ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ

СТ РК 34.023-2006

Издание официальное

Комитет по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан

Астана

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН ТОО «Специальное конструкторско-технологическое бюро «Гранит»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Председателя Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан от 15 декабря 2006 г. № 550

3 В настоящем стандарте реализованы нормы законов Республики Казахстан О техническом регулировании, О языках в Республике Казахстан, О государственных секретах, Соглашения Всемирной торговой организации по техническим барьерам в торговле, Постановление КМ РК №1111-43с 05.11.94 «Об утверждении Положения о государственной системе защиты информации РК и Постановление Правительства Республики Казахстан от 19 октября 2000 года N 1561 Об утверждении Правил выдачи сертификата соответствия технических средств защиты сведений, составляющих государственные секреты

4 СРОК ПЕРВОЙ ПРОВЕРКИ 2011 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

Методика оценки соответствия информационных систем требованиям безопасности является одним из основных документов поддержки СТ РК ГОСТ Р ИСО/МЭК 15408-2006 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (Общие критерии - ОК).

ОК содержат каталог требований безопасности информационных технологий (ИТ) и правила формирования на базе этого каталога совокупностей требований для определенных типов продуктов и систем ИТ в виде профилей защиты, а для конкретных продуктов и систем ИТ – в виде заданий по безопасности. Методика оценки содержит общий методологический подход к проведению оценки ОО (общие методики оценки, которые могут конкретизироваться для каждого продукта или системы).

Сочетание Общих критериев и Методики оценки (МО) обеспечивает возможность единого подхода к оценке безопасности информационных систем и получению объективных и повторяемых результатов.

Настоящий стандарт охватывает все виды деятельности по оценке, соответствующие классам доверия из части 3 ОК, входящим в оценочные уровни доверия.

Принятый подход к разработке документа обеспечил необходимую полноту Методики для возможности ее практического использования при оценке безопасности информационных технологий.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ

Дата введения 2008.01.01

1 Область применения

Настоящий стандарт распространяется на информационные технологии и устанавливает требования к методике оценки информационных систем требованиям безопасности.

Методика оценки соответствия информационных систем требованиям безопасности описывает минимум действий, выполняемых оценщиком при проведении оценки по ОК с использованием критериев и свидетельств оценки, определенных в ОК.

В данном документе представлена методика для оценки большей части компонентов доверия, определенных в ОК и применяемых при оценке ОО, в том числе для всех компонентов доверия, используемых в ОУД 1–4.

МО предназначена, главным образом, для оценщиков, использующих ОК, и экспертов органов по подтверждению соответствия, подтверждающих действия оценщиков. МО может быть использована также заявителями на проведение оценки, разработчиками продуктов и систем ИТ, а также другими сторонами, заинтересованными в обеспечении безопасности ИТ.

Вопросы, связанные с оценкой безопасности ИТ и не рассмотренные в МО, должны быть включены в дополнительно разрабатываемые руководства по применению.

1.1 Общие положения

Принципами, лежащими в основе МО, являются:

1) Объективность – результаты оценки основываются на фактических свидетельствах и не зависят от личного мнения оценщика;

2) Беспристрастность – результаты оценки являются непредубежденными, когда требуется субъективное суждение;

3) Воспроизводимость – действия оценщика, выполняемые с использованием одной и той же совокупности исходных данных для оценки, которые всегда приводят к одним и тем же результатам;

4) Корректность – действия оценщика обеспечивают точную техническую оценку;

5) Достаточность – каждый вид деятельности по оценке осуществляется до уровня, необходимого для удовлетворения всех заданных требований доверия;

6) Приемлемость – каждое действие оценщика способствует повышению доверия, по меньшей мере, пропорционально затраченным усилиям.

1.2 Структура МО

МО разбита на следующие разделы:

Раздел 1 "Область применения" описывает цели, структуру, соглашения, а также вердикт оценщика.

Издание официальное

1.2 Структура МО

МО разбита на следующие разделы:

Раздел 1 "Область применения" описывает цели, структуру, соглашения, а также вердикт оценщика.

Разделы 2-3 содержат нормативные ссылки и описывают терминологию документа.

Раздел 4 "Процесс оценки и соответствующие задачи" описывает задачи, которые относятся ко всем видам деятельности по оценке. Это – задачи получения исходных данных для оценки и оформления результатов оценки.

Разделы 5–11 описывают методику оценивания по классам и компонентам доверия, приведенным в части 3 ОК.

Раздел 12 "Общие указания по оценке" содержит те общие указания, которые применяются при оценивании более чем по одному классу доверия из ОК.

1.3 Принятые соглашения

В отличие от части 3 ОК, где каждый соответствующий элемент во всех компонентах одного семейства доверия имеет один и тот же номер, указанный последней цифрой его условного обозначения, МО может вводить новые шаги оценивания при изменении элемента действий оценщика ОК в зависимости от подвида деятельности. В результате, последняя цифра условного обозначения последующих шагов оценивания изменится, хотя шаг оценивания останется тем же самым. Например, если добавлен новый шаг оценивания, помеченный ADV_FSP.2-7, то номера последующих шагов оценивания подвида деятельности FSP увеличиваются на единицу. Тогда шагу оценивания ADV_FSP.1-8 соответствует шаг оценивания ADV_FSP.2-9; хотя каждый из указанных шагов содержит одно и то же требование, их нумерация внутри своего подвида деятельности более не совпадает.

Любая определенная в методе работа по оценке, которая не следует непосредственно из требований ОК, называется *задачей* или *подзадачей*.

1.3.1 Применение глаголов

Любому основному глаголу описания шага оценивания или подзадачи предшествует вспомогательный глагол *должен*, причем и основной, и вспомогательный глагол выделены ***полужирным курсивом***. Вспомогательный глагол *должен* используется при обязательности содержащего его текста и, следовательно, только в рамках шага оценивания или подзадачи. Шаги оценивания и подзадачи содержат обязательные действия, которые оценщик должен выполнить, чтобы вынести вердикт. Вспомогательный глагол *следует* используется, когда описанный метод явно предпочтителен, но возможно применение и других обоснованных методов. Вспомогательный глагол *может* используется, когда что-либо разрешено, но не указано как предпочтительное.

Текст, сопровождающий шаги оценивания и подзадачи, содержит дальнейшие разъяснения использования формулировок ОК при оценке. Хотя сопроводительный текст не предписывает обязательные меры, он дает представление о том, что ожидается от оценщика при удовлетворении обязательных аспектов шагов оценивания.

Глаголы *проверить*, *исследовать*, *привести в отчете* и *зафиксировать* в тексте МО имеют точный смысл, указанный в разделе 3.

1.3.2 Общие указания по оценке

Материал, который применим более чем к одному подвиду деятельности, приводится МО один раз. Указания, применяемые к нескольким видам деятельности, чтобы не повторяться, собраны в разделе 12. Указания, относящиеся к нескольким

подвидам одного вида деятельности, содержатся во вводной части описания этого вида деятельности. Если указания относятся к единственному подвиду деятельности, они содержатся в его описании.

1.3.3 Взаимосвязь между структурами ОК и МО

Имеется прямая взаимосвязь между структурой ОК (класс-семейство-компонент-элемент) и структурой МО. Рисунок 1.1 иллюстрирует соответствие между такими конструкциями ОК, как классы, компоненты и элементы действий оценщика, и рассматриваемыми в МО видами деятельности, подвидами деятельности и действиями. Некоторые шаги оценивания МО могут следовать из требований ОК, содержащихся в элементах действий разработчика или содержания и представления свидетельств, на что по тексту имеются соответствующие ссылки в виде кратких имен соответствующих элементов требований из части 3 ОК.

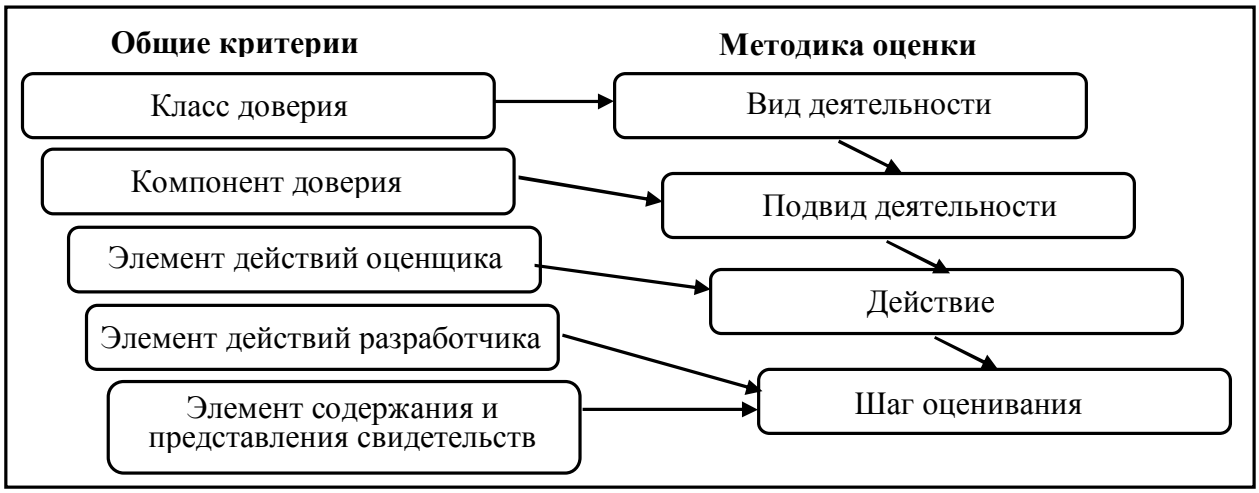


Рисунок 1.1 – Соотношение структур ОК и МО

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК ГОСТ Р ИСО/МЭК 15408-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

СТ РК ГОСТ Р ИСО/МЭК 15408-2-2006 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

3 Термины, определения, обозначения и сокращения

В настоящем стандарте применяются термины, определения и сокращения в соответствии с СТ РК ГОСТ Р ИСО/МЭК 15408-2006 и следующие термины с определениями и сокращениями, которые используются в МО, но не представлены в ОК:

3.1 Вид деятельности (activity): Комплекс работ по проверке выполнения требований класса доверия из части 3 ОК.

3.2 Подвид деятельности (sub-activity): Комплекс работ по проверке выполнения требований компонента доверия из части 3 ОК. Семейства доверия прямо не рассматриваются в МО, поскольку при проведении оценки всегда используется только один компонент доверия из применяемого семейства.

3.3 Действие (action): Комплекс работ по проверке выполнения требований элементов действий оценщика из части 3 ОК. Эти действия или сформулированы в явном виде как действия оценщика, или неявно следуют из действий разработчика (подразумеваемые действия оценщика) в рамках компонентов доверия из части 3 ОК.

3.4 Вердикт (Verdict*)*: Вывод оценщика «положительно», «отрицательно» или «неокончательно», применительно к некоторому элементу действий оценщика, компоненту или классу доверия из ОК. (См. также общий вердикт).

3.5 Вердикт органа по подтверждению соответствия (Authority Verdict): Вывод органа по подтверждению соответствия, подтверждающий или отклоняющий **общий вердикт**, который основан на результатах деятельности по надзору за оценкой.

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

3.7 Интерпретация (Interpretation): Разъяснение или расширение требования ОК. МО или системы оценки.

3.8 Исследовать (Examine): Вынести вердикт на основе анализа с использованием специальных знаний и опыта оценщика. Формулировка, в которой используется этот глагол, указывает на то, что конкретно и какие свойства подвергаются анализу.

3.9 Недостаток безопасности (Security flaw): Условие, которое само по себе или совместно с другими условиями определяет пригодную для использования уязвимость. Те нарушения ПБО, которые возникают не из-за проблем, связанных с аппаратной, программной или программно-аппаратной составляющей ОО, а из-за проблем связанных с содержанием **руководств ОО**, также признаются *недостатками безопасности*.

Примечание - Любые способы эксплуатации продукта или системы вне предопределенной среды, приводящие к нарушениям ПБО, не предполагаются для использования и поэтому не рассматриваются, как недостатки безопасности.

3.10 Общий вердикт (Overall Verdict): Положительный или отрицательный вывод оценщика по результатам оценки.

3.11 Отслеживание недостатка безопасности (Tracking n security flaw): Знание текущего состояния недостатка безопасности и его истории.

3.12 Пользователь ОО (TOE user): Служба эксплуатации или уполномоченное лицо, ответственное за получение и применение материалов по исправлению недостатков безопасности. Пользователь ОО может и не являться пользователем в том смысле, как это определено например, в требованиях семейства ОК AGD_USR, но может быть представителем организации, ответственным за устранение **недостатков безопасности**. Использование термина *пользователь ОО* свидетельствует о признании, что различные организации имеют различные процедуры обработки сообщении о недостатках, которая может осуществляться, как каждым пользователем самостоятельно, так и централизованно службой администрирование.

Примечание - Данное определение относится только к тем пользователям ОО, которые занимаются отслеживанием: и устранением выявленных в ОО недостатков, расширяя понятие пользователя ОО для данного конкретного случая.

3.13 Поставка для оценки (Evaluation Deliverable): Любой ресурс, который оценщик или орган по подтверждению соответствия требует от заявителя или разработчика для выполнения одного или нескольких видов деятельности по проведению оценки или по

надзору за оценкой.

3.14 Привести в отчете (сообщении) (Report): Включить результаты опенки и вспомогательные материалы в технический отчет об оценке или в сообщение о проблеме.

3.15 Проверить (Check): Вынести **вердикт** посредством простого сравнения. Специальные знания и опыт оценщика не требуются. В формулировке, в которой используется этот глагол, описывается то, что сравнивается.

3.16 Прослеживание (Tracing): Простая однонаправленная связь между двумя совокупностями сущностей, которая показывает, какие сущности в первой совокупности каким сущностям из второй соответствуют.

