемонстрировано, что использование их в базовом компоненте для проведения атаки невозможно, должен использоваться в качестве исходных данных этой деятельности. Оценщик делает заключение, выполняется ли предположение о невозможности использования данной уязвимости в составном ОО или после сборки компонентов в составной ОО данную уязвимость снова следует рассматривать как потенциально опасную. Например, если во время оценки базового компонента было вынесено предположение, что была отключена некая конкретная служба операционной системы, которая была включена при оценке составного ОО, то любые потенциальные уязвимости, касающиеся этой службы, которые ранее были исключены из рассмотрения согласно вынесенному предположению, теперь следует рассматривать.

Кроме того, этот перечень известных, но непригодных для использования уязвимостей, полученный в результате оценки базового компонента, следует рассматривать в свете любых известных, но потенциально непригодных для использования уязвимостей в других компонентах (например в зависимом компоненте) составного ОО. Это необходимо для рассмотрения случая, когда потенциальную уязвимость, которую не получится использовать при отдельном использовании компонента, можно использовать, если компонент интегрируется с сущностью ИТ, содержащей другую потенциальную уязвимость.

15.7.1.5.2 Шаг оценивания ACO_VUL.1-4

Оценщик должен исследовать остаточные уязвимости после оценки зависимого компонента, чтобы сделать заключение о том, что они не пригодны для использования в составном ОО в его среде функционирования.

Перечень уязвимостей данного продукта, идентифицированных во время оценки зависимого компонента, для которых было продемонстрировано, что использование их в зависимом компоненте для проведения атаки невозможно, должен использоваться в качестве исходных данных этой деятельности. Оценщик делает заключение, выполняется ли предположение о невозможности использования данной уязвимости в составном ОО или после сборки компонентов в составной ОО данную уязвимость снова следует рассматривать как потенциально опасную. Например, если во время оценки базового компонента было вынесено предположение, что продукт ИТ, отвечающий требованиям среды функционирования, не будет возвращать некое значение в ответ на запрос службы, предоставляемой базовым ОО, то любые потенциальные уязвимости, касающиеся этого возвращаемого значения, которые ранее были исключены из рассмотрения согласно вынесенному предположению, теперь следует рассматривать.

Кроме того, этот перечень известных, но непригодных для использования уязвимостей, полученный в результате оценки зависимого компонента, следует рассматривать в свете любых известных, но потенциально непригодных для использования уязвимостей в других компонентах (например в базовом компоненте) составного ОО. Это необходимо для рассмотрения случая, когда потенциальная уязвимость непригодна для использования при использовании компонента отдельно, но становится пригодной для использования при интеграции компонента с сущностью ИТ, содержащей другую потенциальную уязвимость.

15.7.1.6 Действие ACO_VUL.1.3E

15.7.1.6.1 Шаг оценивания ACO_VUL.1-5

Оценщик должен исследовать общедоступные источники информации, чтобы поддержать идентификацию возможных уязвимостей защиты базового компонента, которые стали известны после завершения оценки базового компонента.

Оценщик будет использовать общедоступную информацию для поиска уязвимостей базового компонента так, как описано в AVA_VAN.1-2.

Те потенциальные уязвимости, информация о которых была общедоступной до оценивания базового компонента, не должны исследоваться далее, если только для оценщика не очевидно, что потенциал нападения, требуемый от нарушителя для использования потенциальной уязвимости, был значительно уменьшен. Это может быть реализовано путем внедрения какой-либо новой технологии после оценки базового компонента, что означает, что использование потенциальной уязвимости упростилось.

15.7.1.6.2 Шаг оценивания ACO_VUL.1-6

Оценщик должен исследовать общедоступные источники информации, чтобы поддержать идентификацию возможных уязвимостей защиты зависимого компонента, которые стали известны после завершения оценки зависимого компонента.

Оценщик будет использовать общедоступную информацию так, как описано в AVA_VAN.1-2 для поиска уязвимостей зависимого компонента.

Те потенциальные уязвимости, информация о которых была общедоступной до оценивания зависимого компонента, не должны исследоваться далее, если только для оценщика не очевидно, что потенциал нападения, требуемый от нарушителя для использования потенциальной уязвимости, был значительно уменьшен. Это может быть реализовано путем внедрения какой-либо новой технологии после оценки зависимого компонента, что означает, что возможность использования потенциальной уязвимости была упрощена.

15.7.1.6.3 Шаг оценивания ACO_VUL.1-7

Оценщик должен привести в ТОО идентифицированные потенциальные уязвимости, которые являются кандидатами на тестирование и применимы к данному составному ОО в среде его функционирования.

Чтобы сделать заключение, относятся ли уязвимости к составному ОО в его среде функционирования, используются свидетельства ЗБ, документации руководств и функциональной спецификации.

Оценщик делает запись относительно любых причин исключения уязвимостей из дальнейшего рассмотрения, если он делает заключение о том, что уязвимость невозможно использовать в среде функционирования. В ином случае оценщик фиксирует потенциальную уязвимость для дальнейшего рассмотрения.

Оценщик должен привести в ТОО перечень потенциальных уязвимостей, применимых к составному ОО в его среде функционирования; эта информация может использоваться в качестве исходных данных для действий по тестированию проникновения (то есть для ACO_VUL.1.4E).

15.7.1.7 Действие ACO_VUL.1.4E

15.7.1.7.1 Шаг оценивания ACO_VUL.1-8

Оценщик должен провести тестирование проникновения так, как детально описано в AVA_VAN.1.3E.

Оценщик применяет все шаги оценивания, необходимые для удовлетворения действия оценщика AVA_VAN.1.3E, и приводит в ТОО для составного ОО весь проведенный анализ и вердикты, требующиеся по данному шагу оценивания.

Оценщик также применяет шаги оценивания по действию оценщика AVA_VAN.1.1E, чтобы сделать заключение о том, что предоставленный разработчиком составной ОО является пригодным для тестирования.

15.7.2 Подвид деятельности по оценке (ACO_VUL.2)

15.7.2.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, имеются ли в составном ОО в его среде функционирования уязвимости, легко пригодные для использования нарушителями с Базовым потенциалом нападения.

Разработчик предоставляет детальное описание любых остаточных уязвимостей, которые приводятся в отчете, а также любых уязвимостей, появившихся в результате комбинирования базовых и зависимых компонентов. Оценщик выполняет поиск в общедоступных источниках информации для идентификации любых новых потенциальных уязвимостей в компонентах (то есть тех проблем, о которых сообщалось в общедоступных источниках после проведения оценивания компонентов). Также оценщик выполняет независимый анализ уязвимостей составного ОО и проводит тестирование проникновения.

15.7.2.2 Исходные данные

Свидетельствами оценки этого подвида деятельности являются:

a) пригодный для тестирования составной ОО;

b) составное ЗБ;

c) обоснование композиции;

d) документация руководств;

e) общедоступная информация для поддержки идентификации возможных уязвимостей безопасности;

f) остаточные уязвимости, которые приводятся в отчете во время оценивания каждого компонента.

15.7.2.3 Замечания по применению

См. Замечания по применению для «Подвида деятельности по оценке (AVA_VAN.2)».

15.7.2.4 Действие ACO_VUL.2.1E

ИСО/МЭК 15408-3 ACO_VUL.2.1C: *Составной ОО должен быть пригодным для тестирования.*

15.7.2.4.1 Шаг оценивания ACO_VUL.2-1

Оценщик должен исследовать составной ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Чтобы сделать заключение, правильно ли установлен составной ОО и находится ли в известном состоянии, к составному ОО применяются шаги оценивания ATE_IND.2-1 и ATE_IND.2-2.

Если в пакет доверия включены компоненты семейства ACO_CTT, то оценщик может обратиться к результату шага оценивания ACO_CTT*-1, чтобы продемонстрировать, что эти требования были удовлетворены.

15.7.2.4.2 Шаг оценивания ACO_VUL.2-2

Оценщик должен исследовать конфигурацию составного ОО, чтобы сделать заключение о том, что любые предположения и цели в ЗБ для компонентов, относящимся к сущностям ИТ, выполняются другими компонентами.

В ЗБ для компонентов могут быть включены предположения о других компонентах, которые могут использовать тот компонент, к которому ЗБ имеет отношение, например ЗБ для операционной системы, используемой в качестве базового компонента, может включать предположение, что любые приложения, загруженные в операционной системе, не запускаются привилегированным образом. Эти предположения и цели должны выполняться другими компонентами составного ОО.

15.7.2.5 Действие ACO_VUL.2.2E

15.7.2.5.1 Шаг оценивания ACO_VUL.2-3

Оценщик должен исследовать остаточные уязвимости после оценки базового компонента, чтобы сделать заключение о том, что они не пригодны для использования в составном ОО в его среде функционирования.

Перечень уязвимостей данного продукта, идентифицированных во время оценки базового компонента, для которых было продемонстрировано, что использование их в базовом компоненте для проведения атаки невозможно, должен использоваться в качестве исходных данных этой деятельности. Оценщик делает заключение, выполняется ли предположение о невозможности использования данной уязвимости в составном ОО, или после сборки компонентов в составной ОО данную уязвимость снова следует рассматривать как потенциально опасную. Например, если во время оценки базового компонента было вынесено предположение, что была отключена некая конкретная служба операционной системы, которая была включена при оценке составного ОО, то любые потенциальные уязвимости, касающиеся этой службы, которые ранее были исключены из рассмотрения согласно вынесенному предположению, теперь следует рассматривать.

Кроме того, этот перечень известных, но непригодных для использования уязвимостей, полученный в результате оценки базового компонента, следует рассматривать в свете любых известных, но потенциально непригодных для использования уязвимостей в других компонентах (например в зависимом компоненте) составного ОО. Это необходимо для рассмотрения случая, когда потенциальная уязвимость непригодна для использования при использовании компонента отдельно, но становится пригодной для использования при интеграции компонента с сущностью ИТ, содержащей другую потенциальную уязвимость.

15.7.2.5.2 Шаг оценивания ACO_VUL.2-4

Оценщик должен исследовать остаточные уязвимости после оценки зависимого компонента, чтобы сделать заключение о том, что они не пригодны для использования в составном ОО в его среде функционирования.

Перечень уязвимостей данного продукта, идентифицированных во время оценки зависимого компонента, для которых было продемонстрировано, что использование их в зависимом компоненте для проведения атаки невозможно, должен использоваться в качестве исходных данных этой деятельности. Оценщик делает заключение, выполняется ли предположение о невозможности использования данной

уязвимости в составном ОО, или после сборки компонентов в составной ОО данную уязвимость снова следует рассматривать как потенциально опасную. Например, если во время оценки базового компонента было вынесено предположение, что продукт ИТ, отвечающий требованиям среды функционирования, не будет возвращать некое значение в ответ на запрос службы, предоставляемой базовым ОО, то любые потенциальные уязвимости, касающиеся этого возвращаемого значения, которые ранее были исключены из рассмотрения согласно вынесенному предположению, теперь следует рассматривать.

Кроме того, этот перечень известных, но непригодных для использования уязвимостей, полученный в результате оценки зависимого компонента, следует рассматривать в свете любых известных, но потенциально непригодных для использования уязвимостей в других компонентах (например в базовом компоненте) составного ОО. Это необходимо для рассмотрения случая, когда потенциальная уязвимость непригодна для использования при использовании компонента отдельно, но становится пригодной для использования при интеграции компонента с сущностью ИТ, содержащей другую потенциальную уязвимость.

15.7.2.6 Действие ACO_VUL.2.3E

15.7.2.6.1 Шаг оценивания ACO_VUL.2-5

Оценщик должен исследовать общедоступные источники информации, чтобы поддержать идентификацию возможных уязвимостей защиты базового компонента, которые стали известны после завершения оценки базового компонента.

Оценщик будет использовать общедоступную информацию для поиска уязвимостей базового компонента так, как описано в AVA_VAN.2-2.

Те потенциальные уязвимости, информация о которых была общедоступной до оценивания базового компонента, не должны исследоваться далее, если только для оценщика не очевидно, что потенциал нападения, требуемый от нарушителя для использования потенциальной уязвимости, был значительно уменьшен. Это может быть реализовано путем внедрения какой-либо новой технологии после оценки базового компонента, что означает, что использование потенциальной уязвимости упростилось.

15.7.2.6.2 Шаг оценивания ACO_VUL.2-6

Оценщик должен исследовать общедоступные источники информации, чтобы поддержать идентификацию возможных уязвимостей защиты зависимого компонента, которые стали известны после завершения оценки зависимого компонента.

Оценщик будет использовать общедоступную информацию так, как описано в AVA_VAN.2-2 для поиска уязвимостей зависимого компонента.

Те потенциальные уязвимости, информация о которых была общедоступной до оценивания зависимого компонента, не должны исследоваться далее, если только для оценщика не очевидно, что потенциал нападения, требуемый от нарушителя для использования потенциальной уязвимости, был значительно уменьшен. Это может быть реализовано путем внедрения какой-либо новой технологии после оценки зависимого компонента, что означает, что возможность использования потенциальной уязвимости была упрощена.

15.7.2.6.3 Шаг оценивания ACO_VUL.2-7

Оценщик должен привести в ТОО идентифицированные потенциальные уязвимости, которые являются кандидатами на тестирование и применимы к данному составному ОО в среде его функционирования.

Для вынесения заключения о том, относятся ли уязвимости к составному ОО в его среде функционирования, используются свидетельства ЗБ, документации руководств и функциональной спецификации.

Оценщик делает запись относительно любых причин исключения уязвимостей из дальнейшего рассмотрения, если он делает заключение о том, что уязвимость невозможно использовать в среде функционирования. В ином случае оценщик фиксирует потенциальную уязвимость для дальнейшего рассмотрения.

Оценщик должен привести в ТОО перечень потенциальных уязвимостей, применимых к составному ОО в его среде функционирования; эта информация может использоваться в качестве исходных данных для действий по тестированию проникновения (то есть для ACO_VUL.2.5E).

15.7.2.7 Действие ACO_VUL.2.4E

15.7.2.7.1 Шаг оценивания ACO_VUL.2-8

Оценщик должен провести поиск сведений в ЗБ составного ОО, документации руководств, информации о зависимостях и обосновании композиции, чтобы идентифицировать возможные уязвимости безопасности в составном ОО.

Рассмотрение компонентов составного ОО при независимом анализе уязвимости оценщика для оценки компонентов будет принимать несколько отличающуюся от зарегистрированной в AVA_VAN.2.3E форму, поскольку будет не обязательно рассматривать все уровни представления проекта как относящиеся к пакету доверия. Их будут рассматривать во время оценки компонентов, но свидетельства могут быть недоступны для оценки составного ОО. Однако общий подход, описанный в единицах работы, связанных с AVA_VAN.2.3E, применим, и на его основании следует проводить поиск потенциальных уязвимостей в составном ОО.

Анализ уязвимостей отдельных компонентов, используемых в составном ОО, будет выполнен уже во время оценки отдельных компонентов. Анализ уязвимостей во время оценки составного ОО должен быть направлен на идентификацию любых уязвимостей, введенных в результате интеграции компонентов или внесения любых изменений в использование компонентов между конфигурацией оцененного компонента к конфигурации составного ОО.

Оценщик будет использовать понимание конструкции компонентов согласно детализации в информации о зависимостях для зависимого компонента и информации о разработке и обосновании композиции для базового компонента вместе с информацией о проекте зависимого компонента. Эта информация позволит оценщику получать понимание того, каким образом взаимодействуют базовый компонент и зависимый компонент, а также идентифицировать потенциальные уязвимости, которые могут возникать в результате этого взаимодействия.

Оценщик рассматривает все новые руководства по установке, запуску и функционированию составного ОО для идентификации любых потенциальных уязвимостей, полученных из-за пересмотра данных руководств.

Если над каким-либо из отдельных компонентов были проведены действия по обеспечению непрерывности доверия после завершения оценки компонентов, оценщик рассматривает исправления при проведении независимого анализа уязвимостей. Основным источником исходных данных по поводу внесенных изменений будет информация, представленная в открытом отчете по действиям, обеспечивающим непрерывность доверия (например в отчете об обслуживании). Эта информация дополняется любыми обновлениями документации руководств, следующей из внесения в систему изменений, а также любой общедоступной информацией об изменениях, например на веб-сайте поставщика.

Любые риски, идентифицированные из-за нехватки свидетельств для выяснения полной степени воздействия любых исправлений или отклонений конфигурации компонента от оцененной конфигурации, должны быть зарегистрированы в ходе анализа уязвимости оценщика.

15.7.2.8 Действие ACO_VUL.2.5E

15.7.2.8.1 Шаг оценивания ACO_VUL.2-9

Оценщик должен провести тестирование проникновения так, как детально описано в AVA_VAN.2.4E.

Оценщик применяет все шаги оценивания, необходимые для удовлетворения действия оценщика AVA_VAN.2.4E, и приводит в ТОО для составного ОО весь проведенный анализ и вердикты, требующиеся по данному шагу оценивания.

Оценщик также применяет шаги оценивания по действию оценщика AVA_VAN.2.1E, чтобы сделать заключение о том, что предоставленный разработчиком составной ОО является пригодным для тестирования.

15.7.3 Подвид деятельности по оценке (ACO_VUL.3)

15.7.3.1 Цели

Цель этого подвида деятельности состоит в том, чтобы сделать заключение о том, имеются ли в составном ОО в его среде функционирования уязвимости, легко пригодные для использования нарушителями с Усиленным базовым потенциалом нападения.

Разработчик предоставляет анализ расположения любых остаточных уязвимостей компонентов, которые приводились в отчете, а также любых уязвимостей, появившихся в результате комбинирования базовых и зависимых компонентов. Оценщик выполняет поиск в общедоступных источниках информации для идентификации любых новых потенциальных уязвимостей в компонентах (то есть тех проблем, о которых сообщалось в общедоступных источниках после проведения оценивания компонентов). Также оценщик выполняет независимый анализ уязвимостей составного ОО и проводит тестирование проникновения.

15.7.3.2 Исходные данные

Свидетельствами оценки этого подвида деятельности являются:

a) пригодный для тестирования составной ОО;

b) составное ЗБ;

c) обоснование композиции;

d) информация о зависимостях;

e) документация руководств;

f) общедоступная информация для поддержки идентификации возможных уязвимостей безопасности;

g) остаточные уязвимости, которые приводились в отчете во время оценивания каждого компонента.

15.7.3.3 Замечания по применению

См. Замечания по применению для «Подвида деятельности по оценке (AVA_VAN.3)».

15.7.3.4 Действие ACO_VUL.3.1E

ИСО/МЭК 15408-3 ACO_VUL.3.1C: *Составной ОО должен быть пригодным для тестирования.*

15.7.3.4.1 Шаг оценивания ACO_VUL.3-1

Оценщик должен исследовать составной ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Чтобы сделать заключение, правильно ли установлен составной ОО и находится ли в известном состоянии, к составному ОО применяются шаги оценивания ATE_IND.2-1 и ATE_IND.2-2.

Если в пакет доверия включены компоненты семейства ACO_CTT, то оценщик может обратиться к результату шага оценивания ACO_CTT*-1, чтобы продемонстрировать, что эти требования были удовлетворены.

15.7.3.4.2 Шаг оценивания ACO_VUL.3-2

Оценщик должен исследовать конфигурацию составного ОО, чтобы сделать заключение о том, что любые предположения и цели в ЗБ для компонентов, относящимся к сущностям ИТ, выполняются другими компонентами.

В ЗБ для компонентов могут быть включены предположения о других компонентах, которые могут использовать тот компонент, к которому ЗБ имеет отношение, например ЗБ для операционной системы, используемой в качестве базового компонента, может включать предположение, что любые приложения, загруженные в операционной системе, не запускаются привилегированным образом. Эти предположения и цели должны выполняться другими компонентами составного ОО.

15.7.3.5 Действие ACO_VUL.3.2E

15.7.3.5.1 Шаг оценивания ACO_VUL.3-3

Оценщик должен исследовать остаточные уязвимости после оценки базового компонента, чтобы сделать заключение о том, что они не пригодны для использования в составном ОО в его среде функционирования.

Перечень уязвимостей данного продукта, идентифицированных во время оценки базового компонента, для которых было продемонстрировано, что использование их в базовом компоненте для проведения атаки невозможно, должен использоваться в качестве исходных данных этой деятельности. Оценщик делает заключение, выполняется ли предположение о невозможности использования данной уязвимости в составном ОО, или после сборки компонентов в составной ОО данную уязвимость снова следует рассматривать как потенциально опасную. Например, если во время оценки базового компонента было вынесено предположение, что была отключена некая конкретная служба операционной системы, которая была включена при оценке составного ОО, то любые потенциальные уязвимости, касающиеся этой службы, которые ранее были исключены из рассмотрения согласно вынесенному предположению, теперь следует рассматривать.

Кроме того, этот перечень известных, но непригодных для использования уязвимостей, полученный в результате оценки базового компонента, следует рассматривать в свете любых известных, но потенциально непригодных для использования уязвимостей в других компонентах (например в зависимом компоненте) составного ОО. Это необходимо для рассмотрения случая, когда потенциальную уязвимость, которую не получится использовать при отдельном использовании компонента, можно использовать, если компонент интегрируется с сущностью ИТ, содержащей другую потенциальную уязвимость.

15.7.3.5.2 Шаг оценивания ACO_VUL.3-4

Оценщик должен исследовать остаточные уязвимости после оценки зависимого компонента, чтобы сделать заключение о том, что они не пригодны для использования в составном ОО в его среде функционирования.

Перечень уязвимостей данного продукта, идентифицированных во время оценки зависимого компонента, для которых было продемонстрировано, что использование их в зависимом компоненте для проведения атаки невозможно, должен использоваться в качестве исходных данных этой деятельности. Оценщик делает заключение, выполняется ли предположение о невозможности использования данной уязвимости в составном ОО, или после сборки компонентов в составной ОО данную уязвимость снова следует рассматривать как потенциально опасную. Например, если во время оценки базового компонента было вынесено предположение, что продукт ИТ, отвечающий требованиям среды функционирования,

не будет возвращать некое значение в ответ на запрос службы, предоставляемой базовым ОО, то любые потенциальные уязвимости, касающиеся этого возвращаемого значения, которые ранее были исключены из рассмотрения согласно вынесенному предположению, теперь следует рассматривать.

Кроме того, этот перечень известных, но непригодных для использования уязвимостей, полученный в результате оценки зависимого компонента, следует рассматривать в свете любых известных, но потенциально непригодных для использования уязвимостей в других компонентах (например в базовом компоненте) составного ОО. Это необходимо для рассмотрения случая, когда потенциальную уязвимость, которую не получится использовать при отдельном использовании компонента, можно использовать, если компонент интегрируется с сущностью ИТ, содержащей другую потенциальную уязвимость.

15.7.3.6 Действие ACO_VUL.3.3E

15.7.3.6.1 Шаг оценивания ACO_VUL.3-5

Оценщик должен исследовать общедоступные источники информации, чтобы поддержать идентификацию возможных уязвимостей защиты базового компонента, которые стали известны после завершения оценки базового компонента.

Оценщик будет использовать общедоступную информацию для поиска уязвимостей базового компонента так, как описано в AVA_VAN.3-2.

Те потенциальные уязвимости, информация о которых была общедоступной до оценивания базового компонента, не должны исследоваться далее, если только для оценщика не очевидно, что потенциал нападения, требуемый от нарушителя для использования потенциальной уязвимости, был значительно уменьшен. Это может быть реализовано путем внедрения какой-либо новой технологии после оценки базового компонента, что означает, что использование потенциальной уязвимости упростилось.

15.7.3.6.2 Шаг оценивания ACO_VUL.3-6

Оценщик должен исследовать общедоступные источники информации, чтобы поддержать идентификацию возможных уязвимостей защиты зависимого компонента, которые стали известны после завершения оценки зависимого компонента.

Оценщик будет использовать общедоступную информацию так, как описано в AVA_VAN.3-2 для поиска уязвимостей зависимого компонента.

Те потенциальные уязвимости, информация о которых была общедоступной до оценивания зависимого компонента, не должны исследоваться далее, если только для оценщика не очевидно, что потенциал нападения, требуемый от нарушителя для использования потенциальной уязвимости, был значительно уменьшен. Это может быть реализовано путем внедрения какой-либо новой технологии после оценки зависимого компонента, что означает, что возможность использования потенциальной уязвимости была упрощена.

15.7.3.6.3 Шаг оценивания ACO_VUL.3-7

Оценщик должен привести в ТОО идентифицированные потенциальные уязвимости, которые являются кандидатами на тестирование и применимы к данному составному ОО в среде его функционирования.

Для вынесения заключения о том, относятся ли уязвимости к составному ОО в его среде функционирования, используются свидетельства ЗБ, документации руководств и функциональной спецификации.

Оценщик делает запись относительно любых причин исключения уязвимостей из дальнейшего рассмотрения, если он делает заключение о том, что уязвимость невозможно использовать в среде функционирования. В ином случае оценщик фиксирует потенциальную уязвимость для дальнейшего рассмотрения.

Оценщик должен привести в ТОО перечень потенциальных уязвимостей, применимых к составному ОО в его среде функционирования; эта информация может использоваться в качестве исходных данных для действий по тестированию проникновения (то есть для ACO_VUL.3.5E).

15.7.3.7 Действие ACO_VUL.3.4E

15.7.3.7.1 Шаг оценивания ACO_VUL.3-8

Оценщик должен провести поиск сведений в ЗБ составного ОО, документации руководств, информации о зависимостях и обосновании композиции, чтобы идентифицировать возможные уязвимости безопасности в составном ОО.

Рассмотрение компонентов составного ОО при независимом анализе уязвимости оценщика для оценки компонентов будет принимать несколько отличающуюся от зарегистрированной в AVA_VAN.3.3E форму, поскольку будет не обязательно рассматривать все уровни представления проекта как относящиеся

к пакету доверия. Их будут рассматривать во время оценки компонентов, но свидетельства могут быть недоступны для оценки составного ОО. Однако общий подход, описанный в единицах работы, связанных с AVA_VAN.3.3E, применим, и на его основании следует проводить поиск потенциальных уязвимостей в составном ОО.

Анализ уязвимостей отдельных компонентов, используемых в составном ОО, будет выполнен уже во время оценки отдельных компонентов. Анализ уязвимостей во время оценки составного ОО должен быть направлен на идентификацию любых уязвимостей, введенных в результате интеграции компонентов или внесения любых изменений в использование компонентов между конфигурацией оцененного компонента к конфигурации составного ОО.

Оценщик будет использовать понимание конструкции компонентов согласно детализации в информации о зависимостях для зависимого компонента и информации о разработке и обосновании композиции для базового компонента вместе с информацией о проекте зависимого компонента. Эта информация позволит оценщику получать понимание того, каким образом взаимодействуют базовый компонент и зависимый компонент, а также идентифицировать потенциальные уязвимости, которые могут возникать в результате этого взаимодействия.

Оценщик рассматривает все новые руководства по установке, запуску и функционированию составного ОО для идентификации любых потенциальных уязвимостей, полученных из-за пересмотра данных руководств.

Если над каким-либо из отдельных компонентов были проведены действия по обеспечению непрерывности доверия после завершения оценки компонентов, оценщик рассматривает исправления при проведении независимого анализа уязвимостей. Основным источником исходных данных по поводу внесенных изменений будет информация, представленная в открытом отчете по действиям, обеспечивающим непрерывность доверия (например в отчете об обслуживании). Эта информация дополняется любыми обновлениями документации руководств, следующей из внесения в систему изменений, а также любой общедоступной информацией об изменениях, например на веб-сайте поставщика.

Любые риски, идентифицированные из-за нехватки свидетельств для выяснения полной степени воздействия любых исправлений или отклонений конфигурации компонента от оцененной конфигурации, должны быть зарегистрированы в ходе анализа уязвимости оценщика.

15.7.3.8 Действие ACO_VUL.3.5E

15.7.3.8.1 Шаг оценивания ACO_VUL.3-9

Оценщик должен провести тестирование проникновения так, как детально описано в AVA_VAN.3.4E.

Оценщик применяет все шаги оценивания, необходимые для удовлетворения действия оценщика AVA_VAN.3.4E, и приводит в ТОО для составного ОО весь проведенный анализ и вердикты, требующиеся по данному шагу оценивания.

Оценщик также применяет шаги оценивания по действию оценщика AVA_VAN.2.1E, чтобы сделать заключение о том, что предоставленный разработчиком составной ОО является пригодным для тестирования.

Приложение А
(информативное)

Общие указания по оценке

А.1 Цели

Цель данного подраздела состоит в том, чтобы охватить общие вопросы руководства обеспечением технического подтверждения результатов оценки. Использование такого общего руководства помогает достичь объективности, повторяемости и воспроизводимости работы, выполненной оценщиком.

А.2 Выборка

Данный подраздел предоставляет общие указания по осуществлению выборки. Конкретная и подробная информация дана в шагах оценивания, соответствующих определенным элементам действий оценщика, где выборку необходимо выполнить.

Выборка — определенная процедура, выполняемая оценщиком, посредством которой некоторое подмножество требуемой совокупности свидетельств оценки исследуется и предполагается репрезентативным (представительным) для совокупности в целом. Это позволяет оценщику получить достаточную уверенность в правильности конкретного свидетельства оценки без его анализа в полном объеме. Выборка производится для экономии ресурсов при поддержании адекватного уровня доверия. Выборка из свидетельства может приводить к двум возможным результатам:

a) На подмножестве не обнаружено никаких ошибок, что дает оценщику определенную уверенность в том, что совокупность в целом корректна.

b) На подмножестве найдены ошибки, и поэтому правильность совокупности в целом подвергается сомнению. Даже устранение всех обнаруженных ошибок может оказаться недостаточным для получения оценщиком необходимой уверенности, и поэтому оценщику придется либо увеличить размер подмножества, либо прекратить использование выборки для этого конкретного свидетельства.

Выборка — это метод, который может использоваться для получения заслуживающих доверия выводов, когда состав свидетельства относительно однороден по существу, например если свидетельство является результатом полностью определенного процесса.

Выборка в случаях, указанных в ИСО/МЭК 15408 или специально оговоренных в шагах оценивания методологии, признается как экономичный подход к действиям, выполняемым оценщиком. Выборка в других областях разрешается только в исключительных случаях, там, где выполнение конкретного вида деятельности в целом потребовало бы усилий, непропорциональных другим видам деятельности, и где оно не повысило бы соответственно доверие. В таких случаях потребуется обоснование применения выборки в этой области. Ни тот факт, что ОО является объемным и сложным, ни то, что он имеет много функциональных требований безопасности, не является достаточным обоснованием, так как при оценке объемных и сложных ОО как раз и могут потребоваться большие усилия. Скорее предполагается, что это исключение ограничивается такими случаями, когда подход к разработке ОО дает большое количество материала для конкретного требования ИСО/МЭК 15408, который обычно весь требуется проверить или исследовать, и когда не ожидается, что такое действие повысит соответственно степень доверия.