3.17 Релиз ОО (Release of a TOE): Продукт или система, являющаяся релизом **сертифицированного ОО**, в который вносились изменения.

Примечание - действие выданного ранее сертификата не распространяется на те версии, в которые внесены изменения независимо от причин изменений).

3.18 Руководства ОО (TOE guidance): Руководства, предназначенные для администраторов и пользователей, в том числе руководство по устранению недостатков, процедуры поставки, процедуры установки генерации и запуска.

3.19 Свидетельство оценки (Evolution Evidence): Фактическая поставка для оценки.

3.20 Сертифицированный ОО (Certified TOE): Продукт или система и связанные с ними руководства, являвшиеся объектом оценки, оценка которого завершена, а ЗБ, отчет о подтверждении соответствия и сертификат официально выпущены.

3.21 Система оценки (Scheme): Совокупность правил установленных органом по подтверждению соответствия и определяющих среду оценки, включая критерии и **методику**, требуемые для проведения оценки безопасности ИТ.

3.22 Сообщение о проблеме; СП (Observation Report): Сообщение, документально оформленное оценщиком, в котором он просит разъяснений или указывает на возникшую при оценке проблему.

3.23 Технический отчет об оценке; ТОО (Evaluation Technical Report): Отчет, выпущенный оценщиком и представленный в орган по подтверждению соответствия, в котором приводится **общий вердикт** и его строгое обоснование.

3.24 Шаг оценивания (work unit): Описывает далее неразделимый фрагмент работы по оценке. Каждое действие в МО включает один или несколько шагов оценивания, которые объединены в пределах действия МО согласно содержанию ОК и представлению элемента содержания свидетельств или действий разработчика. Шаги оценивания представлены в МО в том же порядке, что и элементы ОК, из которых они следуют. Шаги оценивания указаны с левой стороны условным обозначением типа ALC_TAT.1-2. В этом обозначении последовательность символов ALC_TAT.1 указывает на компонент ОК (т.е. на подвид деятельности МО), а завершающая цифра (2) указывает, что это второй шаг оценивания в подвиде деятельности ALC_TAT.1.

4 Процесс оценки и связанные с ним задачи

4.1 Введение

Данный раздел содержит краткий обзор процесса оценки и определяет задачи, решаемые оценщиком при проведении оценки.

Каждая оценка ОО проводится в одном и том же порядке и, в общем случае, включает три задачи оценщика: задача получения исходных данных для оценки, задача оформления результатов оценки и подвиды деятельности по оценке.

В этом разделе описаны задача получения исходных данных для оценки и задача оформления результатов оценки, которые связаны с получением свидетельств оценки и

созданием отчетов и сообщений. Каждая задача объединяет подзадачи, применяемые для всех оценок по ОК и являющиеся для них нормативными.

Этот раздел дает только общее представление о подвидах деятельности по оценке, а полностью они описаны в следующих разделах.

В отличие от подвидов деятельности по оценке, выполнение задач получения исходных данных для оценки и оформления результатов оценки не приводит к вердиктам, связанным с ними, поскольку в ОК нет элементов действий оценщика, соответствующих этим задачам.

4.2 Краткий обзор процесса оценки

4.2.1 Цели

Этот подраздел представляет общую модель методологии и определяет:

а) роли[1] и обязанности сторон, вовлеченных в процесс оценки;

б) общую модель оценки.

4.2.2 Обязанности участников оценки

Общая модель определяет следующие роли: заявитель, разработчик, оценщик и орган по подтверждению соответствия.

Заявитель отвечает за запрос и поддержку оценки. Это означает, что заявитель устанавливает различные соглашения по проведению оценки (например, заявку на оценку). Помимо этого, заявитель отвечает за обеспечение оценщика свидетельствами, требуемыми для оценки.

Разработчик предъявляет ОО и отвечает за представление свидетельств, требуемых для оценки (например, по проектной документации, оценке уязвимостей), от имени заявителя.

Оценщик решает задачи, требуемые при проведении оценки: оценщик принимает свидетельства оценки от разработчика от имени заявителя или непосредственно от заявителя, выполняет подвиды деятельности по оценке и представляет результаты оценки органу по подтверждению соответствия.

Орган по подтверждению соответствия устанавливает и поддерживает (сопровождает) систему оценки, контролирует процесс оценки и выдает отчеты о сертификации, а также сертификаты соответствия, основанные на результатах, представленных оценщиками в соответствии с частью 3 ОК.

4.2.3 Взаимоотношения участников оценки

Для предотвращения влияния на оценку негативных воздействий требуется определенное разделение ролей. Это подразумевает, что обязанности, описанные выше, выполняются различными субъектами системы подтверждения соответствия, за исключением возможного совмещения ролей разработчика и заявителя.

Кроме этого, некоторые оценки (например, оценка на ОУД 1) могут не требовать участия разработчика. В этом случае сам заявитель представляет оценщику объект оценки и исходные данные для оценки.

4.2.4 Общая модель оценки[2]

Процесс оценки состоит из выполнения оценщиком задачи получения исходных данных для оценки, задачи оформления результатов оценки и подвидов деятельности по

[1] Роль – это субъект (участник) системы подтверждения соответствия

[2] Общая модель оценки – это этапы (схема) проведения оценки

оценке. Рисунок 4.1 дает общее представление о взаимосвязи этих задач и подвидов деятельности по оценке.

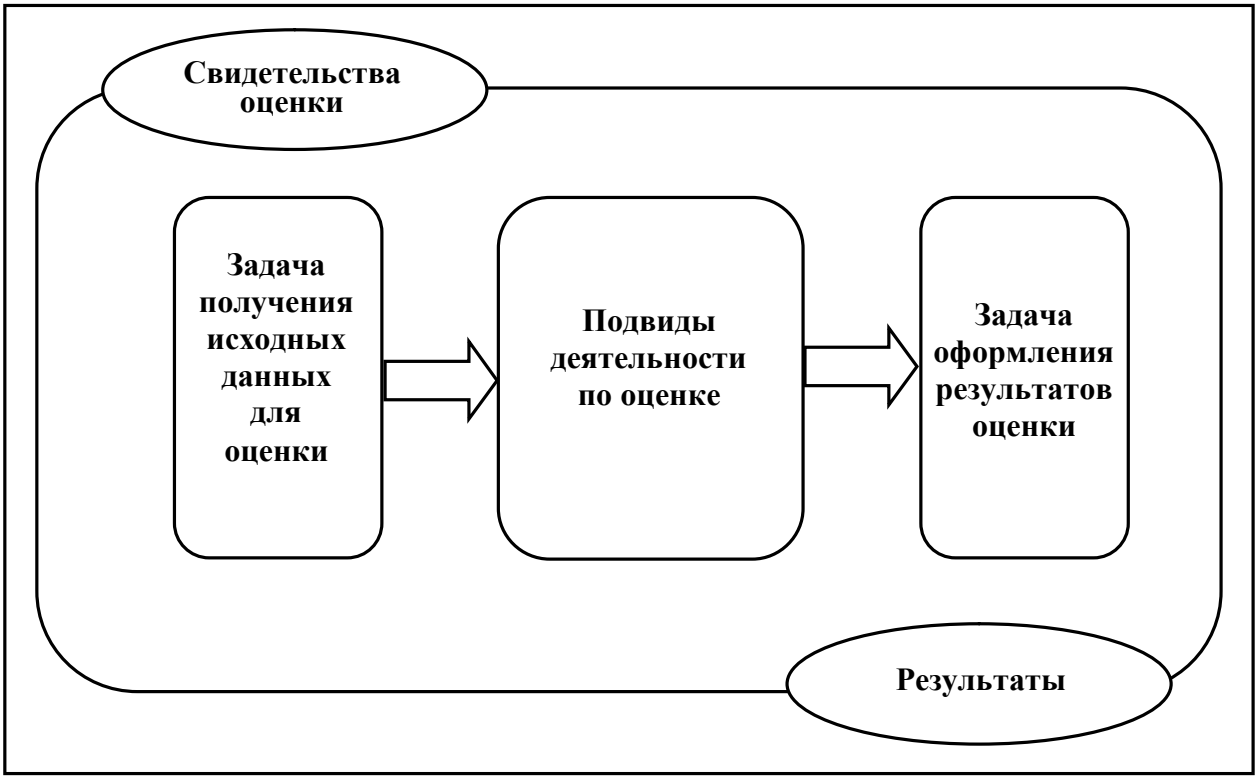


Рисунок 4.1 – Общая модель оценки

Процессу оценки может предшествовать стадия подготовки, когда устанавливается первоначальный контакт между заявителем и оценщиком. Выполняемая работа и взаимодействие различных участников оценки на этой стадии могут варьироваться. Как правило, на этой стадии оценщик анализирует возможность выполнения оценки, оценивая вероятность ее успеха.

4.2.5 Вердикты оценщика

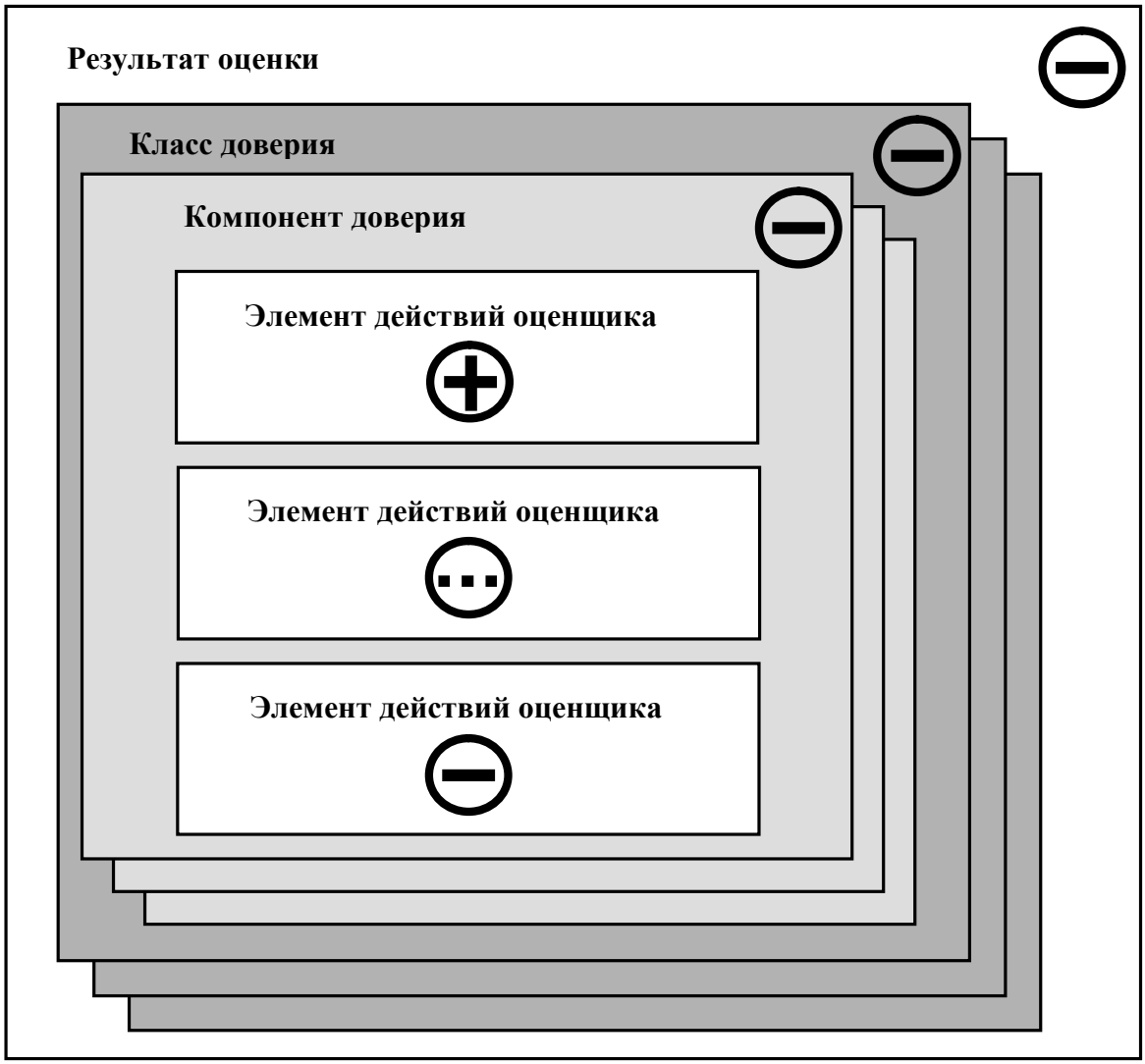
Оценщик выносит вердикт относительно выполнения требований ОК, а не требований МО. Наименьшая структурная единица ОК, по которой выносится вердикт – элемент действий оценщика (явный или подразумеваемый). Вердикт по выполняемому элементу действий оценщика из ОК выносится как результат выполнения соответствующего действия из МО и составляющих его шагов оценивания. В итоге, результат оценки формируется в соответствии с подразделом 5.3 части 1 ОК (СТ РК ГОСТ Р ИСО/МЭК 15408-1).

В МО различаются три взаимоисключающих вида вердикта:

а) условиями *положительного* вердикта являются завершение оценщиком элемента действий оценщика из ОК и определение, что при оценке требования к ОО выполнены. Для элемента условием положительного вердикта является успешное завершение всех шагов оценивания, составляющих соответствующее действие из МО;

б) условиями *отрицательного* вердикта являются завершение оценщиком элемента действий оценщика из ОК и определение, что при оценке требования к ОО не выполнены;

в) все вердикты поначалу *неокончательны* и остаются такими до вынесения *положительного* или *отрицательного* вердикта.