Выборка нуждается в логическом обосновании, принимая во внимание возможное влияние на цели безопасности и угрозы ОО. Влияние зависит от того, что может быть пропущено в результате выборки. Необходимо также учитывать характер свидетельства, проверяемого выборочно, и требование не игнорировать любые функции безопасности и не снижать их роль.

Следует признать, что выборка из свидетельства, прямо связанного с реализацией ОО (например результатов теста разработчика), требует подхода, отличного от применяемого при выборке, связанного с вынесением заключения о том, правильно ли выполнялся процесс. Во многих случаях, когда от оценщика требуется определить, что процесс действительно выполняется, рекомендуется стратегия выборки. Подход, который применяется при выборке результатов тестирования разработчиком, будет отличаться. Это происходит потому, что в первом случае речь идет об уверенности в том, что процесс выполняется, а во втором мы имеем дело с определением корректности реализации ОО. Как правило, более объемные выборки следует анализировать в случаях, связанных с правильной реализацией ОО, нежели с необходимостью удостовериться, что процесс выполняется.

В определенных случаях для оценщика может быть уместно придавать большее значение повторению тестирований, проведенных разработчиком. Например, если независимые тесты, которые осталось провести оценщику, только поверхностно отличаются от включенных в обширный набор проверок, проведенных разработчиком (допустим, что разработчик провёл тестирование в большем объеме, чем необходимо для удовлетворения критериев классов ATE_COV «Покрытие» и ATE_DPT «Глубина»), тогда оценщику целесообразнее сосредоточить усилия на повторении проверок, проведенных разработчиком. Следует отметить, что это не обязательно подразумевает требование большой доли выборки при повторении тестов разработчика; на самом деле, учитывая обширный набор проверок, проведенных разработчиком, оценщик может обосновать необходимость повторения лишь весьма малого процента тестовых испытаний.

В тех случаях, когда разработчик для проведения функционального тестирования применил автоматизированное средство тестирования, оценщику обычно будет проще повторно запустить средство тестирования и провести полную проверку заново, нежели выборочно повторить тестирования, проведенные разработчиком. Однако оценщик обязан проверить, что автоматизированное тестирование не дает искаженных результатов. Подразумевается, что эта проверка должна быть выполнена с выборкой среди тестов, проведенных автоматизированным средством тестирования, по принципу оказания предпочтения проверке некоторых тестов из всех возможных и при этом с обеспечением достаточности объема выборки.

При выборке рекомендуется всегда придерживаться следующих принципов:

a) Осуществление выборки не должно носить случайный характер, выборка должна проводиться таким образом, чтобы она являлась репрезентативной (показательной) для всех свидетельств. Объем выборки и её состав всегда должны быть обоснованы.

b) В случае, когда выборка имеет отношение к верной реализации ОО, следует, чтобы она была репрезентативна по всем аспектам, относящимся к областям применения выборки. В частности, следует, чтобы выборка охватила все разнообразие компонентов, функций безопасности, мест разработки и эксплуатации (если их несколько) и типов аппаратных платформ (если их несколько). Объем выборки следует сопоставить с эффективностью затрат на проведение оценки, он зависит от некоторых характеристик ОО (например от размеров и сложности ОО, от объема документации).

c) Также, в случае, когда осуществление выборки касается получения конкретного свидетельства того, что тестирование, проводимое разработчиком, является повторяемым и воспроизводимым, используемая выборка должна быть достаточной для того, чтобы представить все аспекты тестовых проверок, проводимых разработчиком, например такие, как различные тестовые режимы. Используемая выборка должна быть достаточной для обнаружения любой систематически возникающей проблемы в функциональном процессе тестирования, проводимого разработчиком. Вклад оценщика, складывающийся из повторения тестов, проведенных разработчиком, и выполнения независимых тестов, должен быть достаточным для обращения к основным важным характеристикам ОО.

d) Когда выборка осуществляется для получения свидетельства выполнения некоторого процесса (например контроля посетителей или анализа проекта), оценщику следует выбрать объем информации, достаточный для получения приемлемой уверенности в выполнении процесса.

e) Заявителя и разработчика не следует заблаговременно информировать о точном составе выборки. При этом следует учитывать необходимость обеспечения своевременности поставки выборки и вспомогательных материалов, например комплексов тестовых программ и оборудования оценщику в соответствии с графиком проведения оценки.

f) Следует, чтобы отбор при выборке по возможности был непредвзятым (не стоит выбирать всегда только первый или последний номер в списке). В идеале отбор следует поручить не оценщику, а кому-то другому.

Ошибки, найденные в выборке, могут быть отнесены к двум категориям — систематические или случайные. Если ошибка систематическая, следует устранить ее причину и полностью выполнить новую выборку. При надлежащем объяснении разработчика вопрос о случайных ошибках может быть решен без проведения новой выборки, хотя такое объяснение следует подтвердить. Оценщику следует руководствоваться здравым смыслом при определении, увеличить ли объем выборки или использовать другую выборку.

А.3 Зависимости

В общем случае выполнение требуемых видов и подвидов деятельности и действий по оценке возможно в произвольном порядке или параллельно. Тем не менее, имеются различные виды зависимостей, которые необходимо учитывать оценщику. Этот подраздел представляет общее руководство по учету зависимостей между различными видами и подвидами деятельности и действиями по оценке.

А.3.1 Зависимости между видами деятельности

В некоторых случаях для различных классов доверия может быть рекомендована или даже потребована определенная последовательность выполнения связанных с ними видов деятельности по оценке. Конкретный пример — вид деятельности по оценке ЗБ. Вид деятельности по оценке ЗБ начинается прежде каких-либо видов деятельности по оценке ОО, так как ЗБ предоставляет основу и контекст их выполнения. Однако сделать итоговое заключение по оценке ЗБ до завершения оценки ОО может оказаться невозможным, т. к. результаты деятельности по оценке ОО могут привести к изменениям в ЗБ.

А.3.2 Зависимости между подвидами деятельности

Оценщику необходимо учитывать зависимости между компонентами, указанные в ИСО/МЭК 15408-3. Большинство таких зависимостей являются односторонними, например Подвид деятельности по оценке AVA_VAN.1 зависит от Подвидов деятельности по оценке ADV_FSP.1 и AGD_OPE.1. Есть и примеры взаимной зависимости, когда оба компонента зависят друг от друга, например Подвид деятельности по оценке ATE_FUN.1 и Подвид деятельности по оценке ATE_COV.1.

Обычно положительный вердикт по подвиду деятельности можно принять только при успешном завершении всех тех подвидов деятельности, от которых в одностороннем порядке зависит данный подвид деятельности. Например, как правило, положительный вердикт по Подвидам деятельности по оценке AVA_VAN.1 может быть принят, если только по подвидам деятельности, относящимся к Подвидам деятельности по оценке ADV_FSP.1 и AGD_OPE.1, также принят положительный вердикт. В случае взаимной зависимости порядок выполнения этих компонентов определяет оценщик, принимающий решение о том, какой подвид деятельности осуществить раньше. Следует учесть, что это означает, что положительный вердикт может быть принят только в случае его принятия для обоих зависящих друг от друга подвидов деятельности.

Поэтому при определении того, будет ли некоторый подвид деятельности влиять на другой подвид деятельности, оценщику следует выяснить, зависит ли этот подвид деятельности от потенциальных результатов оценки любых зависимых подвидов деятельности. Действительно, может случиться, что зависимый подвид деятельности сам станет влиять на этот подвид деятельности, требуя выполнить заново ранее завершенные действия.

Существенное влияние приобретают зависимости при обнаружении оценщиком недостатков. Если недостаток идентифицирован в результате проведения одного из подвидов деятельности, то положительный вердикт по зависимому подвиду деятельности может оказаться невозможным до устранения всех недостатков, относящихся к подвиду деятельности, от которого он зависит.

А.3.3 Зависимости между действиями

Может случиться, что результаты, полученные оценщиком во время одного действия, используются при выполнении другого действия. Например, действия по анализу полноты и непротиворечивости не могут быть завершены, пока не завершена проверка содержания и представления свидетельств. Это означает, например что оценщику рекомендуется оценивать обоснование ПЗ/ЗБ после оценки составных частей ПЗ/ЗБ.

А.4 Посещение объектов

А.4.1 Введение

В класс доверия ALC включены требования к:

a) применению управления конфигурацией. Эти требования обеспечивают сохранение целостности ОО;

b) мерам, процедурам и стандартам, касающимся безопасной поставки ОО. Эти требования обеспечивают, что система защиты информации, предоставляемая ОО, не была поставлена под угрозу во время передачи пользователю;

c) мерам безопасности, используемым для защиты среды разработки.

Посещение объектов разработки — полезный способ определения оценщиком, выполняются ли процедуры способом, не противоречащим описанию в документации.

Объекты посещаются для того, чтобы ознакомиться с:

a) использованием системы УК, как описано в плане УК;

b) практическим применением процедур поставки, как описано в документации по поставке;

c) применением мер безопасности во время разработки и поддержания функционирования ОО, как описано в документации по разработке системы безопасности.

Конкретная и подробная информация дается в шагах оценивания для тех действий, когда выполняется посещение объектов:

a) «Возможности УК» (ALC_CMC).n, где n ≥ 3 (особенно в шагах оценивания ALC_CMC.3-10 = ALC_CMC.4-13 = = ALC_CMC.5-19);

b) «Поставка» (ALC_DEL) — особенно в шаге оценивания ALC_DEL.1-2;

c) «Безопасность разработки» (ALC_DVS) — особенно в шагах оценивания ALC_DVS.1-3 = ALC_DVS.2-4.

А.4.2 Общий подход

Во время оценки часто необходимы несколько встреч оценщика с разработчиком, и один из обычных вопросов рационального планирования — совмещение посещений объектов для уменьшения затрат. Например, можно совмещать посещение объектов для проверки управления конфигурацией, безопасности, обеспечиваемой разработчиком, и выполнения поставок. Могут также оказаться необходимыми несколько посещений одного и того же объекта для проверки всех стадий разработки. Следует учесть, что разработка может происходить в нескольких помещениях одного и того же здания, в нескольких зданиях, расположенных на одной территории, или же в нескольких местах.

Первое посещение объекта следует запланировать на ранних стадиях оценки. Для оценки, которая начинается на стадии разработки ОО, это позволит внести, при необходимости, коррективы. Для оценки, проводимой после завершения разработки ОО, раннее посещение даст возможность предпринять меры по исправлению, если в применяемых процедурах будут выявлены серьезные неточности. Это позволит избежать лишних усилий при оценке.

Интервью также является полезным способом определения, отражают ли задокументированные процедуры то, что делается в действительности. При проведении подобных интервью оценщик стремится к получению более глубокого понимания анализируемых процедур на месте разработки, их практического использования и применения в соответствии с представленными свидетельствами оценки. Такие интервью дополняют, но не заменяют исследование свидетельств оценки.

В качестве первого шага при подготовке к посещению объекта, оценщик должен выполнить шаги оценивания относительно класса доверия ALC, исключая аспекты, описывающие результаты посещения. На основании информации, предоставленной в соответствующей документации, полученной от разработчика, и остающихся нерешенными вопросов, на которые в полученной документации нет ответа, оценщики составляют контрольный список вопросов, которые должны быть решены при посещении объекта.

Первая версия отчета об оценке относительно класса ALC и контрольный список вопросов служит в качестве исходной информации для консультации с органом оценки относительно посещения объекта.

Контрольный список служит в качестве руководства при посещении объекта и выступает в виде памятки о том, какие вопросы следует решить путем проведения интервью, а также исследования соответствующих мер и средств, их применения и результатов. Где это представляется целесообразным, для получения необходимого уровня уверенности используется выборка (см. Подраздел А.2).

Результаты посещения объекта документируются и служат исходными данными для окончательной версии отчета об оценке относительно класса доверия ALC.

Следует рассмотреть иные подходы получения уверенности, предоставляющие эквивалентный уровень доверия (например проанализировать свидетельства оценки). Решение об отмене посещения объекта следует принимать после консультации с органом оценки. Приемлемые критерии безопасности и методология должны основываться на других стандартах области систем управления информационной безопасностью.

А.4.3 Примерное руководство по подготовке контрольного листа проверок

Ниже приводятся некоторые ключевые слова и темы, которые должны быть проверены при проведении аудита.

А.4.3.1 Аспекты управления конфигурацией

Базовые аспекты

- Пункты списка конфигурации, включая ОО, исходный код, подключаемые программные библиотеки (библиотеки времени исполнения), проектная документация, средства разработки (ALC_CMC.3-8).
- Прослеживание проектной документации, исходного кода, руководства пользователя к различным версиям ОО.
- Интеграция системы конфигурации в процесс проектирования и разработки, разработки планов испытания, проведения тестовых проверок и процедур управления качеством.

Тестовые проверки

- Прослеживание планов проведения испытаний и результатов тестирования к конкретным настройкам и версиям ОО.
- Управление доступом к системам разработки
- Политики управления доступом и ведения журналов.
- Политики назначения и изменения прав доступа, специфические для данного проекта.
- Перевод ОО в исходное состояние
- Политики перевода ОО в исходное состояние и руководство пользователя, предоставляемое пользователю ОО.
- Политика для тестирования и одобрения компонентов ОО и самого ОО перед развертыванием.

А.4.3.2 Аспекты безопасности разработки

Инфраструктура

- Меры безопасности при организации физического контроля доступа на участок разработки и обоснование эффективности этих мер.

Организационные меры

- Организационная структура компании по отношению к безопасности среды разработки.
- Организационное разделение процессов разработки, производства, тестирования и обеспечения качества.

Меры безопасности, связанные с персоналом

- Меры по обучению персонала аспектам безопасности разработки.
- Меры и юридические соглашения о неразглашении внутренней конфиденциальной информации.

Управление доступом

- Назначение защищаемых объектов (для ОО, исходного кода, подключаемым программным библиотекам (библиотекам времени исполнения), проектной документации, средств разработки, пользовательского руководства) и политик безопасности.
- Политики и обязанности в отношении управления доступом и обработки аутентифицирующей информации.
- Политики занесения в журнал факта любого доступа к участку разработки и защиты данных этих журналов.

Ввод, обработка и вывод данных

- Меры безопасности для защиты устройств ввода/вывода (принтеров, плоттеров и мониторов).
- Обеспечение защиты локальной сети и коммуникаций.

Хранение, передача и уничтожение документов и данных

- Политики обращения с документами и данными.
- Политики и обязанности по уничтожению рассортированных документов и занесение в журнал этих событий.

Защита данных

- Политики и обязанности по защите информации (например по выполнению резервных копий).

План непрерывности бизнес-процессов

- Применяемые действия и обязанности персонала в случае возникновения чрезвычайной ситуации.
- Документация мер управления доступом в условиях чрезвычайной ситуации.
- Информация для персонала о применяемых действиях в условиях чрезвычайной ситуации.

А.4.4 Пример контрольного листа проверки

Примеры контрольных списков проверки при выезде на объект представлены в таблицах для подготовки к аудиту и для представления результатов аудита.

Представленная ниже структура контрольного листа проверки является неокончательным вариантом. В зависимости от конкретного содержания новых руководств может потребоваться внесение изменений в эту структуру.

В контрольном списке выделяют три подраздела согласно темам, обозначенным во Введении (пункт А.4.1 данного приложения):

a) Система управления конфигурацией.

b) Процедуры поставки.

c) Меры безопасность во время разработки.

Эти разделы соответствуют классу ALC актуального ИСО/МЭК 15408, в особенности семействам «Возможности УК» (ALC_CMC).n, где $n \geq 3$, «Поставка» (ALC_DEL) и «Безопасность разработки» (ALC_DVS).

Далее эти подразделы разделяются в ряды, соответствующие шагам оценивания данного стандарта.

Колонки в таблице, которую представляет собой контрольный список, содержат в свою очередь:

- последовательный номер,
- шаг оценивания, на который ссылаются при проверке,
- ссылки на соответствующую документацию разработчика,
- явное воспроизведение мер, предпринятых разработчиком,
- особые примечания и вопросы, которые требуется прояснить во время посещения объекта (помимо стандартной задачи оценщика по проверке применения обозначенных мер),
- результат проверки во время посещения.

Если принято решение о том, что для подготовки к аудиту и для представления результатов проведенного аудита заводятся отдельные контрольные списки, колонка результата проверки в списке для подготовки опускается; соответственно исключается колонка примечаний и вопросов в списке, служащем для представления результатов аудита. Остальные колонки должны быть идентичными в обоих списках.

Таблица А.1. Пример контрольного списка проверки по ОУД 4 (фрагмент)

№	Шаг оценивания	Документация разработчика	Меры	Вопросы и примечания	Результат
А. Проверка системы УК (ALC_CMC.4 и ALC_CMS.4)					
A.1	ALC_CMC.4-11, ALC_CMC.4-12	«Система управления конфигурацией», главы…	Система, автоматически управляющая файлами исходного кода, способна администрировать профили пользователей и права доступа, а также проверять правильность идентификации и аутентификации пользователей	Требуется ли прохождение пользователем процедуры аутентификации при чтении или изменении файлов исходного кода?	Если у пользователя нет прав доступа к конфиденциальному документу, он даже не видит этот документ в списке файлов
B. Проверка процедур поставки (ALC_DEL.1)					
B.1	ALC DEL.1-1, ALC DEL.1-2	«Поставка ОО», главы…	Программное обеспечение передается заказчику с зашифрованной средствами PGP подписью и расшифровывается заказчиком	—	Процесс проверен оценщиками, принято решение, что он правильно описан, кроме того, передается и контрольная сумма
C. Проверка организационной и инфраструктурной безопасности среды разработки (ALC_DVS.1, ALC_LCD.1, ALC_TAT.1)					
C.1	ALC DVS.1-1, ALC DVS.1-2	«Безопасность среды разработки», главы… (Территория)	Территория, на которой ведется разработка, по периметру защищена ограждениями	Достаточно ли прочное и высокое заграждение для того, чтобы предотвратить возможность проникновения на территорию?	Оценщиками принято решение, что ограждение является достаточно прочным и высоким
C.2	ALC DVS.1-1, ALC DVS.1-2	«Безопасность среды разработки», главы… (Здания и сооружения)	Возможны следующие пути доступа в здание: главный вход, где есть проходная (вход закрыт, если на проходной нет сотрудников) и вход через проходную, где осуществляется приемка товара (проход через турникет)	Является ли список возможных путей доступа полным?	Помимо указанных путей доступа в здание, есть также аварийный выход, дверь которого не может быть открыта снаружи. Упомянутые в описании турникеты управляются только изнутри, находящимся на проходной сотрудником

А.5 Сфера ответственности системы оценки

Настоящий стандарт описывает минимальный объем технической работы, которую необходимо выполнить при оценках, проводимых под контролем органов оценки. Тем не менее в нем также указаны (как явно, так и неявно) виды деятельности или методы, на которые не распространяется взаимное признание результатов оценки. Для внесения здесь ясности и в целях уточнения границ, показывающих, где заканчивается настоящий стандарт и где начинается методология конкретной системы оценки, ниже перечислены вопросы, оставленные на усмотрение систем. В конкретной системе оценки возможно как решение всех указанных вопросов, так и оставление некоторых из них неопределенными. (Было сделано все возможное для обеспечения полноты приведенного списка; оценщикам, столкнувшимся с вопросом, не приведенным ниже и не рассмотренным в настоящем стандарте, следует проконсультироваться в своей системе оценки, чтобы выяснить, к чьей компетенции относится решение этого вопроса.)

К вопросам, которые могут определяться в конкретной системе оценки, относятся:

a) требуемое для обеспечения достаточности оценки — каждая система имеет способ (средства) верификации технической компетенции, понимания работы и собственно работы ее оценщиков, либо требуя от оценщиков представления их результатов органу оценки, либо требуя от органа оценки повторения работы оценщика, или ещё каким-либо способом, обеспечивающим, что все органы оценки выполняют работу приемлемым образом и выдают сопоставимые результаты;

b) процесс распоряжения свидетельствами оценки после завершения оценки;

c) требования по конфиденциальности (как со стороны оценщика, так и относительно неразглашения информации, полученной в процессе оценки);

d) действия, предпринимаемые при возникновении проблем в процессе оценки (после решения проблемы процесс оценки либо возобновляется, либо немедленно прекращается и исправленный продукт необходимо заново представить для оценки);

e) конкретный (естественный) язык, на котором необходимо представить документацию;

f) документальные свидетельства, которые необходимо представить в составе ТОО; настоящий стандарт определяет минимум, который следует привести в ТОО, а в конкретных системах оценки возможно требование включения дополнительной информации;

g) дополнительные отчеты (помимо ТОО), требуемые от оценщиков, например отчеты о тестировании;

h) любые специфические СП, которые могут потребоваться в соответствии с системой, включая структуру, получателей и т.д. для таких СП;

i) структура конкретного содержания документальных сообщений (отчетов), разрабатываемых при оценке ЗБ, — система оценки может иметь установленный формат для всех сообщений (отчетов), детализирующих результаты оценки, будь это оценка ОО или ЗБ;

j) любая требуемая дополнительно информация по идентификации ПЗ/ЗБ;

k) любые виды деятельности по принятию решения о пригодности сформулированных в явном виде требований в ЗБ;

l) любые требования по подготовке свидетельства оценщика для поддержки переоценки и повторного применения свидетельств;

m) любые конкретные способы применения идентификаторов, эмблем, торговых марок и т.д. системы оценки;

n) любые конкретные указания по применению криптографии;

o) способы трактовки и применения системы оценки, национальных и международных интерпретаций;

p) перечень или описание приемлемых альтернатив тестированию там, где тестирование неосуществимо;

q) механизм, посредством которого орган оценки может определить, какие шаги оценщик предпринял при тестировании;

r) предпочтительный подход при тестировании (если таковой имеется): на внутреннем интерфейсе или на внешнем интерфейсе;

s) перечень или характеристика приемлемых способов (средств) проведения оценщиком анализа уязвимостей (например методология гипотез о недостатках);

t) информация относительно любых уязвимостей и недостатков, которые необходимо принимать во внимание.

Приложение В
(информативное)

Оценка уязвимостей (AVA)

В данном приложении приводится объяснение критериев AVA_VAN, а также рассматриваются примеры их использования. В данном приложении не определяются собственно критерии AVA; это определение представлено в разделе ИСО/МЭК 15408-3 класс «AVA: Оценка уязвимостей».

Данное приложение состоит из двух основных частей:

a) *Руководство по завершению независимого анализа уязвимостей*. Краткое описание приводится в подразделе В.1, а более подробное — в подразделе В.2. Эти подразделы описывают, каким образом оценщик должен подходить к проведению независимого анализа уязвимости.

b) Руководство по тому, каким образом характеризовать и использовать предполагаемый потенциал нападения нарушителя. Описание этого вопроса приводится в подразделах В.3 — В.5. В этих подразделах приводится пример описания того, каким образом можно охарактеризовать потенциал нападения и как его можно использовать, а также приводятся примеры использования.

В.1 Что представляет собой анализ уязвимостей

Цель деятельности по оценке уязвимостей состоит в том, чтобы сделать заключение о наличии недостатков и уязвимостей ОО в среде его функционирования, а также о возможности использования этих уязвимостей. Вынесение данного заключение основывается на результатах анализа, выполненного оценщиком, и поддерживается тестированием, проведенным оценщиком.

На самых низких уровнях доверия семейства «Анализа уязвимостей» (AVA_VAN) оценщик просто изучает общедоступную информацию в целях идентификации любых известных недостатков и слабостей ОО, в то время как на более высоких уровнях доверия оценщик выполняет структурированный анализ свидетельств оценки ОО.

При выполнении анализа уязвимостей имеют значение три основных фактора, а именно:

a) идентификация потенциальных уязвимостей;

b) оценка в целях вынесения заключения о том, могут ли идентифицированные потенциальные уязвимости позволить нарушителю с соответствующим потенциалом нападения привести к нарушению ФТБ;

c) тестирование проникновения в целях вынесения заключения о том, могут ли идентифицированные уязвимости данного ОО в его среде функционирования быть использованы нарушителем.

Может быть проведена дальнейшая декомпозиция идентификации уязвимостей до конкретных свидетельств, которые нужно отыскать (и до определения того, насколько тщательно должен проводиться подобный поиск) в целях идентификации потенциальных уязвимостей. Подобным образом и тестирование проникновения может быть разложено на составные компоненты — анализ потенциальных уязвимостей в целях определения методов атаки и демонстрацию методов и способов атакующего воздействия.

Эти основные факторы деятельности по природе своей являются итерационными, то есть тестирование проникновения для потенциальных уязвимостей может привести к идентификации других потенциальных уязвимостей. По этой причине они выполняются как единый вид деятельности по анализу.

В.2 Структура анализа уязвимости, проводимого оценщиком

Анализ уязвимости проводится оценщиком в целях вынесения заключения о том, является ли ОО способным противостоять атакам проникновения, выполняемым нарушителем с базовым (для AVA_VAN.1 и AVA_VAN.2), усиленным базовым (для AVA_VAN.3), умеренным (для AVA_VAN.4) или высоким (для AVA_VAN.5) потенциалом нападения. Оценщик сначала оценивает степень возможности использования всех выявленных потенциальных уязвимостей. Это достигается путем проведения тестирования проникновения. Оценщик должен при попытке осуществить проникновение к ОО принимать на себя роль нарушителя с соответственно базовым (для AVA_VAN.1 и AVA_VAN.2), усиленным базовым (для AVA_VAN.3), умеренным (для AVA_VAN.4) или высоким (для AVA_VAN.5) потенциалом нападения.

Оценщик рассматривает все потенциальные уязвимости, которые обнаруживает оценщик во время поведения других действий оценивания. Тестирование проникновения, проводимое оценщиком в целях вынесения заключения о способности ОО противостоять атакам, направленным на эти потенциальные уязвимости, должно выполняться с применением на себя ролей нарушителя с базовым (для AVA_VAN.1 и AVA_VAN.2), усиленным базовым (для AVA_VAN.3), умеренным (для AVA_VAN.4) или высоким (для AVA_VAN.5) потенциалом нападения.

Однако анализ уязвимостей не следует проводить как отдельное действие. Он тесно связан с ADV и AGD. Оценщик выполняет эти другие действия по оцениванию, уделяя особое внимание вопросам идентификации потенциальных уязвимостей или «проблемных областей». Поэтому требуется знакомство оценщика с общим руководством по уязвимостям (приведенном в пункте В.2.1).

В.2.1 Общее руководство по уязвимостям

В приведенных ниже пяти категориях приводится обсуждение общих уязвимостей.

B.2.1.1 Обход мер безопасности

Обход включает любой способ, посредством которого нарушитель мог бы избежать осуществления мер безопасности путем:

a) использования возможностей интерфейсов ОО или утилит, которые могут взаимодействовать с ОО;

b) наследования привилегий или других возможностей, которые следовало бы наоборот запретить;

c) (когда важна конфиденциальность) чтения чувствительных данных, сохраненных или скопированных в недостаточно защищенные области.

В ходе независимого анализа уязвимостей, выполняемого оценщиком, следует рассмотреть (когда это уместно) каждый из следующих аспектов:

a) Нападения, основанные на использовании возможностей интерфейсов или утилит, обычно используют в своих целях отсутствие требуемых мер безопасности для этих интерфейсов. Например, получение доступа к функциональным возможностям, которые реализованы на более низком уровне, чем тот, на котором осуществляется управление доступом. Возможные варианты включают:

1) изменение предопределенной последовательности вызова функций;

2) выполнение дополнительной функции;

3) использование некоторого компонента в непредусмотренном контексте или с непредусмотренной целью;

4) использование подробностей реализации, представленных в менее абстрактных представлениях;

5) использование задержки между временем проверки доступа и временем использования.

b) Изменение предопределенной последовательности вызова компонентов следует рассматривать, когда имеется предусмотренный порядок вызова интерфейсов ОО (например команд пользователя) для выполнения некоторой функции безопасности (например открытия файла для доступа и затем чтения данных из него). Если функция безопасности вызывается на одном из интерфейсов ОО (например проверка управления доступом), то оценщику следует рассмотреть, возможен ли обход функции безопасности путем выполнения соответствующего вызова в более поздней точке последовательности или пропуска ее целиком.

c) Выполнение дополнительного компонента (в предопределенной последовательности) является формой нападения, похожей на только что описанную, но включает вызов некоторого другого интерфейса ОО в некоторой точке последовательности. Оно может также включать нападения, основанные на перехвате передаваемых по сети чувствительных данных путем использования анализаторов сетевого трафика (дополнительным компонентом здесь является анализатор сетевого трафика).

d) Использование некоторого компонента в непредусмотренном контексте или с непредусмотренной целью включает использование для обхода функции безопасности не относящегося к делу интерфейса ОО, используя его для достижения цели, которая для него не планировалась или не предполагалась. Скрытые каналы являются примером этого типа нападения. Использование недокументированных интерфейсов (которые могут быть небезопасными) также попадает в эту категорию (включая недокументированные возможности по поддержке и помощи).

e) Использование подробностей реализации, приведенных в менее абстрактных представлениях, опять включает использование скрытых каналов, через которые нарушитель использует в своих целях дополнительные функциональные возможности, ресурсы или атрибуты, представленные в ОО как последствия процесса усовершенствования (например использование переменной, обеспечивающей блокировку, в качестве скрытого канала). Дополнительные функциональные возможности также могут обеспечиваться тестовыми фрагментами кода, содержащимися в программных модулях ОО.

f) Использование задержки между временем проверки доступа и временем использования включает сценарии, в которых выполняется проверка управления доступом и предоставляется доступ, а нарушитель впоследствии способен создать условия, при которых во время выполнения проверки доступа мог бы произойти сбой проверки доступа. Примером является пользователь, порождающий фоновый процесс для чтения и отправки высокочувствительных данных на терминал пользователя и затем осуществляющий выход из системы и повторный вход в систему на более низком уровне чувствительности. Если фоновый процесс не завершается при выходе пользователя из системы, то проверки в соответствии с мандатным управлением доступом могут быть фактически обойдены.

g) Нападения, основанные на наследовании привилегий, в основном базируются на незаконном приобретении привилегий или возможностей некоторого привилегированного компонента обычно путем выхода из него неконтролируемым или непредусмотренным способом. Возможные варианты включают:

1) выполнение данных, не предназначенных для выполнения или преобразование их в возможные для выполнения;

2) генерацию непредусмотренных исходных данных для некоторого компонента;

3) нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня.

h) Выполнение данных, не предназначенных для выполнения или преобразование их в возможные для выполнения, включает нападения с использованием вирусов (например помещение в некоторый файл выполняемого кода или команд, которые автоматизировано выполняются при редактировании данного файла или получении доступа к нему, наследуя, таким образом, привилегии, которые имеет владелец файла).

i) Генерация непредусмотренных исходных данных для некоторого компонента может приводить к непредусмотренным результатам, которыми может воспользоваться нарушитель. Например, если ОО является приложением, реализующим функции безопасности, которые можно обойти при получении пользователем доступа к базовой операционной системе, то может оказаться возможным получить такой доступ сразу после выполнения входной последовательности, исследуя, пока пароль аутентифицируется, результаты ввода различных управляющих или escape-последовательностей.

j) Нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня, включает нападения, основанные на выходе из-под действия ограничений приложения для получения доступа к базовой операционной системе, чтобы обойти функции безопасности, реализуемые приложением. В этом случае предположение, которое нарушается, состоит в том, что для пользователя приложения невозможно получить такой доступ. Подобное нападение можно предвидеть, если функции безопасности реализуются приложением, работающим под управлением системы управления базами данных: опять же есть возможность обхода функций безопасности, если нарушитель сможет выйти из-под действия ограничений приложения.

k) Нападения, основанные на чтении чувствительных данных, сохраненных в недостаточно защищенных областях (применимо, когда важна конфиденциальность), включают следующие вопросы, которые следует рассматривать как возможные способы получения доступа к чувствительным данным:

1) сбор «мусора» на диске;

2) доступ к незащищенной памяти;

3) использование доступа к совместно используемым по записи файлам или другим совместно используемым ресурсам (например к файлам подкачки);

4) Активация восстановления после ошибок, чтобы определить, какой доступ могут получить пользователи. Например, после отказа автоматическая система восстановления файлов для файлов без заголовков может использовать каталог для потерянных и найденных файлов, которые присутствуют на диске без меток. Если ОО реализует мандатное управление доступом, то важно исследовать, какой уровень безопасности поддерживается для этого каталога (например наивысший для системы) и кто имеет доступ к этому каталогу.