Общий вердикт *положительный* тогда и только тогда, когда все составляющие

Рисунок 4.2 – Пример правила вынесения вердикта

вердикта *положительны*. В примере, показанном на рисунке 4.2, вердикт для одного из элементов действий оценщика *отрицательный*, поэтому вердикты для соответствующего компонента доверия, класса доверия и общий вердикт также *отрицательны*.вердикта *положительны*. В примере, показанном на рисунке 4.2, вердикт для одного из элементов действий оценщика *отрицательный*, поэтому вердикты для соответствующего компонента доверия, класса доверия и общий вердикт также *отрицательны*.

4.3 Задача получения исходных данных для оценки

4.3.1 Цели

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

4.3.2 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 продуктам, которые являются частями ОО. Область применения и требуемое содержание такого свидетельства оценки независимы от уровня контроля разработчиком каждого из продуктов, составляющих ОО. Например, если требуется проект верхнего уровня, то требования семейства ADV_HLD относятся ко всем подсистемам, осуществляющим ФБО. Кроме того, требования доверия, согласно которым требуется выполнение определенных процедур (например, из семейств ACM_CAP и ADO_DEL), также относят к ОО в целом (включая любой продукт другого разработчика).

Оценщику рекомендуется совместно с заявителем представить список требуемых свидетельств оценки. Этот список 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, а 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 могут представляться и предварительные материалы свидетельств в помощь оценщику, например, при предварительной неформальной проверке, но не для использования в качестве основы для вердиктов. Оценщику может быть полезно ознакомиться с предварительными версиями следующих типов свидетельств оценки:

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

б) проектная документация, обеспечивающая оценщику исходную информацию для понимания конструкции ОО;

в) 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 ОК).

4.3.3 Подзадача управления свидетельством оценки

4.3.3.1 Контроль конфигурации

Оценщик ***должен осуществлять*** контроль конфигурации свидетельства оценки.

ОК подразумевают, 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.

4.3.3.2 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:

а) возврат свидетельств оценки;

б) архивирование свидетельств оценки;

в) уничтожение свидетельств оценки.

4.3.3.3 Конфиденциальность

Во время проведения оценки оценщик может получить доступ к конфиденциальной информации заявителя и разработчика (например, информации о конструкции ОО или специальных инструментальных средствах). Система оценки может предъявить к оценщику требования по поддержке 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 последующее использование свидетельств оценки.

4.4 Подвиды деятельности по оценке

При оценке ОО подвиды деятельности зависят от выбранных требований доверия.

Разделы 5–11 организованы единообразно, основываясь на работе, требуемой при оценке.

Данные разделы, соответствующие различным классам ОК, связаны с работой, необходимой для достижения результатов оценки ОО по компонентам ОК.

4.5 Задача оформления результатов оценки

4.5.1 Цели

Цель этого подраздела состоит в описании сообщения о проблеме (СП) и технического отчета об оценке (ТОО). Система оценки может потребовать дополнительные сообщения (отчеты) оценщика типа сообщений (отчетов) об отдельных шагах оценивания или же представление дополнительной информации в СП и ТОО. МО не препятствует включению дополнительной информации в эти сообщения (отчеты), поскольку МО 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 по подтверждению соответствия.

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

а) подготовка СП (если это необходимо при выполнении оценки);

б) подготовка ТОО.

4.5.2 Замечания по применению

В данной версии МО требования обеспечения оценщика свидетельствами для поддержки переоценки или продления действия сертификата (вид деятельности, соответствующий классу поддержки доверия АМА) не сформулированы. Когда заявителю

потребуется информация для переоценки или продления действия сертификата, следует проконсультироваться в системе оценки, в которой проводилась оценка.

4.5.3 Управление выходными материалами оценки

Оценщик представляет органу по подтверждению соответствия ТОО, а также любые СП, имеющиеся в наличии. Требования по управлению отработкой ТОО и СП устанавливаются в соответствии с системой оценки, которая может включать их поставку заявителю или разработчику. ТОО и СП могут включать чувствительную информацию или информацию, которая может нуждаться в изъятии до передачи их заявителю.

4.5.4 Подзадача подготовки СП

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

При отрицательном вердикте оценщик ***должен представить*** СП для отражения результата оценки.

Оценщик может также использовать СП как один из способов выражения потребности в разъяснении.

В любом СП оценщик ***должен привести*** следующее:

а) идентификатор оцениваемого ОО;

б) задача/подвид деятельности по оценке, при выполнении которой/которого проблема была выявлена;

в) суть проблемы;

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

д) организация, ответственная за решение вопроса;

е) рекомендуемые сроки решения;

ж) влияние на оценку отрицательного результата решения проблемы.

Адресаты рассылки СП и процедуры обработки сообщения зависят от характера содержания сообщения и от применяемой системы оценки. Система оценки может различать типы СП или определять дополнительные, различающиеся по требуемой информации и рассылке (например, СП органу по подтверждению соответствия и заявителю).

4.5.5 Подзадача подготовки ТОО

4.5.5.1 Цели

Оценщик ***должен подготовить*** ТОО, чтобы представить строгое техническое обоснование вердиктов.

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

ТОО помогает органу по подтверждению соответствия подтвердить проведение оценки согласно требуемому стандарту, но документированные результаты могут не содержать всю необходимую информацию, так что может понадобиться дополнительная информация, требуемая системой оценки. Этот аспект находится за рамками МО.

4.5.5.2 ТОО при оценке ОО

В данном подпункте приведено минимально необходимое содержание информации,

включаемой в ТОО при оценке ОО. Содержание ТОО показано на рисунке 4.3; этот рисунок может использоваться как образец при построении структурной схемы ТОО.

Рисунок 4.3 – Содержание ТОО при оценке ОО

4.5.5.2.1 Введение

Оценщик ***должен привести в отчете*** идентификаторы системы подтверждения соответствия.

Идентификаторы системы подтверждения соответствия (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 (например, название, дата составления и номер версии) требуются, чтобы определить для органа по подтверждению

соответствия, 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.

4.5.5.2.2 Описание архитектуры ОО

Оценщик ***должен привести в отчете*** высокоуровневое описание ОО и его главных компонентов, основанное на свидетельстве оценки, указанном в семействе доверия ОК "Проект верхнего уровня" (ADV_HLD), где оно применимо.

Назначение этого раздела состоит в указании степени архитектурного разделения главных компонентов. Если в ЗБ нет требования представления проекта верхнего уровня (ADV_HLD), этот раздел не применим.

4.5.5.2.3 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 испытаниях.

Оценщик ***должен привести в отчете*** сведения о любых ограничениях, принятых при оценке, об ограничениях при обработке 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.

4.5.5.2.4 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, определяющего этот вид деятельности, как результат выполнения соответствующего действия МО и составляющих его шагов оценивания.

Обоснование представляет объяснение для вынесения вердикта, сделанного на основе ОК, МО, 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 МО.

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.

4.5.5.2.5 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 5 части 1 ОК и процедурой вынесения вердикта, описанной в 4.2.5 "Вердикты оценщика".

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

4.5.5.2.6 Перечень свидетельств оценки

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

– составитель (например, разработчик, заявитель);

– название;

– уникальная ссылка (например, дата составления и номер версии).

4.5.5.2.7 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 ОК или МО.

4.5.5.2.8 Сообщения о проблемах

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

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

5 Вид деятельности ACM

5.1 Введение

Этот вид деятельности предназначен для определения того, что в процессе уточнения и модификации ОО и связанной с ним информации поддерживаются установленный порядок и управление, и для обеспечения доверия к тому, что ОО и документация, используемые при оценке, именно те, которые подготовлены к распространению.

Вид деятельности ACM включает: "Автоматизацию УК", "Возможности УК" и "Область УК". Подвид деятельности, соответствующий компоненту ACM_AUT.1, состоит из подразумеваемого действия оценщика, основанного на ACM_AUT.1.1D. Отметим, что руководство для ACM_SCP.2 изменено по сравнению с ACM_SCP.1, хотя шаги оценивания не изменились.

5.2 Цели

Целью этого вида деятельности является определение того, что в процессе уточнения и модификации ОО и связанной с ним информации поддерживается установленный порядок и управление конфигурацией.

5.3 Оценка автоматизации УК

5.3.1 Подвид деятельности ACM_AUT.1

5.3.1.1 Цели

Цель данного подвида деятельности – сделать заключение, контролируется ли при поддержке автоматизированных инструментальных средств внесение изменений в представление реализации в целях достижения меньшей восприимчивости системы УК к человеческой ошибке или небрежности.

5.3.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является документация УК.

5.3.1.3 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а) ACM_AUT.1.1E;

б) Подразумеваемое действие оценщика, основанное на ACM_AUT.1.1D.

5.3.1.3.1 Действие ACM_AUT.1.1E

ACM_AUT.1.1C

ACM_AUT.1-1 Оценщик ***должен проверить*** план УК в части описания автоматизированных средств контроля доступа к представлению реализации ОО.

ACM_AUT.1-2 Оценщик ***должен исследовать*** автоматизированные средства контроля доступа, чтобы сделать заключение об их эффективности для предотвращения несанкционированной модификации представленной реализации ОО.

Оценщик просматривает документацию УК, чтобы идентифицировать тех лиц или те роли, которые уполномочены изменять представление реализации ОО. Например, если представление реализации находится под управлением конфигурацией, то доступ к его элементу может быть разрешен только лицу, исполняющему роль интегратора программного обеспечения.

Оценщику следует опробовать автоматизированные средства контроля доступа, чтобы сделать заключение, может ли неуполномоченный пользователь или роль их обойти. Для заключения потребуется несколько базовых тестов.

ACM_AUT.1.2C

ACM_AUT.1-3 Оценщик ***должен проверить*** документацию УК в части автоматизированных средств поддержки генерации ОО из его представления реализации.

На этом шаге оценивания термин *генерация* применяется к процессам, принятым разработчиком для преобразования ОО из его реализации в состояние готовности к поставке конечному потребителю.

Оценщику следует верифицировать наличие автоматизированных процедур поддержки генерации в документации УК.

ACM_AUT.1-4 Оценщик ***должен исследовать*** автоматизированные процедуры генерации, чтобы сделать заключение, могут ли они использоваться для поддержки генерации ОО.

Оценщик делает заключение, что при следовании процедурам генерации будет сгенерирован ОО, отражающий его представление реализации. Потребитель тогда может быть уверен, что версия ОО, поставленная для установки, реализует ПБО, как описано в ЗБ. Например, в случае программного ОО это может включать проверку, что автоматизированные процедуры генерации помогают обеспечить включение в откомпилированный объектный код всех исходных файлов и связанных библиотек, направленных на осуществление ПБО.

Следует отметить, что это требование является только требованием предоставления поддержки. Например, подход, при котором make-файлы Unix помещены под управление

конфигурацией, следует считать достаточным для достижения данной цели, учитывая, что такой подход к автоматизации существенно содействовал бы точной генерации ОО. Автоматизированные процедуры могут способствовать определению надлежащих элементов конфигурации, которые необходимо использовать при генерации ОО.

ACM_AUT.1.3C

ACM_AUT.1-5 Оценщик ***должен проверить,*** что план УК содержит информацию относительно автоматизированных инструментальных средств, используемых в системе УК.

ACM_AUT.1.4C

ACM_AUT.1-6 Оценщик ***должен исследовать*** информацию, относящуюся к автоматизированным инструментальным средствам, представленным в плане УК, чтобы сделать заключение, что в нем описано, как они используются.

Информация, представленная в плане УК, обеспечивает необходимую детализацию для пользователя системы УК, чтобы дать возможность правильно использовать автоматизированные инструментальные средства для сохранения целостности ОО. Например, представленная информация может содержать описание:

а) функциональности, обеспечиваемой инструментальными средствами;

б) того, как эта функциональность используется разработчиком для управления изменениями в представлении реализации;

в) того, как эта функциональность используется разработчиком для поддержки генерации ОО.

5.3.1.3.2 Подразумеваемое действие оценщика

ACM_AUT.1.1D

ACM_AUT.1-7 Оценщик ***должен исследовать*** систему УК, чтобы сделать заключение, что используются те автоматизированные инструментальные средства и процедуры, которые описаны в плане УК.

Этот шаг оценивания может рассматриваться как процесс, дополнительный по отношению к параллельно выполняемому оценщиком исследованию применения системы УК, требуемому ACM_CAP. Оценщик старается получить свидетельство применения инструментальных средств и процедур. Для этого рекомендуется посетить объект разработки, чтобы лично убедиться в функционировании инструментальных средств и процедур, а также провести исследование свидетельств, получаемых при их применении.

Руководство по посещению объектов приведены в подразделе 12.5.

5.4 Оценка возможностей УК

5.4.1 Подвид деятельности ACM_CAP.1

5.4.1.1 Цели

Цель данного подвида деятельности – сделать заключение, четко ли разработчик идентифицировал ОО.

5.4.1.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

а) ЗБ;

б) ОО, пригодный для тестирования;

5.4.1.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ACM_CAP.1.1E.

5.4.1.3.1 Действие ACM_CAP.1.1E

ACM_CAP.1.1C

ACM_CAP.1-1 Оценщик ***должен проверить***, что версия ОО, представленная для оценки, уникально обозначается.

В этом компоненте доверия отсутствуют какие-либо другие требования к разработчику по использованию системы УК, кроме требования уникальной маркировки. В результате оценщик способен верифицировать уникальность версии ОО только путем проверки, что другие доступные для приобретения версии ОО не маркированы так же. При оценке, когда система УК представлена сверх требований ACM_CAP.1, оценщик мог бы подтвердить уникальность маркировки путем проверки списка конфигурации. Свидетельство уникальной маркировки версии ОО, представленной для оценки, может оказаться неполным, если во время оценки исследовалась только одна версия; поэтому оценщику рекомендуется выяснить систему маркирования, которая способна поддерживать уникальные маркировки (например, используя цифры, буквы или даты). Тем не менее, отсутствие какой-либо маркировки обычно будет приводить к отрицательному заключению по этому требованию, пока оценщик не станет уверен в возможности уникальной идентификации ОО.

Оценщику следует стремиться исследовать несколько версий ОО (например, полученных в ходе доработки после обнаружения уязвимости) для проверки, что любые две версии маркированы по-разному.

ACM_CAP.1.2C

ACM_CAP.1-2 Оценщик ***должен проверить***, что ОО, представленный для оценки, помечен его маркировкой.

Оценщику следует удостовериться, что ОО содержит уникальную маркировку, позволяющую отличать разные версии ОО. Этого можно достичь, используя помеченную упаковку или носители, или же метку, отображаемую ОО при функционировании. Это обеспечивает потребителю возможность идентификации ОО (например, в месте приобретения или использования).

ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, программный ОО 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 физического нанесения на нем соответствующего номера.

ACM_CAP.1-3 Оценщик ***должен проверить*** непротиворечивость используемой маркировки ОО.

Если ОО помечен несколько раз, то необходима согласованность меток. Например, следует предусмотреть возможность связать любое помеченное 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 версией руководства, необходимой для эксплуатации данного ОО в соответствии с его ЗБ.

Оценщик также верифицирует, что маркировка ОО согласуется с ЗБ.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

5.4.2 Подвид деятельности ACM_CAP.2

5.4.2.1 Цели

Цель данного подвида деятельности – сделать заключение, четко ли разработчик идентифицировал ОО и связанные с ним элементы конфигурации.

5.4.2.2 Замечания по применению

В этом компоненте вынесение заключения об использовании системы УК

ограничено проверкой идентификации ОО и исследованием списка конфигурации. В ACM_CAP.3 требования расширены сверх этих двух вопросов, и требуется более подробное свидетельство использования системы УК.

5.4.2.3 Исходные данные

Свидетельства оценки для этого подвида деятельности:

а) ЗБ;

б) ОО, пригодный для тестирования;

в) документация управления конфигурацией.

5.4.2.4 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ACM_CAP.2.1E.

5.4.2.4.1 Действие ACM_CAP.2.1E

ACM_CAP.2.1C

ACM_CAP.2-1 Оценщик ***должен проверить***, что версия ОО, представленная для оценки, уникально маркируется.

Оценщику следует использовать систему УК, применяемую разработчиком, для подтверждения уникальности маркировки, проверяя список конфигурации с целью удостовериться, что элементы конфигурации уникально идентифицированы. Свидетельство уникальной маркировки версии ОО, представленной для оценки, может оказаться неполным, если во время оценки исследовалась только одна версия; поэтому оценщику рекомендуется выяснить систему маркирования, которая может поддерживать уникальную маркировку (например, используя цифры, буквы или даты). Тем не менее, отсутствие какой-либо маркировки обычно будет приводить к отрицательному заключению по этому требованию, пока оценщик не станет уверен в возможности уникальной идентификации ОО.

Оценщику следует стремиться исследовать несколько версий ОО (например, полученных в ходе доработки после обнаружения уязвимости) для проверки, что любые две версии маркированы по-разному.

ACM_CAP.2.2C

ACM_CAP.2-2 Оценщик ***должен проверить***, что ОО, представленный для оценки, помечен его маркировкой.

Оценщику следует удостовериться, что ОО содержит уникальную маркировку, позволяющую отличать разные версии ОО. Этого можно достичь, используя помеченную упаковку или носители, или же метку, отображаемую ОО при функционировании. Это обеспечивает потребителю возможность идентификации ОО (например, в месте приобретения или использования).

ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, программный ОО 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 физического нанесения на нем соответствующего номера.

ACM_CAP.2-3 Оценщик ***должен проверить*** непротиворечивость используемой маркировки ОО.

Если ОО помечен несколько раз, то необходима согласованность меток. Например, следует предусмотреть возможность связать любое помеченное 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 версией руководства, необходимой для функционирования данного ОО в соответствии с его ЗБ. Оценщик может использовать

список конфигурации, который является частью представленной документации УК, чтобы верифицировать согласованное использование идентификаторов.

Оценщик также верифицирует, что маркировка ОО согласуется с ЗБ.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

ACM_CAP.2.3C

ACM_CAP.2-4 Оценщик ***должен проверить***, что представленная документация УК включает список конфигурации.

Список конфигурации идентифицирует элементы, находящиеся под управлением конфигурацией.

ACM_CAP.2.4C

ACM_CAP.2-5 Оценщик ***должен исследовать*** список конфигурации, чтобы сделать заключение, что он идентифицирует элементы конфигурации, входящие в состав ОО.

Минимальный состав элементов конфигурации, которые необходимо включить в список конфигурации, задается требованиями семейства ACM_SCP. Если компоненты из ACM_SCP не используются, список конфигурации охватывает тот ОО, который поставляется потребителю. В общем случае в него следует включить документацию пользователя и администратора, а также аппаратные средства, программно-аппаратные средства и программное обеспечение ОО. Аппаратные, программно-аппаратные и программные элементы конфигурации ОО следует контролировать либо на уровне представления реализации, либо на уровне собственно ОО, например, объектного кода или аппаратных средств. Степень детализации элементов конфигурации оставлена на усмотрение разработчика.

ACM_CAP.2.5C

ACM_CAP.2-6 Оценщик ***должен исследовать*** способ идентификации элементов конфигурации, чтобы сделать заключение, что он описывает, каким образом элементы конфигурации идентифицируются уникально.

ACM_CAP.2.6C

ACM_CAP.2-7 Оценщик ***должен проверить***, что список конфигурации уникально идентифицирует каждый элемент конфигурации.

Список конфигурации содержит список элементов конфигурации, которые составляют ОО, вместе с достаточной информацией для уникальной идентификации, какая версия каждого элемента использовалась (обычно номер версии). Использование этого списка позволит оценщику проверить, что во время оценки использовались соответствующие элементы конфигурации и соответствующая версия каждого элемента.

5.4.3 Подвид деятельности ACM_CAP.3

5.4.3.1 Цели

Цель данного подвида деятельности – сделать заключение, четко ли разработчик идентифицировал ОО и связанные с ним элементы конфигурации, а также контролируется ли должным образом возможность изменения этих элементов.

5.4.3.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

а) ЗБ;

б) ОО, пригодный для тестирования;

в) документация управления конфигурацией.

5.4.3.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ACM_CAP.3.1E.

5.4.3.3.1 Действие ACM_CAP.3.1E

ACM_CAP.3.1C

ACM_CAP.3-1 Оценщик ***должен проверить***, что версия ОО, представленная для оценки, уникально маркируется.

Оценщику следует использовать систему УК, применяемую разработчиком, для подтверждения уникальности маркировки, проверяя список конфигурации с целью удостовериться, что элементы конфигурации уникально идентифицированы. Свидетельство уникальной маркировки версии ОО, представленной для оценки, может оказаться неполным, если во время оценки исследовалась только одна версия; поэтому оценщику рекомендуется выяснить систему маркирования, которая может поддерживать уникальную маркировку (например, используя цифры, буквы или даты). Тем не менее, отсутствие какой-либо маркировки обычно будет приводить к отрицательному заключению по этому требованию, пока оценщик не станет уверен в возможности уникальной идентификации ОО.

Оценщику следует стремиться исследовать несколько версий ОО (например, полученных в ходе доработки после обнаружения уязвимости) для проверки, что любые две версии маркированы по-разному.

ACM_CAP.3.2C

ACM_CAP.3-2 Оценщик ***должен проверить***, что ОО, представленный для оценки, помечен его маркировкой.

Оценщику следует удостовериться, что ОО содержит уникальную маркировку, позволяющую отличать разные версии ОО. Этого можно достичь, используя помеченную упаковку или носители, или же метку, отображаемую ОО при функционировании. Это обеспечивает потребителю возможность идентификации ОО (например, в месте приобретения или использования). ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, программный ОО 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 физического нанесения на нем соответствующего номера.

ACM_CAP.3-3 Оценщик ***должен проверить*** непротиворечивость используемой маркировки ОО.

Если ОО помечен несколько раз, то необходима согласованность меток. Например, следует предусмотреть возможность связать любое помеченное 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 версией руководства, необходимой для функционирования данного ОО в соответствии с его ЗБ. Оценщик может использовать список конфигурации, который является частью представленной документации УК, чтобы верифицировать согласованное использование идентификаторов.

Оценщик также верифицирует, что маркировка ОО согласуется с ЗБ.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

ACM_CAP.3.3C

ACM_CAP.3-4 Оценщик ***должен проверить***, что представленная документация УК включает список конфигурации.

Список конфигурации идентифицирует элементы, находящиеся под управлением конфигурацией.

ACM_CAP.3-5 Оценщик ***должен проверить***, что представленная документация УК содержит план УК.

ACM_CAP.3.4C

ACM_CAP.3-6 Оценщик ***должен исследовать*** список конфигурации, чтобы сделать

заключение, что он идентифицирует элементы конфигурации, входящие в состав ОО.

Минимальный состав элементов конфигурации, которые необходимо включить в список конфигурации, задается требованиями семейства ACM_SCP. Если компоненты из ACM_SCP не используются, список конфигурации охватывает тот ОО, который поставляется потребителю. В общем случае в него следует включить документацию пользователя и администратора, а также аппаратные средства, программно-аппаратные средства и программное обеспечение ОО. Аппаратные, программно-аппаратные и программные элементы конфигурации ОО следует контролировать либо на уровне представления реализации, либо на уровне собственно ОО, например, объектного кода или аппаратных средств. Степень детализации элементов конфигурации оставлена на усмотрение разработчика.

ACM_CAP.3.5C

ACM_CAP.3-7 Оценщик ***должен исследовать*** способ идентификации элементов конфигурации, чтобы сделать заключение, что он описывает, каким образом элементы конфигурации идентифицируются уникально.

ACM_CAP.3.6C

ACM_CAP.3-8 Оценщик ***должен проверить***, что список конфигурации уникально идентифицирует каждый элемент конфигурации.

Список конфигурации содержит список элементов конфигурации, которые составляют ОО, вместе с достаточной информацией для уникальной идентификации, какая версия каждого элемента использовалась (обычно номер версии). Использование этого списка позволит оценщику проверить, что во время оценки использовались соответствующие элементы конфигурации и соответствующая версия каждого элемента.

ACM_CAP.3.7C

ACM_CAP.3-9 Оценщик ***должен исследовать*** план УК, чтобы сделать заключение, что он описывает, как система УК используется в целях сохранения целостности элементов конфигурации ОО.

Описания, содержащиеся в плане УК, могут включать:

а) все операции, выполняемые в среде разработки ОО, которые подчинены процедурам управления конфигурацией (например, создание, модификация или удаление элемента конфигурации);

б) роли и обязанности лиц, требуемые для выполнения операций на отдельных элементах конфигурации (для различных типов элементов конфигурации, например, для документации и исходного кода, могут быть идентифицированы различные роли);

в) процедуры, которые используются для обеспечения того, чтобы только уполномоченные лица могли изменять элементы конфигурации;

г) процедуры, которые используются для обеспечения отсутствия проблем параллелизма, возникающих в результате одновременных изменений элементов конфигурации;

д) свидетельство, которое генерируется в результате применения процедур. Например, при изменении элемента конфигурации система УК могла бы 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 могла бы заноситься в журнал аудита произведенных изменений или в протокол контроля изменений;

е) подход к контролю версий и уникальной маркировке версий ОО (охватывающий, например, выпуск исправлений («патчей») для операционных систем и последующее обнаружение их применения).

ACM_CAP.3.8C

ACM_CAP.3-10 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 ACM_CAP.3.9C. Пример выходных материалов мог бы включать формы контроля изменений или формы разрешения доступа к элементам конфигурации.

ACM_CAP.3-11 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 под УК, выполняемых на элементах конфигурации (например, создание, модификация, 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 приведено в подразделе 12.2.

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 убедиться, 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 дополнительного разъяснения понадобится интервью.

Предполагается, что для поддержки этих действий оценщик посетит объект разработки.

Руководство по посещению объектов приведено в подразделе 12.5.

ACM_CAP.3.9C

ACM_CAP.3-12 Оценщик ***должен проверить***, что элементы конфигурации, идентифицированные в списке конфигурации, сопровождаются системой УК.

Система УК, используемая разработчиком, предназначена для сохранения целостности ОО. Оценщику следует проверить, чтобы для каждого типа элементов конфигурации (например, проекта верхнего уровня или модулей исходного кода), содержащегося в списке конфигурации, были примеры свидетельства, сгенерированного процедурами, описанными в плане УК. В этом случае подход к выборке будет зависеть от степени детализации, используемой в системе УК при управлении элементами конфигурации. Если, например, в списке конфигурации идентифицированы 10000 модулей исходного кода, то следует применить стратегию выборки, отличающуюся от применяемой в случае, когда их только пять или всего один. Особое внимание в данном виде деятельности следует уделить тому, чтобы убедиться в правильном функционировании УК, а не обнаружению какой-либо незначительной ошибки.

Руководства по выборке приведено в подразделе 12.2.

ACM_CAP.3.10C

ACM_CAP.3-13 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.

Оценщику разрешается использовать несколько методов для заключения об эффективности мер контроля доступа в УК. Например, оценщик может опробовать меры контроля доступа, чтобы удостовериться, что процедуры нельзя обойти. Оценщику разрешается использовать выходные материалы, сгенерированные процедурами системы УК и уже подвергавшиеся исследованию на шаге оценивания ACM_CAP.3-12. Оценщику может быть также продемонстрирована система УК, чтобы он убедился, что используемые меры контроля доступа выполняются эффективно.

Если компонент семейства ACM_AUT включен в требования доверия, то пригодность любых мер автоматизации управления доступом может быть верифицирована в соответствующем этому компоненту подвиде деятельности.