Существует множество различных методов, использование которых позволяет оценщику идентифицировать программу скрытого удаленного администрирования (так называемый «бэкдор», backdoor), среди них выделяют два основных. Во-первых, оценщик может случайно выявить во время тестирования интерфейс, для которого есть возможность неправильного использования. Во-вторых, можно провести тестирование каждого из внешних интерфейсов ФБО в режиме отладки кода, чтобы идентифицировать любые модули, которые не являются вызванными как часть тестирования документированных интерфейсов, а затем провести анализ этого невызываемого участка программного кода в целях вынесения заключения о том, является ли он внедренной программой удаленного администрирования («бэкдором»).

В случае, когда объектом оценки является программное обеспечение, где «Подвид деятельности по оценке» ADV_IMP.2 и «Подвид деятельности по оценке» ALC_TAT.2 или компоненты более высокого уровня включаются в пакет доверия, оценщик может во время проведения анализа инструментов разработки рассмотреть программные библиотеки и пакеты, которые связаны между собой программой-компилятором на стадии компиляции, чтобы сделать заключение о том, что на данной стадии не были выявлены «бэкдоры».

B.2.1.2 Вмешательство

Вмешательство включает любое нападение, основанное на попытке нарушителя повлиять на режим выполнения функции безопасности или механизма (т. е. исказить или блокировать выполнение), например путем:

a) доступа к данным, на конфиденциальность или целостность которых полагается функция или механизм безопасности;

b) вынуждения ОО функционировать в необычных или непредусмотренных условиях;

c) отключения или задержки обеспечения безопасности

d) физического изменения ОО.

В ходе независимого анализа уязвимостей оценщику следует рассмотреть (когда это уместно) каждый из следующих аспектов:

a) Нападения, основанные на доступе к данным, на конфиденциальность или целостность которых полагается функция или механизм безопасности, включают:

1) чтение, запись или модификацию внутренних данных прямо или косвенно;

2) использование некоторого компонента в непредусмотренном контексте или с непредусмотренной целью;

3) использование взаимного влияния компонентов, которые невидимы на более высоком уровне абстракции.

b) Чтение, запись или модификация внутренних данных прямо или косвенно охватывают следующие типы нападений, которые следует рассмотреть:

1) чтение «секретов», хранимых внутри ОО, таких как пароли пользователей;

2) подмена внутренних данных, на которые полагаются механизмы, обеспечивающие безопасность;

3) изменение переменных среды (например логических имен) или данных в файлах конфигурации или временных файлах.

c) Может оказаться возможным обмануть доверенный процесс для модификации защищенного файла, к которому этот процесс штатно не должен обращаться.

d) Оценщику следует также рассмотреть следующие «опасные характеристики»:

1) исходный код вместе с компилятором, постоянно имеющиеся в наличии в ОО (например может оказаться возможным изменение исходного кода, связанного с входом в систему);

2) интерактивный отладчик и средства внесения изменений (например может оказаться возможным изменение исполняемого образа);

3) возможность внесения изменений на уровне контроллеров устройств, на котором файловой защиты не существует;

4) диагностический код, который присутствует в исходном коде и может быть опционально включен;

5) инструментальные средства разработчика, оставленные в ОО.

e) Использование некоторого компонента в непредусмотренном контексте или с непредусмотренной целью включает, например случай, когда ОО является приложением, полагающимся на операционную систему, а пользователи используют знания пакета текстового процессора или другого редактора, чтобы изменить свой собственный командный файл (например чтобы приобрести большие привилегии).

f) Использование взаимного влияния компонентов, которое невидимо на более высоком уровне абстракции, включает нападения, использующие совместный доступ к ресурсам, когда модификация ресурса одним компонентом может влиять на режим выполнения другого (доверенного) компонента, например на уровне исходного кода, через использование глобальных данных или косвенных механизмов, таких как совместно используемая память или семафоры.

g) Следует всегда учитывать нападения, основанные на принуждении ОО функционировать в необычных или непредусмотренных обстоятельствах. Возможные варианты включают:

1) генерацию непредусмотренных исходных данных для некоторого компонента;

2) нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня.

h) Генерация непредусмотренных исходных данных для компонента включает исследование режима функционирования ОО, когда имеет место:

1) переполнение буферов ввода команд (возможно «разрушение стека» или перезапись другой области хранения, которыми нарушитель может быть способен воспользоваться в своих интересах, или принудительная выдача аварийного дампа, который может содержать чувствительную информацию, такую как открытый текст паролей);

2) ввод неправильных команд или параметров (включая установку параметра в состояние «только для чтения» для интерфейса, который предполагает выдачу данных через этот параметр);

3) вставка маркера конца файла (например CTRL/Z или CTRL/D) или нулевого символа в журнал аудита.

i) Нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня, включает нападения, использующие ошибки в исходном коде, где предполагается (явно или неявно), что относящиеся к безопасности данные находятся в конкретном формате или имеют конкретный диапазон значений. В таких случаях оценщику следует формируя данные в другом формате или присваивая им другие значения, сделать заключение, могут ли нападения привести к нарушению таких предположений и, если это так, может ли это предоставить преимущества нарушителю.

j) Корректный режим выполнения функций безопасности может зависеть от предположений, которые нарушаются в критических обстоятельствах, когда исчерпываются лимиты ресурсов или параметры достигают своего максимального значения. Оценщику следует рассмотреть (если это целесообразно) режим функционирования ОО, когда эти пределы достигаются, например:

1) изменение дат (например исследования, как ведет себя ОО при переходе датой критического порога);

2) переполнение дисков;

3) превышение максимального числа пользователей;

4) заполнение журнала аудита;

5) переполнение очередей сигналов безопасности, выдаваемых на консоль;

6) перегрузка различных частей многопользовательского ОО, который сильно зависит от компонентов связи;

7) забивание сети или отдельных хостов трафиком;

8) заполнение буферов или полей.

k) Нападения, основанные на отключении или задержке обеспечения безопасности, включают следующие аспекты:

1) использование прерываний или функций составления расписаний, чтобы нарушить последовательное выполнение операций;

2) нарушения при параллельном выполнении;

3) использование взаимного влияния между компонентами, которое невидимо на более высоком уровне абстракции.

l) Использование прерываний или функций составления расписаний, чтобы нарушить последовательность выполнения операций, включает исследование режима функционирования ОО при:

1) прерывании команды (по CTRL/C, CTRL/Y и т. п.);

2) порождении второго прерывания до того, как будет распознано первое.

m) Необходимо исследовать результаты завершения процессов, критических для безопасности (например выполнения в фоновом режиме программы аудита). Аналогично может оказаться возможной такая задержка регистрации записей аудита или выдачи/получения предупреждающих сигналов, что они становятся бесполезными для администратора (так как нападение может уже достичь цели).

n) Нарушения при параллельном выполнении включают исследование режима функционирования ОО, когда два или более субъектов предпринимают попытку одновременного доступа. Возможно, ОО и сможет справиться с блокировкой, необходимой, когда два субъекта предпринимают попытку одновременного доступа, но при этом его поведение станет не полностью определенным при наличии дополнительных субъектов. Например, критичный по безопасности процесс может быть переведен в состояние ожидания получения ресурса, если два других процесса осуществляют доступ к ресурсу, который ему требуется.

o) Использование взаимного влияния компонентов, которое невидимо на более высоком уровне абстракции, может обеспечить способ задержки критического по времени доверенного процесса.

p) Среди физических нападений могут быть выделены следующие категории: физическое зондирование (сканирование), физическая манипуляция, физическая модификация и подмена.

1) Физическое сканирование заключается в проникновении и получении доступа к внутренним целевым качествам ОО, например в считывании внешних интерфейсов, данных шин или областей памяти.

2) Физическая манипуляция может быть осуществлена над внутренними частями ОО и нацелена на внутренние искажения ОО (например путем использования в качестве процесса взаимодействия оптического индуцирования сбоев), на внешние интерфейсы компонентов ОО (например путем организации сбоев энергоснабжения или настроек времени), на среду функционирования ОО (например путем изменения температуры).

3) Физическая модификация — изменение осуществляющих безопасность атрибутов внутренних качеств ОО в целях предоставления им привилегий или других характеристик, которые не допускаются в обычном режиме функционирования. Такие изменения могут быть вызваны, например оптическим индуцированием сбоев. Нападения, основанные на физической модификации, могут также привести к изменениям в самих ФБО, вызывая ошибки передачи данных внутренних программ перед их выполнением. Следует отметить, что такой вид обхода, при котором вносятся изменения в сами ФБО, подвергает опасности все ФБО в целом, особенно в случае отсутствия иных мер и средств (например защиты среды), которые препятствуют получению нарушителем физического доступа к ОО.

4) Физическая подмена, когда ОО заменяется другой сущностью ИТ, осуществляется во время поставки или работы с ОО. Возможность подмены во время передачи ОО из среды проектирования пользователю должна быть предотвращена путем применения безопасных процедур поставки (таких, как рассмотренные в семействе ALC_DVS «Безопасность разработки»). Подмену ОО во время его работы можно предотвратить комбинацией мер — соблюдением требований руководства пользователя по эксплуатации и внедрением мер и средств защиты среды функционирования таким образом, чтобы пользователь был уверен в том, что взаимодействует именно с данным ОО.

B.2.1.3 Прямые нападения

Прямое нападение включает идентификацию любых тестов проникновения, необходимых для подтверждения или опровержения стойкости перестановочных, вероятностных и других механизмов функций безопасности в случае прямого нападения.

Например, может быть неверным предположение, что конкретная реализация генератора псевдослучайных чисел будет обладать требуемой энтропией, необходимой для задания начального числа при генерации псевдослучайных чисел механизма безопасности.

В тех случаях, когда вероятностный или перестановочный механизм полагается на выбор значения атрибута безопасности (например выбор длины пароля) или ввод данных человеком-пользователем (например выбор пароля), в сделанных предположениях должны быть отражены худшие случаи из возможных.

Вероятностные или перестановочные механизмы должны быть идентифицированы во время исследования свидетельств оценки, требуемых в качестве исходных данных к определенному подвиду деятельности (ЗБ, функциональная спецификация, подмножество проекта ОО и представления реализации), кроме того, любая другая документация по ОО (например руководство) может содержать идентификацию дополнительных вероятностных или перестановочных механизмов.

В тех случаях, когда проектные свидетельства или представленные в руководствах включают утверждения или предположения (например о том, сколько попыток аутентификации возможно произвести за минуту), оценщик должен путем независимого тестирования или анализа подтвердить, что эти предположения являются правильными.

Прямые нападения, направленные на уязвимости алгоритма шифрования, нельзя рассматривать в рамках семейства «Анализ уязвимостей» (AVA_VAN), поскольку это выходит за рамки ИСО/МЭК 15408. Правильность реализации алгоритма шифрования рассматривают во время действий по оценке ADV и ATE.

B.2.1.4 Мониторинг

Информация — абстрактное представление отношений между свойствами сущностей, то есть сигнал содержит информацию для системы, если ОО в состоянии реагировать на данный сигнал. Ресурсы ОО обрабатывают и хранят информацию, представленную пользовательскими данными. Таким образом:

- информация с пользовательскими данными может циркулировать между субъектами по внутренним каналам ОО или экспортироваться из ОО;
- информация может быть сгенерирована и передана к другим пользовательским данным;
- информация может быть получена посредством мониторинга операций над данными, представляющими информацию.

Информация, представленная пользовательскими данными для осуществления контроля действий над данными, может быть охарактеризована таким атрибутом безопасности, как например «степень секретности», который может принимать значения: несекретная информация, конфиденциальная информация, секретная, совершенно секретная. Эта информация и, соответственно, этот признак безопасности могут быть изменены в результате проведения некоторых операций, например в FDP_ACC.2 может быть описано уменьшение уровня требований к сокрытию информации или усиление уровня путем комбинирования данных. Это один из аспектов анализа информационных потоков, который направлен на анализ контролируемых операций контролируемых субъектов над контролируемыми объектами.

Другой аспект — анализ несанкционированных потоков информации. Этот аспект является более общим, чем прямой доступ к объектам, содержащим пользовательские данные, к которым обращается семейство FDP_ACC. *Ненавязанные* каналы связи, по которым информация передается под контролем политики контроля информационных потоков, могут быть вызваны мониторингом обработки информации на объекте, содержащем информацию, или так или иначе связанном с этой информацией (например атака по сторонним каналам). *Навязан-*

ные каналы связи можно идентифицировать с точки зрения ресурсов, оказывающих целенаправленное влияние на субъекты, а также по тому фактору, что субъект или пользователь может наблюдать такое влияние. Классически, скрытые каналы идентифицируют либо как каналы памяти, либо как каналы времени, в зависимости от того, подвергался ли ресурс модификации или модуляции. Что касается других атак, связанных с мониторингом, использование ОО должно осуществляться в соответствии с ФТБ.

Скрытые каналы обычно применимы в том случае, когда у ОО есть требования политики скрытности и многоуровневого разделения. Скрытые каналы обычно определяются во время действий по анализу уязвимостей и самого проекта и поэтому должны быть протестированы. Однако обычно такие атаки мониторинга выявляются специальными аналитическими методами, так называемыми методами «анализа скрытых каналов». Эти методы были предметом серьезных исследований, по данному вопросу опубликовано множество работ. Руководство по проведению анализа скрытых каналов должно быть получено от органа оценки.