5.4.4 Подвид деятельности ACM_CAP.4

5.4.4.1 Цели

Цель данного подвида деятельности – сделать заключение, четко ли разработчик идентифицировал ОО и связанные с ним элементы конфигурации, а также контролируется ли должным образом возможность изменения этих элементов.

5.4.4.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

а) ЗБ;

б) ОО, пригодный для тестирования;

в) документация управления конфигурацией.

5.4.4.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ACM_CAP.4.1E.

5.4.4.3.1 Действие ACM_CAP.4.1E

ACM_CAP.4.1C

ACM_CAP.4-1 Оценщик ***должен проверить***, что версия ОО, представленная для оценки, уникально маркируется.

Оценщику следует использовать систему УК, применяемую разработчиком, для подтверждения уникальности маркировки, проверяя список конфигурации с целью удостовериться, что элементы конфигурации уникально идентифицированы. Свидетельство уникальной маркировки версии ОО, представленной для оценки, может оказаться неполным, если во время оценки исследовалась только одна версия; поэтому оценщику рекомендуется выяснить систему маркирования, которая может поддерживать уникальную маркировку (например, используя цифры, буквы или даты). Тем не менее, отсутствие какой-либо маркировки обычно будет приводить к отрицательному заключению по этому требованию, пока оценщик не станет уверен в возможности уникальной идентификации ОО.

Оценщику следует стремиться исследовать несколько версий ОО (например, полученных в ходе доработки после обнаружения уязвимости) для проверки, что любые две версии маркированы по-разному.

ACM_CAP.4.2C

ACM_CAP.4-2 Оценщик ***должен проверить***, что ОО, представленный для оценки, помечен его маркировкой.

Оценщику следует удостовериться, что ОО содержит уникальную маркировку, позволяющую отличать разные версии ОО. Этого можно достичь, используя помеченную

упаковку или носители, или же метку, отображаемую ОО при функционировании. Это обеспечивает потребителю возможность идентификации ОО (например, в месте приобретения или использования).

ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, программный ОО 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 физического нанесения на нем соответствующего номера.

ACM_CAP.4-3 Оценщик должен проверить непротиворечивость используемой маркировки ОО.

Если ОО помечен несколько раз, то необходима согласованность меток. Например, следует предусмотреть возможность связать любое помеченное 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 версией руководства, необходимой для функционирования данного ОО в соответствии с его ЗБ. Оценщик может использовать список конфигурации, который является частью представленной документации УК, чтобы верифицировать согласованное использование идентификаторов.

Оценщик также верифицирует, что маркировка ОО согласуется с ЗБ.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

ACM_CAP.4.3C

ACM_CAP.4-4 Оценщик ***должен проверить***, что представленная документация УК включает список конфигурации.

Список конфигурации идентифицирует элементы, находящиеся под управлением конфигурацией.

ACM_CAP.4-5 Оценщик ***должен проверить***, что представленная документация УК содержит план УК.

ACM_CAP.4-6 Оценщик ***должен проверить***, что представленная документация УК содержит план приемки.

ACM_CAP.4.4C

ACM_CAP.4-7 Оценщик ***должен исследовать*** список конфигурации, чтобы сделать заключение, что он идентифицирует элементы конфигурации, входящие в состав ОО.

Минимальный состав элементов конфигурации, которые необходимо включить в список конфигурации, задается требованиями семейства ACM_SCP. Если компоненты из ACM_SCP не используются, список конфигурации охватывает тот ОО, который поставляется потребителю. В общем случае в него следует включить документацию пользователя и администратора, а также аппаратные средства, программно-аппаратные средства и программное обеспечение ОО. Аппаратные, программно-аппаратные и программные элементы конфигурации ОО следует контролировать либо на уровне представления реализации, либо на уровне собственно ОО, например, объектного кода или аппаратных средств. Степень детализации элементов конфигурации оставлена на усмотрение разработчика.

ACM_CAP.4.5C

ACM_CAP.4-8 Оценщик ***должен исследовать*** способ идентификации элементов конфигурации, чтобы сделать заключение, что он описывает, каким образом элементы конфигурации идентифицируются уникально.

ACM_CAP.4.6C

ACM_CAP.4-9 Оценщик ***должен проверить***, что список конфигурации уникально идентифицирует каждый элемент конфигурации.

Список конфигурации содержит список элементов конфигурации, которые

составляют ОО вместе с достаточной информацией для уникальной идентификации, какая версия каждого элемента использовалась (обычно номер версии). Использование этого списка позволит оценщику проверить, что во время оценки использовались соответствующие элементы конфигурации и соответствующая версия каждого элемента.

ACM_CAP.4.7C

ACM_CAP.4-10 Оценщик ***должен исследовать*** план УК, чтобы сделать заключение, что он описывает, как система УК используется в целях сохранения целостности элементов конфигурации ОО.

Описания, содержащиеся в плане УК, могут включать:

а) все операции, выполняемые в среде разработки ОО, которые подчинены процедурам управления конфигурацией (например, создание, модификация или удаление элемента конфигурации);

б) роли и обязанности лиц, требуемые для выполнения операций на отдельных элементах конфигурации (для различных типов элементов конфигурации, например, для документации и исходного кода, могут быть идентифицированы различные роли);

в) процедуры, которые используются для обеспечения того, чтобы только уполномоченные лица могли изменять элементы конфигурации;

г) процедуры, которые используются для обеспечения отсутствия проблем параллелизма, возникающих в результате одновременных изменений элементов конфигурации;

д) свидетельство, которое генерируется в результате применения процедур. Например, при изменении элемента конфигурации система УК могла бы 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 могла бы заноситься в журнал аудита произведенных изменений или в протокол контроля изменений;

е) подход к контролю версий и уникальной маркировке версий ОО (охватывающий, например, выпуск исправлений («патчей») для операционных систем и последующее обнаружение их применения).

ACM_CAP.4.8C

ACM_CAP.4-11 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 ACM_CAP.4.9C. Пример выходных материалов мог бы включать формы контроля изменений или формы разрешения доступа к элементам конфигурации.

ACM_CAP.4-12 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 под УК, выполняемых на элементах конфигурации (например, создание, модификация, 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 приведено в подразделе 12.2.

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 убедиться, 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 дополнительного разъяснения понадобится интервью.

Предполагается, что для поддержки этих действий оценщик посетит объект разработки.

Руководство по посещению объектов приведено в подразделе 12.5.

ACM_CAP.4.9C

ACM_CAP.4-13 Оценщик ***должен проверить***, что элементы конфигурации, идентифицированные в списке конфигурации, сопровождаются системой УК.

Система УК, используемая разработчиком, предназначена для сохранения целостности ОО. Оценщику следует проверить, чтобы для каждого типа элементов конфигурации (например, проекта верхнего уровня или модулей исходного кода), содержащегося в списке конфигурации, были примеры свидетельства, сгенерированного процедурами, описанными в плане УК. В этом случае подход к выборке будет зависеть от степени детализации, используемой в системе УК при управлении элементами конфигурации. Если, например, в списке конфигурации идентифицированы 10000 модулей исходного кода, то следует применить стратегию выборки, отличающуюся от применяемой в случае, когда их только пять или всего один. Особое внимание в данном виде деятельности следует уделить тому, чтобы убедиться в правильном функционировании УК, а не обнаружению какой-либо незначительной ошибки.

Руководства по выборке приведено в подразделе 12.2.

ACM_CAP.4.10C

ACM_CAP.4-14 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.

Оценщику разрешается использовать несколько методов для заключения об эффективности мер контроля доступа в УК. Например, оценщик может опробовать меры контроля доступа, чтобы удостовериться, что процедуры нельзя обойти. Оценщику разрешается использовать выходные материалы, сгенерированные процедурами системы УК и уже подвергавшиеся исследованию на шаге оценивания ACM_CAP.3-12. Оценщику может быть также продемонстрирована система УК, чтобы он убедился, что используемые меры контроля доступа выполняются эффективно.

Если компонент семейства ACM_AUT включен в требования доверия, тогда пригодность любых мер автоматизации управления доступом может быть верифицирована в соответствующем этому компоненту подвиде деятельности.

ACM_CAP.4.11C

ACM_CAP.4-15 Оценщик ***должен проверить*** документацию УК в части процедур поддержки генерации ОО.

На этом шаге оценивания термин генерация применяется к процессам, принятым разработчиком для преобразования ОО из его реализации в состояние готовности к поставке конечному потребителю.

Оценщик убеждается в существовании процедур поддержки генерации в

документации УК. Процедуры поддержки генерации, предоставленные разработчиком, могут быть автоматизированы, и в таком случае их существование может быть подтверждено в соответствии с элементом ACM_AUT.1.2C.

ACM_CAP.4-16 Оценщик ***должен исследовать*** процедуры генерации ОО, чтобы сделать заключение об их эффективности в обеспечении использования надлежащих элементов конфигурации при генерации ОО.

Оценщик делает заключение, что при следовании процедурам поддержки генерации версия ОО, ожидаемая потребителем (т.е. отвечающая описанию в ЗБ этого ОО и состоящая из надлежащих элементов конфигурации) была бы сгенерирована и поставлена для установки по месту расположения потребителя. Например, для программного ОО это может включать проверку, что процедуры обеспечивают применение всех исходных файлов и связанных библиотек при создании откомпилированного объектного кода.

Оценщику следует иметь в виду, что система УК необязательно обладает способностью генерировать ОО, но ей бы следовало предоставлять поддержку для процесса, который будет способствовать уменьшению вероятности человеческой ошибки.

ACM_CAP.4.12C

ACM_CAP.4-17 Оценщик ***должен исследовать*** процедуры приемки, чтобы сделать заключение, что они описывают критерии приемки, которые необходимо применять к вновь созданным или модифицированным элементам конфигурации.

План приемки описывает процедуры, которые необходимо использовать для обеспечения соответствующего качества составляющих частей ОО до их встраивания в ОО. В плане приемки определяются применяемые процедуры приемки:

а) на каждой стадии "сборки" ОО (например, для модулей, их интеграции, системы в целом);

б) для программных, программно-аппаратных и аппаратных компонентов;

в) для ранее оцененных компонентов.

Описание критериев приемки может содержать идентификацию:

а) обязанности разработчиков или отдельных лиц, ответственных за приемку таких элементов конфигурации;

б) любых критериев приемки, применяемых до принятия элементов конфигурации (например, успешный просмотр документа или успешное тестирование в случае программного обеспечения, программируемого оборудования или аппаратных средств).

5.5 Оценка области УК

5.5.1 Подвид деятельности ACM_SCP.1

5.5.1.1 Цели

Цель данного подвида деятельности – сделать заключение, выполняет ли разработчик, как минимум, управление конфигурацией для представления реализации ОО, проекта, тестов, руководств администратора и пользователя, а также документации УК.

5.5.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является список элементов конфигурации.

5.5.1.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ACM_SCP.1.1E.

5.5.1.3.1 Действие ACM_SCP.1.1E

ACM_SCP.1.1C

ACM_SCP.1-1 Оценщик ***должен проверить***, что список элементов конфигурации содержит совокупность элементов, требуемую ОК.

Список включает следующее:

а) представление реализации ОО (т.е. компоненты или подсистемы, которые составляют ОО). Для полностью программного ОО представление реализации может состоять только из исходного кода; для ОО, который включает аппаратную платформу, представление реализации может ссылаться на комбинацию программных и программно-аппаратных средств и описания аппаратных средств (или ссылки на платформу);

б) свидетельства оценки, требуемые компонентами доверия в ЗБ.

5.5.2 Подвид деятельности ACM_SCP.2

5.5.2.1 Цели

Цель данного подвида деятельности – сделать заключение, выполняет ли разработчик, как

минимум, управление конфигурацией для представления реализации ОО, проекта, тестов, руководств администратора и пользователя, документации УК и недостатков безопасности.

5.5.2.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является список элементов конфигурации.

5.5.2.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ACM_SCP.2.1E.

5.5.2.3.1 Действие ACM_SCP.2.1E

ACM_SCP.2.1C

ACM_SCP.2-1 Оценщик ***должен проверить***, чтобы список элементов конфигурации содержал совокупность элементов, требуемую ОК.

Список включает следующее:

а) представление реализации ОО (т.е. компоненты или подсистемы, которые составляют ОО). Для полностью программного ОО представление реализации может состоять только из исходного кода; для ОО, который включает аппаратную платформу, представление реализации может ссылаться на комбинацию программных и программно-аппаратных средств и описания аппаратных средств (или ссылки на платформу);

б) свидетельства оценки, требуемые компонентами доверия в ЗБ;

в) документацию, используемую для фиксации подробностей сообщенных недостатков безопасности, связанных с реализацией (например, сообщения о состоянии проблем, полученные из ведущейся разработчиком базы данных сообщений о проблемах).

5.5.3 Подвид деятельности ACM_SCP.3

5.5.3.1 Цели

Цель данного подвида деятельности – сделать заключение, выполняет ли разработчик, как минимум, управление конфигурацией для представления реализации ОО, проекта, тестов, руководств администратора и пользователя, документации УК, недостатков безопасности и инструментальных средств разработки.

5.5.3.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является список элементов конфигурации.

5.5.3.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ACM_SCP.3.1E.

5.5.3.3.1 Действие ACM_SCP.3.1E

ACM_SCP.3.1C

ACM_SCP.3-1 Оценщик ***должен проверить***, чтобы список элементов конфигурации содержал совокупность элементов, требуемую ОК.

Список включает следующее:

а) представление реализации ОО (т.е. компоненты или подсистемы, которые составляют ОО). Для полностью программного ОО представление реализации может состоять только из исходного кода; для ОО, который включает аппаратную платформу, представление реализации может ссылаться на комбинацию программных и программно-аппаратных средств и описания аппаратных средств (или ссылки на платформу);

б) свидетельства оценки, требуемые компонентами доверия в ЗБ;

в) документацию, используемую для фиксации подробностей сообщенных недостатков безопасности, связанных с реализацией (например, сообщения о состоянии проблем, полученные из ведущейся разработчиком базы данных сообщений о проблемах);

г) инструментальные средства разработки (например, языки программирования и компиляторы) и относящаяся к ним документация (например, опции компилятора, опции установки/генерации, опции сборки).