Атаки мониторинга *ненавязанных* информационных потоков включают в себя методы пассивного анализа, направленные на раскрытие чувствительных внутренних данных ОО путем такого управления ОО, которое не противоречит положениям руководств.

Анализ сторонних каналов включает методы криптоанализа, основанные на утечке информации от ОО по физическому каналу. Такая утечка по физическому каналу может произойти в результате сбора информации, касающейся времени задержки сигнала, уровня потребления энергии или её излучения во время обработки вычислений ФБО. Информация по поводу времени задержки сигнала может быть получена нарушителем удалённо (при условии, что у него есть сетевой доступ к ОО); каналы утечки, связанные с энергетическими каналами и подключением к сети электропитания, требуют для реализации, чтобы нарушитель находился в непосредственной близости от места расположения ОО.

Методы подслушивания включают в себя и перехват любых форм энергии, например электромагнитного или оптического излучения дисплеев компьютеров. При этом не обязательно, чтобы нарушитель находился в непосредственной близости от места расположения ОО.

К мониторингу же относится и использование недостатков протоколов, например атака на реализацию протокола SSL.

B.2.1.5 Неправильное применение

Неправильное применение может явиться результатом:

a) неполноты руководств;

b) необоснованности положений руководств;

c) непреднамеренной неверной настройки ОО;

d) вынужденного нестандартного режима функционирования ОО.

Если документация руководств является неполной, пользователь может не знать, каким образом работать с ОО в соответствии с ФТБ. Оценщик должен использовать своё хорошее знание ОО, полученное в ходе выполнения других действий оценки, чтобы вынести заключение о том, что руководство является полным. В частности, оценщик должен рассмотреть функциональную спецификацию. ФБО, описанные в этом документе, должны быть описаны в руководстве согласно требованиям, для разрешения безопасного администрирования и использования через доступные пользователям ИФБО. Кроме того, следует рассмотреть различные режимы работы, чтобы удостовериться, что руководство охватывает все режимы функционирования.

Оценщик может, в рамках оказания содействия, подготовить неформальное отображение соответствия между руководством и этими документами. Любые пропуски в данном отображении соответствия могут указать на неполноту.

Руководство, как полагают, является необоснованным, если в нём выдвинуты требования по использованию ОО или среды его функционирования, которые не согласуются с ЗБ или излишне обременительны для поддержания безопасности.

В ОО может быть множество способов, которые помогают пользователю эффективно использовать данный ОО в соответствии с ФТБ и предотвратить непреднамеренную неверную настройку ОО. В ОО могут быть использованы функции (свойства) уведомления пользователя о том, что ОО находится в состоянии, несоответствующем ФТБ. ОО могут быть поставлены вместе с дополнительным руководством, содержащим предложения, подсказки, процедуры и т.д., по максимально эффективному использованию существующих механизмов безопасности; например руководство по использованию функции аудита для помощи в обнаружении угрозы невыполнения ФТБ; а именно для выявления незащищенного состояния.

Оценщик рассматривает функциональные возможности ОО, его назначение и ЗБ среды функционирования для того, чтобы прийти к выводу, возможно ли обоснованное ожидание того, что при выполнении положений руководства переход в потенциально опасное состояние ОО будет своевременно обнаружен.

Потенциальную возможность перехода ОО в незащищенное состояние можно определить при помощи полученной для оценки документации, такой как ЗБ, функциональная спецификация и любые другие проектные представления, предоставленные в качестве свидетельств компонентов, включенных в пакет доверия для ОО (например спецификация проекта ОО/ФБО, если при этом в пакет включен компонент семейства ADV_TDS «Проект ОО»).

Случаи вынужденного нестандартного режима функционирования ФБО могут включать в себя следующее (и не только):

a) режим функционирования ОО при активизации процедур запуска, завершения работы или восстановления после ошибки;

b) режим функционирования ОО в экстремальных условиях (иногда называемый режимом перегрузки или асимптотическим режимом функционирования), особенно в случаях, когда это может привести к деактивации или выведению из строя частей ФБО;

c) любая возможность непреднамеренной неверной настройки или использования незащищенным образом, являющаяся результатом нападений, отмеченных в пункте «Вмешательство», приведенном выше.

B.2.2 Идентификация потенциальных уязвимостей

Потенциальные уязвимости могут быть идентифицированы оценщиком во время различных действий. Они могут быть выявлены во время деятельности по оценке или в результате анализа свидетельств, проводимого в целях поиска уязвимостей.

B.2.2.1 Выявленные уязвимости

Идентификация уязвимостей, которые обнаружил оценщик при проведении оценивания, — это тот случай, когда потенциальные уязвимости идентифицированы оценщиком непосредственно во время проведения действий оценки, то есть не производится анализ свидетельств с конкретной целью идентификации потенциальных уязвимостей.

Такой метод непосредственного выявления сильно зависит от опыта и знаний оценщика; эти вопросы контролирует орган оценки. В методике это не воспроизводимо, но документируется в целях обеспечения воспроизводимости заключений и выводов относительно потенциальных уязвимостей, которые приводит в отчете оценщик.

Не существует формальных аналитических критериев, требуемых для данного метода. Потенциальные уязвимости идентифицируются по свидетельствам, полученным на основании знаний и опыта оценщика. Однако данный метод идентификации не ограничивается каким-либо подмножеством свидетельств.

Предполагается, что оценщик обладает знанием о типе технологии, использованной в ОО, и известных уязвимостей, находящихся в открытом доступе. Предполагаемый уровень знаний — знания, получаемые из почтовой рассылки по вопросам безопасности данного типа ОО, бюллетеней (по ошибкам, уязвимостям и спискам недостатков безопасности), регулярно издаваемых организациями, исследующими вопросы безопасности продуктов и технологий, находящихся в широком использовании. Вовсе не обязательно, что оценщик по AVA_VAN.1 или AVA_VAN.2 знает также и результаты слушаний конференций или детализированные тезисы, произведенные университетскими исследованиями. Однако, для того, чтобы удостовериться, что применяемые при оценке знания не устарели, оценщику может потребоваться провести поиск материалов, находящихся в открытом доступе, в целях определения актуальности имеющихся знаний.

Для компонентов от AVA_VAN.3 до AVA_VAN.5 поиск оценщиком информации, находящейся в открытом доступе, как ожидается, будет включать в себя и результаты слушаний конференций и детализированные тезисы университетских исследований, а также исследований, проведенных другими соответствующими организациями.

Примеры того, каким образом могут быть выявлены уязвимости (каким образом оценщик может их обнаружить):

a) в ходе исследования оценщиком некоторых свидетельств он вспоминает о потенциальной уязвимости, которая была когда-то идентифицирована для продукта подобного типа, и предполагает, что и в оцениваемом ОО данная уязвимость также имеет место;

b) исследуя некоторые свидетельства, оценщик определяет недостаток спецификации интерфейса, который отражает потенциальную уязвимость.

О потенциальной уязвимости ОО оценщик может узнать, прочитав о типовых уязвимостях данного конкретного типа продукции ИТ в публикациях по безопасности или в рассылке электронных писем по безопасности, на которую подписан оценщик.

Методы нападения могут быть напрямую развиты на основе потенциальных уязвимостей. Поэтому потенциальные уязвимости, которые обнаруживает оценщик, подробно рассматриваются во время осуществления тестов проникновения, основывающихся на результатах анализа уязвимостей, проведенного оценщиком. Не представляется возможным установить явно некое действие, которое однозначно позволит оценщику выявить потенциальную уязвимость. Поэтому оценщик руководствуется подразумеваемыми действиями, которые описаны в AVA_VAN.1.2E и AVA_VAN.*.4E.

Текущая информация относительно типовых уязвимостей и атак, информация о которых имеется в открытом доступе, может быть предоставлена оценщику, например органом оценки. Эта информация должна быть принята во внимание оценщиком при сопоставлении выявленных уязвимостей и методов нападения, выполняемом при подготовке к тестированию проникновения.

B.2.2.2 Виды анализа

Следующие типы анализа представлены в рамках действий оценщика.

B.2.2.2.1 Неструктурированный анализ

Данный тип действий по анализу, осуществляемых оценщиком (для Подвида деятельности по оценке AVA_VAN.2) позволяет оценщику рассмотреть типовые уязвимости (как рассматривалось в B.2.1). Оценщик также применяет свой опыт и знания уязвимостей схожих технологических продуктов.

B.2.2.2.2 Фокусированный анализ

Во время проведения действий оценивания оценщик может также идентифицировать проблемные области. К ним относятся определенные части свидетельств ОО, которые хотя формально и соответствуют требованиям деятельности, с которой связано данное свидетельство, но у оценщика есть к ним некоторые замечания. Например, конкретная спецификация интерфейса представляется особенно сложной, и поэтому может вызвать ошибку или при разработке ОО, или при функционировании ОО. На данном этапе нет явной потенциальной уязвимости, поэтому требуется дальнейшее исследование, что означает, что такой анализ находится вне области выявленных уязвимостей, т. е. таких, которые обнаруживает оценщик при проведении действий по оценке.

Разница между потенциальной уязвимостью и проблемной областью заключается в следующем:

a) Потенциальная уязвимость — оценщику известен метод нападения, который может использовать недостаток или слабость защиты ОО, или оценщику известна информация об уязвимости, которая имеет отношение к данному ОО.

b) Проблемная область — оценщик может не рассматривать проблемную область как потенциальную уязвимость, основываясь на информации, полученной из других источников. При чтении спецификации интерфейса оценщик идентифицирует, что из-за чрезвычайной (нецелесообразной) сложности интерфейса в этой области может быть потенциальная уязвимость, хотя это и не было явно выявлено на этапе начального исследования.

Фокусированный подход к идентификации уязвимостей — анализ свидетельств в целях идентификации любых потенциальных уязвимостей, которые становятся очевидны при изучении содержащейся в свидетельствах информации. Такой анализ является неструктурированным, поскольку методика проведения не предопределена. Этот подход к идентификации потенциальных уязвимостей может использоваться во время независимого анализа уязвимостей, требуемого «Подвидом деятельности по оценке» (AVA_VAN.3).

Такой анализ может быть проведен с использованием различных подходов, которые приведут к соразмерным уровням уверенности. При этом ни один из подходов строго не определяет формат проведения исследования свидетельств.

Выбранный подход руководствуется результатами оценки свидетельств, проведенной оценщиком в целях вынесения заключения о том, что данные свидетельства удовлетворяют требованиям подвидов деятельности AVA/AGD. Поэтому исследование свидетельств наличия потенциальных уязвимостей может руководствоваться следующими факторами:

a) проблемные области идентифицированы во время исследования свидетельств при проведении действий по оценке;

b) уверенность в некой функции, обеспечивающей разделение, идентифицированное во время анализа проекта архитектуры (в «Оценке подвида деятельности» (ADV_ARC.1)) и требующее, чтобы в ходе дальнейшего анализа была определена невозможность обхода данной функции;

c) исследование представления свидетельств, чтобы выдвинуть гипотезу о потенциальных уязвимостях ОО.

Оценщик приводит в отчете информацию о том, какие меры были приняты для идентификации потенциальных уязвимостей в свидетельствах. Однако оценщик может быть не в состоянии описать последовательные шаги идентификации потенциальных уязвимостей перед началом исследования. Подход будет развит на основании результатов действий по оценке.

Проблемные области могут быть выявлены в результате исследования любого свидетельства, представленного для удовлетворения ТДБ, определенных для оценки ОО. Также рассматривается и информация, находящаяся в открытом доступе.

Действия, выполняемые оценщиком, могут быть повторены, и с точки зрения уровня доверия ОО при этом могут быть сделаны такие же выводы, хотя шаги оценивания для достижения этих выводов могут меняться. Так как оценщик документирует форму проведённого анализа, то фактические шаги оценивания, предпринятые для достижения этих выводов, также легко воспроизводимы.

B.2.2.2.3 Методический анализ

Методический подход к анализу принимает форму структурированного исследования свидетельств. Для данного метода требуется, чтобы оценщик определил структуру и форму анализа до его начала (то есть манера, в которой будет проведён анализ, предопределена, в отличие от направленного метода идентификации уязвимостей). Метод определяется в терминах того, какая информация будет подвергнута рассмотрению, каким образом и с какой целью. Такой подход к идентификации потенциальных уязвимостей может использоваться во время независимого анализа уязвимостей, требуемого «Подвидом деятельности по оценке» (AVA_VAN.4) и «Подвидом деятельности по оценке» (AVA_VAN.5).

Такой анализ свидетельств является преднамеренным и предварительно планируется; все идентифицированные свидетельства при этом идентифицируются в качестве исходных данных для анализа.

Все свидетельства, предоставленные для удовлетворения требований доверия (ADV), определенных в пакете доверия, используются в качестве исходных данных для деятельности по идентификации потенциальных уязвимостей.

«Методическое» описание для этого анализа используется в попытке характеризовать, что эта идентификация потенциальных уязвимостей основывается на структурированном и запланированном подходе. При проведении исследования должны быть использованы «метод» или «система». Оценщику следует описать метод, который будет им использоваться, в терминах того, какие именно свидетельства будут рассмотрены, какая именно информация данных свидетельств должна быть исследована и какие гипотезы должны выводиться на основании данных исследований.

Ниже представлены некоторые примеры гипотез:

a) рассмотрение плохо сформированных исходных данных интерфейсов, доступных нарушителям на уровне внешних интерфейсов;

b) исследование механизма безопасности, такого как разделение доменов, при котором выдвигается гипотеза возможности переполнения внутреннего буфера, приводящее к снижению эффективности разделения;

c) анализ, проводимый для идентификации любых объектов, созданных в представлении реализации ОО, которые не находятся полностью под управлением ФБО и могут быть использованы нарушителем для компрометации выполнения ФТБ.

Например, оценщик может идентифицировать, что интерфейсы — это потенциальная проблемная область ОО и специфицировать подход к анализу, заключающийся в том, что «все спецификации интерфейсов, предоставленные в функциональной спецификации и проекте ОО, будут проанализированы в целях выдвижения гипотезы о потенциальных опасных областях», а затем объяснить методы, используемые при выдвижении гипотезы.

Такой метод идентификации обеспечивает составление плана нападений на ОО, которые будут выполнены оценщиком в рамках проведения тестирования проникновения с использованием потенциальных уязвимостей ОО. Обоснование метода идентификации предоставляет свидетельства покрытия и определение глубины возможного использования уязвимостей, выполнимой для ОО.

В.3 Случаи применения потенциала нападения

В.3.1 Разработчиком

Потенциал нападения применяется автором ПЗ/ЗБ во время разработки ПЗ/ЗБ с учетом угроз среды и выбора компонентов доверия. Это может быть как просто определением, что потенциал нападения предполагаемых нарушителей в общем характеризуется как базовый, усиленный базовый, умеренный или высокий, так и спецификацией в ПЗ/ЗБ отдельных уровней конкретных факторов, которые могут быть присущи нарушителям (например может предполагаться, что нарушители — эксперты по данному технологическому типу ОО, имеющие доступ к специализированному оборудованию).

Автор ПЗ/ЗБ рассматривает профиль угрозы, разработанный во время оценки уровня риска (данный вопрос находится вне области ИСО/МЭК 15408, но используется в качестве исходных данных для разработки ПЗ/ЗБ с точки зрения определения проблемы безопасности или, в случае низкого уровня доверия ЗБ, изложения требований). Рассмотрение такого профиля угрозы с точки зрения одного из подходов, рассматриваемых в следующих подразделах, позволит составить спецификацию потенциала нападения, которому должен противостоять ОО.