6 Вид деятельности ADO

6.1 Введение

Вид деятельности "Поставка и эксплуатация" предназначен для определения достаточности документации по процедурам, используемым для обеспечения установки, генерации и запуска ОО способом, предусмотренным разработчиком, а также для обеспечения поставки ОО без модификаций. Сюда включаются процедуры, выполняемые как при пересылке ОО, так и при установке, генерации и запуске.

Вид деятельности "Поставка и эксплуатация" содержит подвиды деятельности, связанные со следующими компонентами:

а) ADO_DEL.1;

б) ADO_DEL.2;

в) ADO_DEL.3;

г) ADO_IGS.1;

д) ADO_IGS.2.

6.2 Цели

Целью вида деятельности "Поставка и эксплуатация" является определение достаточности

документации по процедурам, используемым для обеспечения установки, генерации и запуска ОО способом, предусмотренным разработчиком.

6.3 Оценка поставки

6.3.1 Подвид деятельности ADO_DEL.1

6.3.1.1 Цели

Цель данного подвида деятельности – сделать заключение, описаны ли в

документации поставки все процедуры, применяемые для поддержания целостности при распространении ОО по объектам использования.

6.3.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является документация поставки.

6.3.1.3 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а) ADO_DEL.1.1E;

б) Подразумеваемое действие оценщика, основанное на ADO_DEL.1.2D.

6.3.1.3.1 Действие ADO_DEL.1.1E

ADO_DEL.1.1C

ADO_DEL.1-1 Оценщик ***должен исследовать*** документацию поставки, чтобы сделать заключение, описаны ли в ней все процедуры, необходимые для поддержания безопасности при распространении версий ОО или его составляющих по объектам использования.

При интерпретации термина *необходимые* требуется учитывать природу ОО и информацию, содержащуюся в ЗБ. Уровень предоставляемой защиты следует соразмерить с предположениями, угрозами, политикой безопасности организации и целями безопасности, идентифицированными в ЗБ. В некоторых случаях они могут не быть явно выражены по отношению к поставке. Оценщику следует сделать заключение о сбалансированности выбранного подхода, при котором поставка не является очевидно слабым звеном по отношению к безопасному в остальном процессу разработки.

В документации поставки следует описать надлежащие процедуры для определения идентификации ОО и поддержания целостности ОО или его составных частей во время пересылки. В документации поставки следует привести процедуры как для распространения физических копий, так и распространения в электронном виде (например, через Internet), где это применимо. Документация поставки относится к ОО в целом, содержащем применяемое программное обеспечение, аппаратные средства, программно-аппаратные средства и документацию.

Акцент на целостности логичен, так как целостность всегда будет иметь значение для поставки ОО. Там, где имеют значение конфиденциальность и доступность, их тоже следует учесть на этом шаге оценивания.

Процедуры поставки следует применять на всех стадиях поставки от среды производства до среды установки (например, при упаковке, хранении и распространении).

Может оказаться приемлемой стандартная коммерческая практика упаковки и поставки. Она предусматривает упаковку в пластиковую пленку, применение ленты безопасности или конверта, скрепленного печатью. Для распространения может быть приемлема общедоступная почта или частная служба доставки.

Термин **"Действие" ("action")** касается элементов действий оценщика из части 3 ОК. Эти действия или сформулированы в явном виде как действия оценщика, или неявно следуют из действий разработчика (подразумеваемые действия оценщика) в рамках компонентов доверия из части 3 ОК.

6.3.1.3.2 Подразумеваемое действие оценщика

ADO_DEL.1.2D

ADO_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 процедур непосредственно, оценщику следует получить и определенную уверенность в их действительном применении. Некоторые возможные подходы перечислены ниже.

а) Посещение объекта (объектов) распространения, где можно наблюдать практическое

применение процедур.

б) Исследование ОО на некоторой стадии поставки или на объекте использования (например, проверка наличия печатей для защиты от вмешательства).

в) Наблюдение за практическим выполнением процесса при получении ОО оценщиком по обычным каналам.

г) Опрос конечных пользователей о том, как им поставлен ОО.

Руководство по посещению объектов приведено в подразделе 12.5.

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 исследование процедур при их применении.

6.3.2 Подвид деятельности ADO_DEL.2

6.3.2.1 Цели

Цель данного подвида деятельности – сделать заключение, описаны ли в документации поставки все процедуры, применяемые для поддержания целостности и обнаружения модификации или подмены ОО при распространении ОО по объектам использования.

6.3.2.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является документация поставки.

6.3.2.3 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а) ADO_DEL.2.1E;

б) Подразумеваемое действие оценщика, основанное на ADO_DEL.2.2D.

6.3.2.3.1 Действие ADO_DEL.2.1E

ADO_DEL.2.1C

ADO_DEL.2-1 Оценщик ***должен исследовать*** документацию поставки, чтобы сделать заключение, описаны ли в ней все процедуры, необходимые для поддержания безопасности при распространении версий ОО или его составляющих по объектам использования.

При интерпретации термина *необходимые* требуется учитывать природу ОО и информацию, содержащуюся в ЗБ. Уровень предоставляемой защиты следует соразмерить с предположениями, угрозами, политикой безопасности организации и целями безопасности, идентифицированными в ЗБ. В некоторых случаях они могут не быть явно выражены по отношению к поставке. Оценщику следует сделать заключение о сбалансированности выбранного подхода, при котором поставка не является очевидно слабым звеном по отношению к безопасному в остальном процессу разработки.

В документации поставки следует описать надлежащие процедуры для определения идентификации ОО и поддержания целостности ОО или его составных частей во время пересылки. В документации поставки следует привести процедуры, как для распространения физических копий, так и распространения в электронном виде (например, через Internet), где это применимо. Документация поставки относится к ОО в целом, содержащем применяемое программное обеспечение, аппаратные средства,

программно-аппаратные средства и документацию.

Акцент на целостности логичен, так как целостность всегда будет иметь значение для поставки ОО. Там, где имеют значение конфиденциальность и доступность, их тоже следует учесть на этом шаге оценивания.

Процедуры поставки следует применять на всех стадиях поставки от среды производства до среды установки (например, при упаковке, хранении и распространении).

Может оказаться приемлемой стандартная коммерческая практика упаковки и поставки. Она предусматривает упаковку в пластиковую пленку, применение ленты безопасности или конверта, скрепленного печатью. Для распространения может быть приемлема общедоступная почта или частная служба доставки.

Выбор процедур поставки зависит от ОО (например, является ли он программным или аппаратным) и целей безопасности. Если процедуры поставки отличаются для различных частей ОО, то для удовлетворения всех целей безопасности потребуется вся совокупность процедур.

ADO_DEL.2.2C

ADO_DEL.2-2 Оценщик ***должен исследовать*** документацию поставки, чтобы сделать заключение, что она содержит описание, каким образом различные процедуры и технические меры обеспечивают обнаружение модификаций или любого расхождения между оригиналом разработчика и версией, полученной на объекте использования.

Для обнаружения вмешательства разработчик может использовать процедуры контрольного суммирования, программные сигнатуры или опечатывание для защиты от вмешательства. Разработчик может также использовать другие процедуры (например, службу регистрации доставки), которые регистрируют имя отправителя и сообщают его получателю.

Технические меры для обнаружения любого расхождения между оригиналом разработчика и версией, полученной на объекте использования, следует описать в процедурах поставки.

ADO_DEL.2.3C

ADO_DEL.2-3 Оценщик ***должен исследовать*** документацию поставки, чтобы сделать заключение, что она содержит описание, каким образом различные механизмы и процедуры позволяют обнаружить попытку подмены отправителя, даже в тех случаях, когда разработчик ничего не отсылал на объект использования.

Это требование может быть выполнено при поставке ОО или его частей (например, доверенным агентом, известным и разработчику, и пользователю). Для программного ОО может быть приемлема цифровая подпись.

Если ОО поставляется в электронном виде по каналам связи, то для поддержки безопасности могут применяться цифровая подпись, контрольные суммы целостности или шифрование.

6.3.2.3.2 Подразумеваемое действие оценщика

ADO_DEL.2.2D

ADO_DEL.2-4 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 процедур непосредственно, оценщику следует получить и определенную уверенность в их действительном применении. Некоторые возможные подходы перечислены ниже.

а) Посещение объекта (объектов) распространения, где может наблюдаться практическое применение процедур.

б) Исследование ОО на некоторой стадии поставки или на объекте использования (например, проверка наличия печатей для защиты от вмешательства).

в) Наблюдение за практическим выполнением процесса при получении ОО оценщиком по обычным каналам.

г) Опрос конечных пользователей о том, как им поставлен ОО.

Руководство по посещению объектов приведено в подразделе 12.5.

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 исследование процедур при их применении.

6.4 Оценка установки, генерации и запуска

6.4.1 Подвид деятельности ADO_IGS.1

6.4.1.1 Цели

Цель данного подвида деятельности – сделать заключение, были ли задокументированы процедуры и шаги для безопасной установки, генерации и запуска ОО и приводят ли они к безопасной конфигурации.

6.4.1.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

а) руководство администратора;

б) процедуры безопасной установки, генерации и запуска;

в) ОО, пригодный для тестирования.

6.4.1.3 Замечания по применению

К рассматриваемым процедурам установки, генерации и запуска относятся все процедуры установки, генерации и запуска, которые необходимы для получения безопасной конфигурации ОО, описанной в ЗБ, независимо от того, выполняются ли они на объекте использования или на объекте разработки.

6.4.1.4 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а) ADO_IGS.1.1E;

б) ADO_IGS.1.2E.

6.4.1.4.1 Действие ADO_IGS.1.1E

ADO_IGS.1.1C

ADO_IGS.1-1 Оценщик ***должен проверить***, чтобы были предоставлены процедуры, необходимые для безопасной установки, генерации и запуска ОО.

Если не ожидается, что процедуры установки, генерации и запуска будут или могут быть повторно применены (например, потому что ОО поставлен в рабочем состоянии), то этот шаг оценивания (или отдельные его части) не применяется.

6.4.1.4.2 Действие ADO_IGS.1.2E

ADO_IGS.1-2 Оценщик ***должен исследовать*** предоставленные процедуры установки, генерации и запуска, чтобы сделать заключение, что они описывают шаги, необходимые для безопасной установки, генерации и запуска ОО.

Если не ожидается, что процедуры установки, генерации и запуска будут или могут быть повторно применены (например, потому что ОО поставлен в рабочем состоянии), то этот шаг оценивания (или отдельные его части) не применяется.

Процедуры установки, генерации и запуска могут предоставлять подробную информацию относительно следующего:

а) изменения конкретных характеристик безопасности элементов, находящихся под управлением ФБО;

б) обработки исключительных ситуаций и проблем;

в) минимально необходимых системных требований, если они имеются, для безопасной установки ОО.

Чтобы подтвердить, что процедуры установки, генерации и запуска приводят к безопасной конфигурации, оценщик может следовать процедурам разработчика или же выполнить те действия, которые, как предполагается, выполнит потребитель для установки, генерации и запуска ОО (если они применимы для данного ОО), используя только поставленные руководства. Этот шаг оценивания может выполняться совместно с шагом оценивания ATE_IND.1-2.

7 Вид деятельности ADV

7.1 Введение

Вид деятельности «Разработка» предназначен для того, чтобы оценить проектную документацию на предмет ее достаточности для понимания, каким образом ФБО предоставляют функции безопасности ОО. Это понимание достигается через исследование последовательно уточняемых описаний проектной документации ФБО. Проектная документация состоит из функциональной спецификации (в которой описываются внешние интерфейсы ОО), проекта верхнего уровня (в котором описывается архитектура ОО в терминах внутренних подсистем) и проекта нижнего уровня (в котором описывается архитектура ОО в терминах внутренних модулей). Дополнительно, имеется описание реализации (описание на уровне исходного кода), внутреннее описание (в котором описывается архитектура и модульность ОО), модель политики безопасности ОО (которая описывает политику безопасности, осуществляемую ОО) и материалы анализа соответствия представлений (в которых представления ОО сопоставляются друг с другом для обеспечения согласованности).

7.2 Цели

Вид деятельности «Разработка» предназначен для того, чтобы оценить проектную документацию на предмет ее достаточности для понимания того, каким образом ФБО предоставляют функции безопасности ОО.

7.3 Замечания по применению

Требования ОК к проектной документации ранжированы по уровню формализации. В отношении вида деятельности «Разработка» в ОК рассматриваются следующие иерархические степени формализации документа: неформальный, полуформальный, формальный. Неформальный документ – это документ, который составлен на естественном языке. Метод оценки не предписывает использовать какой-либо конкретный язык; этот вопрос остается за системой оценки.

7.4 Оценка функциональной спецификации

7.4.1 Подвид деятельности ADV_FSP.1

7.4.1.1 Цели

Цель данного подвида деятельности – сделать заключение, предоставил ли

разработчик адекватное описание функций безопасности ОО, и достаточны ли функции безопасности, предоставляемые ОО, для удовлетворения функциональных требований безопасности, изложенных в ЗБ.

7.4.1.2 Замечания по применению

Неформальная функциональная спецификация включает описание функций безопасности (на уровне, подобном уровню представления краткой спецификации ОО) и описание внешне видимых 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. Если имеются также функции аудита, связанные с обнаружением и регистрацией таких событий, то описание таких 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.

7.4.1.3 Исходные данные

Безусловными свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) функциональная спецификация.

Свидетельствами оценки для этого подвида деятельности, которые требуются для выполнения шагов оценивания, являются:

а) руководство пользователя;

б) руководство администратора.

7.4.1.4 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а) ADV_FSP.1.1E;

б) ADV_FSP.1.2E.

7.4.1.4.1 Действие ADV_FSP.1.1E

ADV_FSP.1.1C

ADV_FSP.1-1 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение, содержит ли она весь необходимый неформальный пояснительный текст.

Если вся функциональная спецификация является неформальной, то рассматриваемый шаг оценивания не применяется.

Для тех частей функциональной спецификации, которые трудны для понимания только на основе полуформального или формального описания, необходимо вспомогательное описание в повествовательной форме (например, чтобы сделать понятными значения всех формальных обозначений).

ADV_FSP.1.2C

ADV_FSP.1-2 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение о ее внутренней непротиворечивости.

Оценщик подтверждает, что функциональная спецификация непротиворечива, удостоверившись, что описание интерфейсов, составляющих ИФБО, согласовано с описанием функций ФБО.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

ADV_FSP.1.3C

ADV_FSP.1-3 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение, определены ли в ней все внешние интерфейсы функций безопасности ОО.

Термин *«внешний»* относится к тому интерфейсу, который является видимым для пользователя. Внешние интерфейсы ОО – это либо непосредственно интерфейсы ФБО, либо интерфейсы не-ФБО-частей ОО. Однако и через не-ФБО-интерфейсы может оказаться возможным доступ к ФБО. Эти внешние интерфейсы, которые прямо или косвенно обращаются к ФБО, совместно составляют интерфейс функций безопасности ОО (ИФБО). На рисунке 7.1 показан ОО, включающий ФБО-части (заштрихованы) и не-ФБО-части (незаштрихованы). Данный ОО имеет три внешних интерфейса: интерфейс *в* – непосредственный интерфейс ФБО; интерфейс *б* – косвенный интерфейс ФБО; интерфейс *а*– интерфейс не-ФБО-частей ОО. Таким образом, интерфейсы *б* и *в* составляют ИФБО.

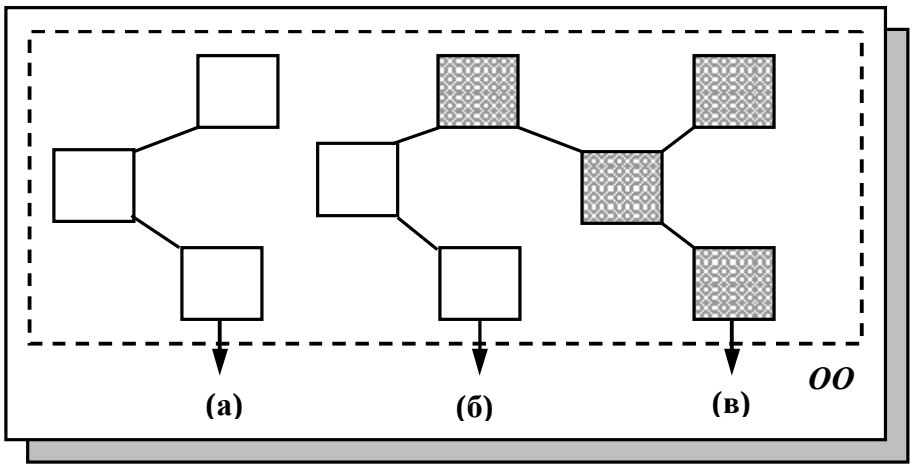


Рисунок 7.1–Интерфейсы ФБО

Следует отметить, что все функции безопасности, отраженные в функциональных требованиях из части 2 ОК (или в компонентах расширения части 2 ОК), будут иметь некоторым образом внешне видимые проявления. И хотя не обязательно все из них являются интерфейсами, через которые могут тестироваться функции безопасности, все они в некотором смысле являются внешне видимыми, а поэтому должны быть включены в функциональную спецификацию.

ADV_FSP.1-4 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение, описаны ли в ней все внешние интерфейсы функций безопасности ОО.

Для ОО, по отношению к которому не имеется угроз, связанных с действиями злонамеренных пользователей (т.е., в его ЗБ справедливо не включены компоненты требований из семейств FPT_PHP, FPT_RVM и FPT_SEP), в функциональной спецификации (и более подробно в описании других представлений ФБО) описываются только интерфейсы ФБО. Отсутствие в ЗБ компонентов требований из семейств FPT_PHP, FPT_RVM и FPT_SEP предполагает, что никакие способы обхода свойств безопасности не рассматриваются, а поэтому не рассматривается какое-либо воздействие, которое другие интерфейсы могли бы оказывать на ФБО.

С другой стороны, если по отношению к ОО имеются угрозы, связанные с действиями злонамеренных пользователей или обходом (т.е., в его ЗБ включены компоненты требований из семейств FPT_PHP, FPT_RVM, и FPT_SEP), то все внешние интерфейсы описываются в функциональной спецификации, но только в объеме, достаточном для понимания их влияния на ФБО: интерфейсы функций безопасности (т.е., интерфейсы *б* и *в* на рисунке 7.1) описываются полностью, в то время как другие

интерфейсы описываются только в объеме, достаточном для понимания того, что ФБО являются недоступными через рассматриваемый интерфейс (т.е., что интерфейс относится к типу *а*, а не типу *б* на рисунке 7.1). Включение компонентов требований из семейств FPT_PHP, FPT_RVM и FPT_SEP предполагает возможность некоторого влияния всех интерфейсов на ФБО. Поскольку каждый внешний интерфейс – это потенциальный интерфейс ФБО, функциональная спецификация должна содержать описание каждого интерфейса с детализацией, достаточной для того, чтобы оценщик мог сделать заключение, является ли интерфейс значимым с точки зрения безопасности.

Некоторые архитектуры позволяют без особого труда предоставить такое описание интерфейсов с достаточной степенью детализации для групп внешних интерфейсов. Например, архитектура на основе ядра такова, что все вызовы операционной системы обрабатываются программами ядра; любые вызовы, которые могли бы нарушить ПБО, должны запрашиваться программой, у которой есть соответствующие привилегии. Все программы, которые выполняются в привилегированном режиме, должны быть включены в функциональную спецификацию. Все программы, внешние по отношению к ядру, которые выполняются в непривилегированном режиме, не способны влиять на ПБО (т.е., такие программы являются интерфейсами типа *а*, а не *б* на рисунке 7.1), а, следовательно, могут не включаться в функциональную спецификацию. Стоит отметить, что, хотя архитектура на основе ядра может ускорить понимание оценщиком описания интерфейсов, такая архитектура не является обязательной.

ADV_FSP.1-5 Оценщик ***должен исследовать*** представление ИФБО, чтобы сделать заключение, адекватно ли и правильно ли в нем описывается режим функционирования ОО на каждом внешнем интерфейсе, включая описание результатов, нештатных ситуаций и сообщений об ошибках.

Оценивая адекватность и правильность представления интерфейсов, оценщик использует функциональную спецификацию, краткую спецификацию ОО из ЗБ, руководства пользователя и администратора, чтобы оценить следующие факторы:

а) Все относящиеся к безопасности, вводимые пользователем параметры (или характеристики этих параметров) должны быть определены. Для полноты должны быть определены параметры, которыми пользователь не управляет напрямую, если они могут использоваться администраторами;

б) Все относящиеся к безопасности режимы функционирования ОО, описанные в рассматриваемых руководствах должны быть отражены при описании семантики в функциональной спецификации. Данное описание должно включать идентификацию режима функционирования ОО в терминах событий и влияния каждого события. Например, если операционная система имеет развитой интерфейс файловой системы и предусматривает различный код ошибок для разных причин неоткрытия файла по запросу (например, доступ запрещен, такого файла не существует, файл используется другим пользователем, пользователю не разрешено открывать файл после 5 часов вечера и т.д.), то в функциональной спецификации должно поясняться, когда файл открывается по запросу, а когда возвращается код ошибки. (Хотя в функциональной спецификации могут быть перечислены все возможные причины ошибок, особой необходимости в такой детализации нет). В описание семантики следует включить описание того, каким образом требования безопасности применяются к интерфейсам (например, является ли использование интерфейса потенциально подвергаемым аудиту событием, и, если да, то какая информация может быть зафиксирована);

в) Описание всех интерфейсов должно быть дано для всех возможных режимов работы. Если для ФБО предусмотрено понятие привилегии, то в описании интерфейса должно быть дано объяснение режимов его функционирования при наличии или отсутствии привилегии;

г) Информация, содержащаяся в описании относящихся к безопасности параметров, и синтаксис интерфейса должны быть непротиворечивы во всей документации.

Верификация изложенного выше осуществляется путем анализа функциональной спецификации и краткой спецификации ОО из ЗБ, а также руководств пользователя и администратора, предоставленных разработчиком. Например, если ОО представляет собой операционную систему и ее аппаратную платформу, то оценщик обычно ищет описание доступных для пользователей программ, описание протоколов, используемых для управления программами, описание доступных для пользователей баз данных, используемых для управления программами, и интерфейсов пользователя (например, команд, интерфейсов прикладных программ), которые применимы к оцениваемому ОО; оценщику также следует удостовериться в наличии описания системы команд процессора.

Данное рассмотрение может быть итерационным вследствие того, что оценщик может не обнаружить неполноту функциональной спецификации до тех пор, пока не исследован проект, исходный код или другое свидетельство на предмет наличия параметров или сообщений об ошибках, которые были пропущены в функциональной спецификации.

ADV_FSP.1.4C

ADV_FSP.1-6 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение о полноте представления ФБО.

Для того, чтобы оценить полноту представления ФБО, оценщик принимает во внимание краткую спецификацию ОО из ЗБ, руководства пользователя и администратора. Ни один из этих документов не должен содержать описание функций безопасности, которые отсутствуют в представлении ФБО в функциональной спецификации.

7.4.1.4.2 Действие ADV_FSP.1.2E

ADV_FSP.1-7 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы делать заключение, является ли она полным отображением функциональных требований безопасности ОО.

Для того чтобы удостовериться, что все функциональные требования безопасности, определенные в ЗБ, охвачены функциональной спецификацией, оценщик может построить отображение краткой спецификации ОО на функциональную спецификацию. Такое отображение могло быть уже представлено самим разработчиком в качестве свидетельства для удовлетворения требований соответствия (ADV_RCR.*), в этом случае оценщику необходимо только верифицировать полноту данного отображения, удостоверившись, что все функциональные требования безопасности отображаются на соответствующие представления ИФБО в функциональной спецификации.

ADV_FSP.1-8 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение, является ли она точным отображением функциональных требований безопасности ОО.

Для каждого интерфейса функции безопасности с конкретными характеристиками в функциональной спецификации должна иметься подробная информация, в точности соответствующая спецификации в ЗБ. Например, если в ЗБ содержатся требования аутентификации пользователя на основе пароля длиной в восемь символов, то ОО должен иметь восьми символьные пароли; если в функциональной спецификации описываются шести символьные пароли фиксированной длины, то функциональная спецификация не является точным отражением требований.

Для каждого интерфейса, описанного в функциональной спецификации, который оказывает влияние на управляемый ресурс, оценщик делает заключение, возвращает ли интерфейс в соответствии с одним из требований безопасности некоторый код ошибки, указывающий на возможный сбой; если код ошибки не возвращается, то оценщик делает заключение, должен ли в этом случае возвращаться код ошибки. Например, операционная

система может представлять интерфейс для ОТКРЫТИЯ управляемого объекта. Описание этого интерфейса может включать код ошибки, который указывает на то, что доступ к объекту не был санкционирован. Если такого кода ошибки не существует, то оценщику следует подтвердить, что это приемлемо (потому что, возможно, посредничество в доступе выполняется при ЧТЕНИИ и ЗАПИСИ, а не при ОТКРЫТИИ).

7.4.2 Подвид деятельности ADV_FSP.2

7.4.2.1 Цели

Цель данного подвида деятельности – сделать заключение, предоставил ли разработчик адекватное описание всех функций безопасности ОО, и достаточны ли функции безопасности, предоставляемые ОО, для удовлетворения функциональных требований безопасности, изложенных в ЗБ.

7.4.2.2 Замечания по применению

Неформальная функциональная спецификация включает описание функций безопасности (на уровне, подобном уровню представления краткой спецификации ОО) и описание внешне видимых 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. Если имеются также функции аудита, связанные с обнаружением и регистрацией таких событий, то описание таких 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.

7.4.2.3 Исходные данные

Безусловными свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) функциональная спецификация.

Свидетельствами оценки для этого подвида деятельности, которые требуются для выполнения шагов оценивания, являются:

а) руководство пользователя;

б) руководство администратора.

7.4.2.4 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а) ADV_FSP.2.1E;

б) ADV_FSP.2.2E.

7.4.2.4.1 Действие ADV_FSP.2.1E

ADV_FSP.2.1C

ADV_FSP.2-1 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение, содержит ли она весь необходимый неформальный пояснительный текст.

Если вся функциональная спецификация является неформальной, то рассматриваемый шаг оценивания не применяется.

Для тех частей функциональной спецификации, которые трудны для понимания только на основе полуформального или формального описания, необходимо вспомогательное описание в повествовательной форме (например, чтобы сделать понятными значения всех формальных обозначений).

ADV_FSP.2.2C

ADV_FSP.2-2 Оценщик ***должен исследовать*** функциональную спецификацию,

чтобы сделать заключение о ее внутренней непротиворечивости.

Оценщик подтверждает функциональную спецификацию, удостоверившись, что описание интерфейсов, составляющих ИФБО, согласовано с описанием функций ФБО.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

ADV_FSP.2.3C

ADV_FSP.2-3 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение, определены ли в ней все внешние интерфейсы функций безопасности ОО.