В.3.2 Оценщиком

Потенциал нападения рассматривается оценщиком отдельно двумя различными способами во время оценки ЗБ и во время действий по оценке уязвимостей.

Потенциал нападения используется оценщиком во время проведения подвида деятельности по анализу уязвимостей, чтобы определить, является ли ОО стойким по отношению к нападениям нарушителей с определенным потенциалом нападения. Если оценщик вынес заключение о том, что возможно использование потенциальной уязвимости в ОО, он должен подтвердить, что использование возможно и с учетом всех аспектов среды предполагаемого функционирования ОО, включая предполагаемый потенциал нападения нарушителя.

Поэтому, используя информацию, предоставленную в изложении угроз ЗБ, оценщик определяет минимальный потенциал нападения, требуемый нарушителем для осуществления нападения, и приходит к некоторому выводу о способности ОО противостоять нападениям. В таблице В.1 отображены отношения между этим анализом и потенциалом нападения.

Таблица В.1 Анализ уязвимостей и потенциал нападения

Компонент анализа уязвимостей	ОО противостоит нарушителю с потенциалом нападения:	Остаточные уязвимости способен использовать только нарушитель с потенциалом нападения:
VAN.5	высокий	Не применимо — успешное нападение за пределами практически возможного
VAN.4	умеренный	высокий
VAN.3	усиленный базовый	умеренный
VAN.2	базовый	усиленный базовый
VAN.1	базовый	усиленный базовый

Запись «успешное нападение за пределами практически возможного» в столбце остаточных уязвимостей вышеприведенной таблицы означает такие потенциальные уязвимости, для использования которых необходимо, чтобы нарушитель обладал более высоким потенциалом нападения, нежели «высокий». Уязвимость, классифицированная как остаточная в этом случае, отражает тот факт, что известная уязвимость имеет место в данном ОО, но в текущей среде функционирования не может быть использована нарушителями с предполагаемым потенциалом нападения.

Для любого уровня потенциала нападения потенциальную уязвимость можно считать «неосуществимой» в случае применения мер противодействия, которые не позволяют допустить использования нарушителем данной уязвимости.

Анализ уязвимости относится ко всем ИФБО, включая те, которые предоставляют доступ к вероятностным или перестановочным механизмам. При этом не делается никаких предположений относительно правильности разработки проекта и реализации ИФБО; также при этом не накладывается ограничений на методы нападения или взаимодействия нарушителя с ОО — если нападение возможно, то его нужно рассмотреть во время анализа уязвимости. Как показано в Таблице В.1, успешно проведенная оценка компонента оценки уязвимостей отражает,

что ФБО разработаны и реализованы таким образом, чтобы обеспечить требуемую защиту от конкретного уровня угрозы.

Оценщику необязательно вычислять потенциал нападения для каждой потенциальной уязвимости. В некоторых случаях уже при разработке возможных методов нападения становится очевидно, соразмерен ли потенциал нападения, необходимый для применения некоторого метода нападения и для управления им, с предполагаемым для среды функционирования потенциалом нападения нарушителя. Для любых уязвимостей, для которых определена возможность использования, оценщик вычисляет потенциал нападения в целях вынесения заключения о том, что возможность использования соответствует уровню потенциала нападения предполагаемого нарушителя.

Описанный ниже подход должен применяться всякий раз, когда необходимо вычислить потенциал нападения, если органом оценки не предусмотрено использование в обязательном порядке некого альтернативного подхода. Значения, приведенные в Таблицах В.2 и В.3, математически не доказаны. Поэтому значения, приводимые в таблицах в качестве примера, возможно, следует приспособить к технологическому типу ОО и определенной среды функционирования. Оценщику следует получить руководство по данному вопросу от органа оценки.

В.4 Вычисление потенциала нападения

В.4.1 Применение потенциала нападения

Потенциал нападения зависит от компетентности, ресурсов и мотивации нарушителя. Существуют различные методы представления и вычисления этих факторов. Кроме того, следует учесть, что для конкретных типов ОО может возникнуть необходимость рассмотреть другие применимые факторы.

В.4.1.1 Трактовка мотивации

Мотивация является фактором потенциала нападения, который может использоваться для описания различных аспектов, относящихся к нарушителю и активам, которые интересуют нарушителя. Во-первых, мотивация может подразумевать определенную вероятность нападения — из угрозы, описанной как высокомотивированная, можно предположить, что нападение неизбежно, а из описания угрозы как немотивированной — что нападения не ожидается. Однако за исключением этих двух крайних уровней мотивации, затруднительно установить вероятность осуществления нападения, исходя только из мотивации.

Во-вторых, мотивация может подразумевать определенную ценность актива в денежном или ином выражении для нарушителя или владельца актива. Более ценный актив обусловит, вероятно, более высокую мотивацию по сравнению с менее ценным активом. Однако, кроме общих рассуждений, трудно связать ценность актива с мотивацией, потому что ценность актива субъективна — она в значительной степени зависит от того, что вкладывает в понятие «ценность» владелец актива.

В-третьих, мотивация может подразумевать определенную компетентность и ресурсы, с помощью которых нарушитель намеревается произвести нападение. Можно предположить, что нарушитель с высокой мотивацией, вероятно, приобретет достаточную компетентность и ресурсы, чтобы преодолеть меры защиты актива. И, наоборот, можно предположить, что нарушитель с высокой компетентностью и значительными ресурсами не захочет, используя их, произвести нападение, если имеет низкую мотивацию.

В ходе подготовки и проведения оценки, так или иначе, рассматриваются все три аспекта мотивации. Первый аспект — вероятность нападения — это то, что может побудить разработчика добиваться оценки. Если разработчик полагает, что у нарушителей имеется достаточная мотивация, чтобы организовать нападение, то оценка может обеспечить доверие к способности ОО помешать усилиям нарушителя. Когда предполагаемая среда полностью определена, например при оценке системы, уровень мотивации нападения может быть известен и повлияет на выбор контрмер.

Рассматривая второй аспект, владелец актива может полагать, что ценность активов (как-либо измеренная) достаточна, чтобы мотивировать нападение на них. Как только оценку посчитают необходимой, рассматривается мотивация нарушителя для определения методов нападения, которое может быть предпринято, а также компетентность и ресурсы, которые могут использоваться при этих нападениях. После проведения исследований разработчик способен выбрать соответствующий уровень доверия, в частности, компоненты требований из класса AVA, соразмерные с потенциалом нападения для данных угроз. В ходе оценки и, в частности, по результатам завершения вида деятельности по оценке уязвимостей оценщик делает заключение, достаточен ли ОО, функционирующий в среде функционирования, чтобы помешать нарушителям с идентифицированной компетентностью и ресурсами.

Для автора ПЗ может иметься возможность вычислить мотивацию нарушителя, поскольку автор ПЗ обладает большим объемом знаний о среде функционирования, в которую должен быть помещен ОО (в соответствии с требованиями ПЗ). Поэтому мотивация может являться явной частью отражения потенциала нападения в ПЗ, наряду с необходимыми методами и мерами определения уровня мотивации.

В.4.2 Характеризация потенциала нападения

В этом подразделе исследуются факторы, которые определяют потенциал нападения, и предоставляется руководство, способствующее устранению некоторой субъективности этого аспекта процесса оценивания.

В.4.2.1 Определение потенциала нападения

Определение потенциала нападения соответствует идентификации усилия, требуемого для подготовки нападения и демонстрации того факта, что это нападение может быть путём использования уязвимости успешно применено к данному ОО (к данным усилиям относят и подготовку или производство любого необходимого испытательного оборудования). Для демонстрации того, что нападение может быть успешно применено, требуется рассмотреть все трудности по получению остальных показанных в лаборатории результатов в целях моделирования успешной атаки. Например, если при проведении эксперимента был получен доступ к некоторым битам или бай-

там элемента конфиденциальных данных (например к криптографическому ключу), то необходимо рассмотреть, как можно получить остальные данные (для рассматриваемого примера некоторые биты информации могут быть получены непосредственно в ходе дальнейших экспериментов, а некоторые могут быть открыты путем применения различных специальных методов, например поиска методом полного перебора). Не всегда обязательно проводить все эксперименты, чтобы идентифицировать полностью проведенное нападение, если очевидно, что нападение фактически доказывает, что был получен доступ к активам ОО и что полное нападение может быть осуществлено в реальных условиях при использовании уязвимости, согласно целевому компоненту семейства AVA_VAN. В некоторых случаях единственный способ доказать, что нападение может быть осуществлено в реальных условиях при использовании уязвимости согласно целевому компоненту семейства AVA_VAN состоит в том, чтобы полностью провести нападение, и затем присвоить данному нападению некий рейтинг в зависимости от того, какие ресурсы потребовались для его реализации. Предполагается, что выходными данными идентификации потенциальной уязвимости является сценарий нападения, который дает пошаговое описание того, каким образом имеющуюся уязвимость данного ОО можно использовать для проведения нападения.

Во многих случаях оценщики проводят оценку параметров, необходимых для того, чтобы нарушитель воспользовался уязвимостью, а не осуществляют полное моделирование такого использования данной уязвимости. Такая оценка и её обоснование будут приведены в ТОО.

В.4.2.2 Учитываемые факторы

В ходе анализа потенциала нападения, требуемого для использования уязвимости, необходимо учитывать следующие факторы:

a) время, затрачиваемое на идентификацию уязвимости и её использование (**общее затрачиваемое время**);

b) требующаяся техническая компетентность специалиста (**компетентность специалиста**);

c) знание проекта ОО и его функционирования (**знание ОО**);

d) **возможность доступа к ОО**;

e) **аппаратные средства/программное обеспечение ИТ или другое оборудование**, требуемое для использования уязвимости.

Во многих случаях эти факторы не являются независимыми и могут в различной степени заменять друг друга. Например, компетентность или аппаратные средства/программное обеспечение могут быть заменой времени. Эти факторы обсуждаются далее (уровни каждого фактора рассматриваются в порядке увеличения). В таком случае в фазе использования уязвимости рассматривается наименее «затратная» комбинация факторов.

Общее затрачиваемое время — это время, которое необходимо нарушителю для идентификации потенциальной уязвимости, которая может существовать в ОО, разработки метода нападения и поддержания усилий по осуществлению нападения на ОО. При рассмотрении данного фактора для определения требуемого нарушителю количества времени используется пессимистичный, наиболее неблагоприятный сценарий. Идентифицированными уровнями отрезков времени являются следующие:

a) менее одного дня;

b) от одного дня до недели:

c) от одной до двух недель;

d) от двух недель до месяца;

e) месяц, два месяца, три — каждый дополнительный месяц до шести означает увеличение значения;

f) более шести месяцев.

Компетентность специалиста относится к уровню общих знаний основополагающих принципов, типа продукта или методов нападения (например знаний об операционной системе Unix, протоколах Интернета, переполнении буфера). Идентифицированными уровнями являются следующие:

a) непрофессионалы слабо осведомлены по сравнению с экспертами или профессионалами, и не обладают специфической компетентностью;

b) профессионалы хорошо осведомлены в том, что касается режима безопасности продукта или системы данного типа;

c) эксперты хорошо знакомы с основными алгоритмами, протоколами, аппаратными средствами, структурами, режимом безопасности, с применяемыми принципами и концепциями безопасности, а также с методами и средствами определения новых атак, криптографическими средствами и методами, классическими атаками на данный тип продукта ИТ, методами нападения и т. п., реализуемыми для данного типа продукта или системы;

d) уровень «Эксперт в нескольких областях знаний или группа экспертов» применяется в случае, когда для осуществления отдельных этапов нападения необходимы знания на уровне Эксперт в различных областях.

Бывают ситуации, когда требуется применить в описании несколько различных типов компетентности. По умолчанию выбирается самый высокий уровень факторов компетентности. В некоторых особых случаях применимо значение уровня «Эксперт в нескольких областях знаний или группа экспертов», но в этом случае необходимо отметить, что области знаний, в которых предполагаемые нарушители являются экспертами, должны быть принципиально разными, например управление аппаратными средствами и криптография.

Знание ОО указывает на определенный уровень знаний об ОО. Оно отличается от общей компетентности, хотя и связано с ней. Идентифицированными уровнями являются следующие:

a) общедоступная информация об ОО (например полученная из сети Интернет);

b) информация ограниченного доступа об ОО (например сведения, которыми управляет организация-разработчик и предоставляет их другим организациям на условиях соглашения о неразглашении информации);

c) чувствительная информация об ОО (например сведения, которыми обладают закрытые рабочие группы организации-разработчика, и доступ к которым имеют только члены данных групп);

d) критически важная информация об ОО (например сведения, которые известны только нескольким лицам, и доступ к которым строго контролируется на основе личной ответственности и необходимости доступа для выполнения рабочих обязанностей).

Уровень знания об ОО может различаться еще и в зависимости от детализации проекта ОО, хотя это осуществимо только на уровне описания основ ОО. Некоторые проекты ОО могут представлять собой общедоступную информацию (или сильно зависящую от общедоступной) и поэтому даже представление проекта будет классифицироваться как общедоступная информация или, в крайнем случае, как информация ограниченного доступа, тогда как доступ к представлению реализации других ОО будет строго контролироваться, т. к. нарушитель может получить из него сведения, которые могут помочь ему в осуществлении нападения, и поэтому такие представления реализации будут считаться чувствительной или даже критически важной информацией.

Бывают ситуации, когда требуется применить в описании несколько различных типов знания. По умолчанию выбирается самый высокий уровень факторов знания об ОО.

Возможность доступа к ОО (Возможность) также является важным обстоятельством и имеет отношение к фактору «общее затрачиваемое время». Идентификация или использование уязвимости могут требовать продолжительного доступа к ОО, что может увеличить вероятность обнаружения. Некоторые методы нападения могут требовать значительных автономных усилий без подключения к ОО и лишь краткого времени доступа к ОО для использования уязвимости. Может также потребоваться непрерывный доступ или доступ в виде нескольких сеансов.

Для некоторых ОО возможность доступа к ОО может равняться числу образцов ОО, которые может получить нарушитель. Это особенно справедливо для тех случаев, когда попытки проникновения к ОО и компрометации ФТБ могут привести к разрушению ОО или превентивному использованию обработки ОО для дальнейшего тестирования, например аппаратных средств. Часто в этих случаях распределение ОО контролируется таким образом, что нарушитель должен потратить дополнительные усилия для получения доступа к остальным образцам ОО.

В целях данного обсуждения:

a) «отсутствие необходимости в доступе/неограниченный доступ» означает, что для нападения не важна возможность доступа к ОО, т. к. нет опасности обнаружения при осуществлении доступа к ОО и нет препятствий для доступа к образцам ОО для нападения;

b) «простой доступ» означает, что доступ требуется менее чем на день, а количество образцов ОО, к которым требуется доступ для осуществления нападения, меньше десяти;

c) «умеренная возможность доступа» означает, что доступ требуется менее чем на месяц, а количество образцов ОО, к которым требуется доступ для осуществления нападения, меньше сотни;

d) «затруднительный доступ» означает, что доступ требуется хотя бы на месяц, а количество образцов ОО, к которым требуется доступ для осуществления нападения, больше или равно ста;

e) «невозможность доступа» означает, что времени возможности доступа недостаточно для осуществления нападения (промежуток времени, во время которого актив, на который направлено нападение, доступен или уязвим, меньше, чем промежуток времени, требуемый для осуществления нападения). Например, криптографический ключ некоторого актива меняется раз в неделю, а для его успешного подбора требуются две недели. Другой подобный случай — когда достаточное для осуществления нападения количество образцов ОО недоступно нарушителю — например если ОО является аппаратным средством, и вероятность его разрушения в процессе нападения больше, чем вероятность успешного завершения нападения, а у нарушителя есть всего один образец ОО.

Рассмотрение данного фактора может привести к вынесению заключения о том, что невозможно реализовать использование уязвимости вследствие того, что требуемый нарушителю промежуток времени доступа больше, чем промежуток времени реальной возможности осуществления доступа.

Аппаратные средства/программное обеспечение ИТ или другое оборудование указывает на оборудование, которое требуется для идентификации или использования уязвимости.

a) Стандартное оборудование — это оборудование либо для идентификации уязвимости, либо для нападения, которое легко доступно нарушителю. Это оборудование может быть частью самого ОО (например отладчик в операционной системе) или может быть легко получено (например программное обеспечение, загружаемое из Интернета, анализаторы протоколов или простые сценарии нападения).

b) Специализированное оборудование, которое не слишком легко доступно для нарушителя, но может быть приобретено без значительных усилий. Это может включать или покупку небольшого количества оборудования (например средств атаки по энергопотреблению, использование сотни ПК, объединенных через сеть Интернет, подойдет к этой категории) или разработку более сложных сценариев и программ нападения. Если для проведения различных этапов нападения требуются различные испытательные стенды со специальным оборудованием, это расценивается как заказное оборудование.

c) Заказное оборудование, недоступное широкому кругу пользователей, поскольку для него либо может потребоваться специальная разработка (например очень сложного программного обеспечения), либо оборудование настолько специализировано, что его распространение контролируется и, возможно, это оборудование является оборудованием ограниченного распространения. Или же данное оборудование очень дорогостоящее.

d) Уровень «Несколько видов заказного оборудования» применяется в том случае, когда для осуществления отдельных этапов нападения необходимо различное, сделанное на заказ оборудование.

Компетентность специалиста и знание ОО связаны с информацией, необходимой нарушителям для того, чтобы быть способными к нападению на ОО. Существует неявная зависимость между компетентностью наруши-

теля (где под нарушителем может пониматься и группа лиц, дополняющих знания друг друга в различных областях) и его способностью эффективно использовать оборудование при нападении. Чем ниже компетентность нарушителя, тем ниже потенциал использования оборудования (аппаратных средств/программного обеспечения ИТ или другого оборудования). Аналогично, чем выше компетентность, тем выше потенциал оборудования, используемого при нападении. Будучи неявной, зависимость между компетентностью и использованием оборудования проявляется не всегда: например если меры безопасности среды предотвращают использование оборудования опытным нарушителем или если кем-то другим созданы и свободно распространяются (например через Интернет) инструментальные средства нападения, требующие невысокой квалификации для эффективного использования.

В.4.2.3 Вычисление потенциала нападения

В таблице В.2 идентифицируются факторы, обсуждавшиеся в предыдущем подразделе, и приводятся числовые значения, а также общее значение для каждого фактора.

Когда значение фактора оказывается близким к границе диапазона, оценщику следует подумать об использовании значения, усредняющего табличные. Например, если для осуществления нападения требуется доступ к двадцати образцам ОО, то для этого фактора может быть выбрано значение между 0 и 4. Или, если проект основан на общедоступном проекте, но разработчик внёс в проект изменения, то для этого фактора может быть выбрано значение между 0 и 3, в соответствии с представлением оценщика о том, насколько данные изменения влияют на проект. Таблица В.2 предназначена для руководства.

К спецификации, отмеченной в таблице «**» при рассмотрении ***Возможности доступа***, не следует относиться как к естественному развитию шкалы времени, определенной в предыдущих диапазонах, связанных с этим фактором. Эта спецификация идентифицирует, что по некоторой особой причине потенциальная уязвимость ОО в предполагаемой среде функционирования не может быть использована нарушителем. Например, несанкционированный доступ к ОО в известной среде функционирования (то есть в случае ОО как системы) может быть обнаружен спустя определенное количество времени при проведении регулярной проверки, и нарушитель не может получить доступ к ОО на необходимые ему две недели, не будучи обнаружен. Однако это не применимо для ОО, подключенного к сети, где есть возможность удаленного доступа к ОО, или в случае, когда физическая среда ОО неизвестна.

Таблица В.2. Вычисление потенциала нападения

Фактор		Значение
Общее затрачиваемое время	≤ 1 день	0
	≤ 1 неделя	1
	≤ 2 недели	2
	≤ 1 месяц	4
	≤ 2 месяца	7
	≤ 3 месяца	10
	≤ 4 месяца	13
	≤ 5 месяца	15
	≤ 6 месяца	17
	> 6 месяцев	19
Компетентность	Непрофессионал	0
	Профессионал	3*(1)
	Эксперт	6
	Группа экспертов	8
Знание ОО	Общедоступная информация	0
	Информация ограниченного доступа	3
	Чувствительная информация	7
	Критически важная информация	11

Окончание таблицы В.2

Фактор		Значение
Возможность доступа к ОО	Отсутствие необходимости в доступе/неограниченный доступ	0
	Простой доступ	1
	Умеренная возможность доступа	4
	Затруднительный доступ	10
	Невозможность доступа	**(2)
Оборудование	Стандартное	0
	Специализированное	4(3)
	Сделанное на заказ	7
	Несколько видов сделанного на заказ оборудования	9

(1) Если требуется несколько поочередно работающих профессионалов для завершения нападения, результирующий уровень компетентности все равно будет «Профессионал» (что соответствует значению 3).

(2) Указывает, что канал атаки невозможно осуществить из-за предпринятых других мер в предполагаемой среде функционирования ОО.

(3) Если для проведения различных этапов нападения требуются различные испытательные стенды со специальным оборудованием, это расценивается как заказное оборудование.

Чтобы определить стойкость ОО по отношению к атакам, использующим идентифицированные потенциальные уязвимости, следует применить следующее:

a) определить возможные сценарии нападения {AS1, AS2..., ASn} на ОО в среде функционирования;

b) для каждого сценария нападения выполнить теоретический анализ и вычислить соответствующий потенциал нападения, используя таблицу В.2;

c) при необходимости для каждого сценария нападения выполнить тесты проникновения, чтобы подтвердить или опровергнуть результаты теоретического анализа;

d) распределить все сценарии нападения {AS1, AS2..., ASn} на две группы:

1) сценарии нападения, которые были успешно реализованы (то есть те, которые использовались для успешной компрометации ФТБ), и

2) сценарии нападения, для которых есть демонстрация того, что они нереализуемы.

e) для каждого успешно реализованного сценария нападения применить таблицу В.3 и сделать заключение о том, нет ли противоречия между стойкостью ОО и выбранным компонентом доверия семейства AVA_VAN (см. последнюю колонку таблицы В.3).

f) в случае обнаружения подобного противоречия, по оценке уязвимостей выносится отрицательный вердикт. Например, если автор ЗБ выбрал компонент AVA_VAN.5, а сценарий нападения с потенциалом нападения 21 («Высокий») нарушил безопасность ОО. В этом случае ОО стойкий только к атакам нарушителя с «Умеренным» потенциалом нападения, что противоречит требованиям AVA_VAN.5. Следовательно, при оценке уязвимостей выносится отрицательный вердикт.

Колонка «Диапазон значений» таблицы В.3 указывает на диапазон значений потенциала нападения (вычисленных с использованием таблицы В.2) тех сценариев нападения, которые не приводят к нарушению выполнения ФТБ.

Подобный подход не позволяет учесть все обстоятельства и факторы, но должен более точно указывать на уровень противодействия нападениям, требуемый для достижения стандартных рейтингов. Другие факторы, такие как расчет на малую вероятность случайных воздействий, не включены в данную базовую модель, но могут использоваться оценщиком как логическое обоснование для рейтинга иного, чем тот, который представлен в базовой модели.

Следует отметить, что в то время как ряд уязвимостей, оцениваемых по отдельности, может указывать на высокий уровень противодействия нападениям, комбинация уязвимостей будет свидетельствовать о применимости более низкого общего рейтинга. Другими словами, наличие одной уязвимости может упростить использование другой.

В случае, если автор ПЗ/ЗБ хочет использовать таблицу потенциала нападения для определения уровня нападения, которому может противостоять ОО (выборка компонентов семейства «Анализ уязвимостей» AVA_VAN), он должен сделать следующее: для всех различных сценариев нападения (то есть для всех различных типов нарушителя и/или различных методов нападения, которые предполагаются автором), которые не должны нарушить выполнение ФТБ, следует использовать таблицу несколько раз в целях определения различных значений предполагаемого потенциала нападения для каждого такого нереализуемого сценария. Затем автор ПЗ/ЗБ выбирает самое большое значение в целях определения уровня стойкости ОО, которое определяется по Таблице В.3: стойкость ОО должна быть, по крайней мере, равной этому наибольшему значению. Например, наибольшее значение потенциалов на-

падения всех сценариев нападения, которые не должны подрывать выполнение политики безопасности ОО, определенное таким способом, будет «Умеренный»; следовательно, уровень стойкости ОО должен быть, по крайней мере, «Умеренным» (то есть либо «Умеренным», либо «Высоким»), поэтому автор ПЗ/ЗБ может выбрать в качестве соответствующего компонента доверия или AVA_VAN.4 (для «Умеренного») или AVA_VAN.5 (для «Высокого»).

Таблица В.3. Рейтинг уязвимостей и уровень стойкости ОО

Диапазон значений	Потенциал нападения, требуемый для использования сценария:	ОО противостоит нарушителю с потенциалом нападения:	Удовлетворяет требованиям компонентов доверия:	Не удовлетворяет требованиям компонентов:
0-9	Базовый	Не противостоит	—	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Усиленный базовый	Базовый	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Умеренный	Усиленный базовый	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	Высокий	Умеренный	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	За пределами высокого	Высокий	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	—

В.5 Пример расчета для случая прямого нападения

Механизмы, подвергающиеся прямому нападению, часто жизненно необходимы для обеспечения безопасности системы, и разработчики часто усиливают эти механизмы. Например, в ОО может быть использован простой механизм аутентификации по цифровому паролю, который может быть преодолен нарушителем, если у того имеется возможность неоднократно повторять попытки угадывания значения пароля другого пользователя. Система может усилить этот механизм, установив тем или иным образом ограничения на значения пароля и на его использование. В процессе оценки анализ этого прямого нападения может проводиться следующим образом.

Информация, полученная из ЗБ и свидетельств проекта, показывает, что идентификация и аутентификация предоставляют основу для управления доступом к сетевым ресурсам с терминалов, расположенных далеко друг от друга. Управление физическим доступом к терминалам каким-либо эффективным способом не осуществляется. Управление продолжительностью доступа к терминалу каким-либо эффективным способом не осуществляется. Уполномоченные пользователи системы подбирают себе свои собственные цифровые пароли для входа в систему во время начальной авторизации использования системы и в дальнейшем — по запросу пользователя. Система содержит следующие ограничения на цифровые пароли, выбираемые пользователем:

a) цифровой пароль должен быть не менее четырех и не более шести цифр длиной;

b) последовательные числовые ряды (типа 7,6,5,4,3) не допускаются;

c) повторение цифр не допускается (каждая цифра должна быть уникальной).

Руководство, предоставляемое пользователям на момент выбора цифрового пароля, является таковым, чтобы цифровые пароли были случайны, насколько это возможно, и не связаны каким-либо способом с конкретным пользователем, например с датой рождения.

Число возможных значений цифровых паролей рассчитывается следующим образом:

a) Шаблоны, используемые людьми, являются важным обстоятельством, которое может влиять на подход к поиску возможных значений цифровых паролей. Допуская самый плохой вариант сценария, когда пользователь выбирает число, состоящее только из четырех цифр, число перестановок цифрового пароля, если предположить, что каждая цифра уникальна, равно:

$$7(8)(9)(10) = 5040$$

b) Число возможных последовательных числовых рядов по возрастанию — семь, как и число таких рядов по убыванию. После отбрасывания этих рядов число возможных значений цифровых паролей равно:

$$5040 - 14 = 5026$$

Основываясь на дополнительной информации, полученной из свидетельств проекта, в механизме цифрового пароля спроектирована характеристика блокировки терминала. После шестой подряд неудачной попытки аутентификации терминал блокируется на один час. Счетчик неудачной аутентификации сбрасывается через пять минут; таким образом, нарушитель в лучшем случае может осуществить пять попыток ввода цифрового пароля каждые пять минут или 60 вводов цифрового пароля в час.

В среднем нарушитель должен был бы ввести 2513 цифровых паролей более чем за 2513 минуты до ввода правильного цифрового пароля. Как результат, в среднем успешное нападение произошло бы чуть меньше, чем за:

$$\frac{2513 \text{ мин}}{60 \frac{\text{мин}}{\text{час}}} \approx 42 \text{ часа}$$

Используя подход к вычислению потенциала нападения, описанный в предыдущем подразделе, можно идентифицировать, что непрофессионал может преодолеть данный механизм аутентификации в течение нескольких дней (при условии незатрудненного доступа к ОО) без использования какого-либо специального оборудования и без знания ОО, что дает значение 1. Получаем результирующую сумму 1, что означает, что потенциал нападения, требуемый для осуществления успешной атаки, не подпадает ни под одну категорию, так как является даже меньшим, чем «Базовый».

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование межгосударственного стандарта
ИСО/МЭК 18045	IDT	ИСО/МЭК 18045:2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» («ISO/IEC Information technology — Security techniques — Methodology for IT security evaluation»
ИСО/МЭК 15408	MOD	ИСО/МЭК 15408 (все части) Информационная технология — Методы и средства обеспечения безопасности — Критерии оценки безопасности ИТ

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических документов и регламентов.

Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандарта:

- IDT — идентичные стандарты;
- MOD — модифицированные стандарты.

Библиография

Данная библиография содержит ссылки на материалы и стандарты, которые могут оказаться полезными для пользователя ИСО/МЭК 18045. При отсутствии в ссылке указания даты пользователю рекомендовано использовать последнюю редакцию документа.

Стандарты и руководства ИСО/МЭК

[1] ISO/IEC 15443 (все части), Information technology — Security techniques — A framework for IT security assurance.

[2] ISO/IEC 15446, Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets.

[3] ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules.

[4] ISO/IEC 19791, Information technology — Security techniques — Security assessment of operational systems.

[5] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements.

[6] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security management.

Другие стандарты и руководства

[7] IEEE Std 610.12—1990, Institute of Electrical and Electronics Engineers, Standard Glossary of Software Engineering Terminology.

[8] Портал Common Criteria, CCRA, www.commoncriteriaportal.org.

УДК 681.324:006.354 ОКС 35.040 П85 ОКСТУ 4002

Ключевые слова: информационная технология, критерии оценки безопасности, задание по безопасности, профиль защиты, объект оценки, функциональные возможности безопасности

Редактор *Т.С. Никифорова*
Технический редактор *А.Г. Костарева*
Корректор *Н.В. Каткова, Г.Н. Старкова*
Компьютерная верстка *Е.Г. Жилиной*

Сдано в набор 24.04.2014. Подписано в печать 02.06.2014. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 28,83. Уч.-изд. л. 25,19. Тираж 53 экз. Зак.

Набрано в Издательском доме «Вебстер»
www.idvebster.ru project@idvebster.ru
Отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256