Термин *«внешний»* относится к тому интерфейсу, который является видимым для пользователя. Внешние интерфейсы ОО – это либо непосредственно интерфейсы ФБО, либо интерфейсы не-ФБО-частей ОО. Однако и через не-ФБО-интерфейсы может оказаться возможным доступ к ФБО. Эти внешние интерфейсы, которые прямо или косвенно обращаются к ФБО, совместно составляют интерфейс функций безопасности ОО (ИФБО). На рисунке 7.2 показан ОО, включающий ФБО-части (заштрихованы) и не-ФБО-части (незаштрихованы). Данный ОО имеет три внешних интерфейса: интерфейс *в* – непосредственный интерфейс ФБО; интерфейс *б* – косвенный интерфейс ФБО; интерфейс *а* – интерфейс не-ФБО-частей ОО. Таким образом, интерфейсы *б* и *в* составляют ИФБО.

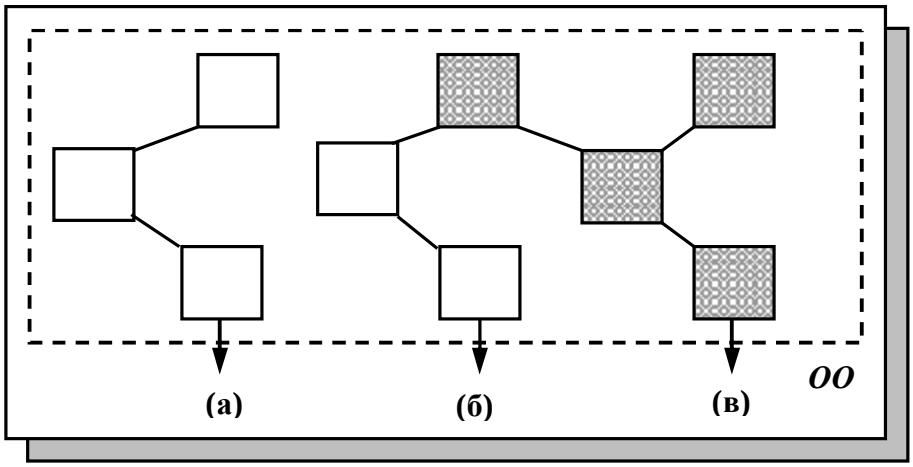


Рисунок 7.2–Интерфейсы ФБО

Следует отметить, что все функции безопасности, отраженные в функциональных требованиях из части 2 ОК (или в компонентах расширения части 2 ОК), будут иметь некоторым образом внешне видимые проявления. И хотя не обязательно все из них являются интерфейсами, через которые могут тестироваться функции безопасности, все они в некотором смысле являются внешне видимыми, а поэтому должны быть включены в функциональную спецификацию.

ADV_FSP.2-4 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение, описаны ли в ней все внешние интерфейсы функций безопасности ОО.

Для ОО, по отношению к которому не имеется угроз, связанных с действиями злонамеренных пользователей (т.е., в ЗБ справедливо не включены компоненты требований из семейств FPT_PHP, FPT_RVM и FPT_SEP), в функциональной спецификации (и более подробно в описании других представлений ФБО) описываются только интерфейсы ФБО. Отсутствие в ЗБ компонентов требований из семейств FPT_PHP, FPT_RVM и FPT_SEP предполагает, что никакие способы обхода свойств безопасности не рассматриваются; поэтому не рассматривается какое-либо влияние, которое другие интерфейсы могли бы оказывать на ФБО.

С другой стороны, если по отношению к ОО имеются угрозы, связанные с действиями злонамеренных пользователей или обходом (т.е., в ЗБ включены компоненты требований из семейств FPT_PHP, FPT_RVM, и FPT_SEP), то все внешние интерфейсы описываются в функциональной спецификации, но только в объеме, достаточном для понимания их влияния на ФБО: интерфейсы функций безопасности (т.е., интерфейсы *б* и *в* на рисунке 7.2) описываются полностью, в то время как другие интерфейсы описываются только в объеме, достаточном для понимания того, что ФБО является недоступным через рассматриваемый интерфейс (т.е., что интерфейс относится к типу *а*, а не типу *б* на рисунке 7.2). Включение компонентов требований из семейств FPT_PHP, FPT_RVM и FPT_SEP предполагает возможность некоторого влияния всех интерфейсов на ФБО. Поскольку каждый внешний интерфейс – это потенциальный интерфейс ФБО, функциональная спецификация должна содержать описание каждого интерфейса с детализацией, достаточной для того, чтобы оценщик мог сделать заключение, является ли интерфейс значимым с точки зрения безопасности.

Некоторые архитектуры позволяют без особого труда предоставить такое описание интерфейсов с достаточной степенью детализации для групп внешних интерфейсов. Например, архитектура на основе ядра такова, что все вызовы операционной системы обрабатываются программами ядра; любые вызовы, которые могли бы нарушить ПБО, должны запрашиваться программой, у которой есть соответствующие привилегии. Все программы, которые выполняются в привилегированном режиме, должны быть включены в функциональную спецификацию. Все программы, внешние по отношению к ядру, которые выполняются в непривилегированном режиме, не способны влиять на ПБО (т.е., такие программы являются интерфейсами типа *а*, а не *б* на рисунке 7.2), а, следовательно, могут не включаться в функциональную спецификацию. Стоит отметить, что, хотя архитектура на основе ядра может ускорить понимание оценщиком описания интерфейсов, такая архитектура не является обязательной.

ADV_FSP.2-5 Оценщик ***должен исследовать*** представление ИФБО, чтобы сделать заключение, адекватно ли и правильно ли в нем описывается в целом режим функционирования ОО на каждом внешнем интерфейсе, включая описание результатов, нештатных ситуаций и сообщений об ошибках.

Оценивая адекватность и правильность представления интерфейсов, оценщик использует функциональную спецификацию, краткую спецификацию ОО из ЗБ, руководства пользователя и администратора, чтобы оценить следующие факторы:

а) Должны быть определены все относящиеся к безопасности вводимые пользователем параметры (или характеристика этих параметров). Для полноты должны быть определены параметры, которыми пользователь не управляет напрямую, если они могут использоваться администраторами.

б) Все относящиеся к безопасности режимы функционирования ОО, описанные в рассматриваемых руководствах должны быть отражены при описании семантики в функциональной спецификации. Данное описание должно включать идентификацию режима функционирования ОО в терминах событий и влияния каждого события. Например, если операционная система имеет развитой интерфейс файловой системы и предусматривает различный код ошибок для разных причин неоткрытия файла по запросу, то в функциональной спецификации должно поясняться, когда файл открывается по запросу, а когда запрос отклоняется с перечислением причин, почему запрос на открытие файла может быть отклонен (например, доступ запрещен, такого файла не существует, файл используется другим пользователем, пользователю не разрешено открывать файл после 5 часов вечера и т.д.).

Простого пояснения в функциональной спецификации того, когда файл открывается по запросу, а когда возвращается код ошибки, было бы недостаточно. В описание

семантики следует включить описание того, каким образом требования безопасности применяются к интерфейсам (например, является ли использование интерфейса потенциально подвергаемым аудиту событием, и, если да, то какая информация может быть зафиксирована).

в) Описание всех интерфейсов должно быть дано для всех возможных режимов работы. Если для ФБО предусмотрено понятие привилегии, то в описании интерфейса должно быть дано объяснение режимов его функционирования при наличии или отсутствии привилегии.

г) Информация, содержащаяся в описании относящихся к безопасности параметров, и синтаксис интерфейса должны быть непротиворечивы во всей документации.

Верификация изложенного выше осуществляется путем анализа функциональной спецификации и краткой спецификации ОО из ЗБ, а также руководств пользователя и администратора, предоставленных разработчиком. Например, если ОО представляет собой операционную систему и ее аппаратную платформу, то оценщик обычно ищет описание доступных для пользователей программ, описание протоколов, используемых для управления программами, описание доступных для пользователей баз данных, используемых для управления программами, и интерфейсов пользователя (например, команд, интерфейсов прикладных программ), которые применимы к оцениваемому ОО; оценщику также следует удостовериться в наличии описания системы команд процессора.

Данное рассмотрение может быть итерационным вследствие того, что оценщик может не обнаружить неполноту функциональной спецификации до тех пор, пока не исследован проект, исходный код или другое свидетельство на предмет наличия параметров или сообщений об ошибках, которые были пропущены в функциональной спецификации.

ADV_FSP.2.4C

ADV_FSP.2-6 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение о полноте представления ФБО.

Для того чтобы оценить полноту представления ФБО, оценщик принимает во внимание краткую спецификацию ОО из ЗБ, руководства пользователя и администратора. Ни один из этих документов не должен содержать описание функций безопасности, которые отсутствуют в представлении ФБО в функциональной спецификации.

ADV_FSP.2.5C

ADV_FSP.2-7 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение, содержит ли она убедительную аргументацию, что ФБО полностью представлены в функциональной спецификации.

Оценщик делает заключение о наличии убедительной аргументации, что нет таких интерфейсов ИФБО, описание которых отсутствовало бы в функциональной спецификации. Аргументация может включать описание процедуры или методологии, которую использовал разработчик для того, чтобы удостовериться в охвате всех внешних интерфейсов. Данная аргументация окажется недостаточной, если, например, оценщик обнаружит в другом свидетельстве оценки отсутствующие в функциональной спецификации описания команд, параметров, сообщений об ошибках или других интерфейсов ФБО.

7.4.2.4.2 Действие ADV_FSP.2.2E

ADV_FSP.2-8 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение, является ли она полным отображением функциональных требований безопасности ОО.

Для того чтобы удостовериться, что все функциональные требования безопасности, определенные в ЗБ, охвачены функциональной спецификацией, оценщик может построить отображение краткой спецификации ОО на функциональную спецификацию. Такое

отображение могло быть уже представлено самим разработчиком в качестве свидетельства для удовлетворения требований соответствия (ADV_RCR.*), в этом случае оценщику необходимо только верифицировать полноту данного отображения, удостоверившись, что все функциональные требования безопасности отображаются на соответствующие представления ИФБО в функциональной спецификации.

ADV_FSP.2-9 Оценщик ***должен исследовать*** функциональную спецификацию, чтобы сделать заключение, является ли она точным отображением функциональных требований безопасности ОО.

Для каждого интерфейса функции безопасности с конкретными характеристиками в функциональной спецификации должна иметься подробная информация, в точности соответствующая спецификации в ЗБ. Например, если в ЗБ содержатся требования аутентификации пользователя на основе пароля длиной в восемь символов, то ОО должен иметь восьми символьные пароли; если в функциональной спецификации описываются шести символьные пароли фиксированной длины, то функциональная спецификация не является точным отражением требований.

Для каждого интерфейса, описанного в функциональной спецификации, который оказывает влияние на управляемый ресурс, оценщик делает заключение, возвращает ли интерфейс некоторый код ошибки (свидетельствующий о возможном отказе) в соответствии с одним из требований безопасности; если код ошибки не возвращается, то оценщик делает заключение, должен ли в этом случае возвращаться код ошибки. Например, операционная система может представлять интерфейс для ОТКРЫТИЯ управляемого объекта. Описание этого интерфейса может включать код ошибки, который указывает на то, что доступ к объекту не был санкционирован. Если такого кода ошибки не существует, то оценщику следует подтвердить, что это приемлемо (потому что, возможно, посредничество в доступе выполняется при ЧТЕНИИ и ЗАПИСИ, а не при ОТКРЫТИИ).

7.5 Оценка проекта верхнего уровня

7.5.1 Подвид деятельности ADV_HLD.1

7.5.1.1 Цели

Цель данного подвида деятельности – сделать заключение, дано ли в проекте верхнего уровня описание ФБО в терминах основных структурных единиц (т.е., подсистем), и является ли проект верхнего уровня корректной реализацией функциональной спецификации.

7.5.1.2 Замечания по применению

Неформальный проект верхнего уровня выражается в терминах последовательностей действий, которые происходят в каждой подсистеме в ответ на инициирующее воздействие на ее интерфейсе. Например, межсетевой экран может состоять из подсистем фильтрации пакетов, удаленного администрирования, аудита, фильтрации на уровне соединения. Проект верхнего уровня межсетевого экрана обычно включает описание предпринимаемых действий, а именно того, какие действия предпринимает каждая подсистема, когда входящий пакет приходит на межсетевой экран.

7.5.1.3 Исходные данные

Безусловными свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) проект верхнего уровня

Свидетельством оценки для этого подвида деятельности, обусловленным зависимостями из ОК, является функциональная спецификация.

7.5.1.4 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а) ADV_HLD.1.1E;
б) ADV_HLD.1.2E.

7.5.1.4.1 Действие ADV_HLD.1.1E

ADV_HLD.1.1C

ADV_HLD.1-1 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы сделать заключение, содержит ли он весь необходимый неформальный пояснительный текст.

Если весь проект верхнего уровня является неформальным, то рассматриваемый шаг оценивания не применяется.

Для тех частей проекта верхнего уровня, которые трудны для понимания только на основе полуформального или формального описания, необходимо вспомогательное описание в повествовательной форме (например, чтобы сделать понятными значения всех формальных обозначений).

ADV_HLD.1.2C

ADV_HLD.1-2 Оценщик ***должен исследовать*** представление проекта верхнего уровня, чтобы сделать заключение о его внутренней непротиворечивости.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

Оценщик подтверждает правильность спецификаций интерфейсов конкретной подсистемы, удостоверившись, что спецификации интерфейсов согласованы с описанием предназначения данной подсистемы.

ADV_HLD.1.3C

ADV_HLD.1-3 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы сделать заключение, описана ли структура ФБО в терминах подсистем.

Применительно к проекту верхнего уровня термин *подсистема* относится к большим связанным единицам (таким, как управление памятью, управление файлами, управление процессами). Разбиение проекта на базовые функциональные области способствует пониманию проекта.

Основная цель исследования проекта верхнего уровня состоит в том, чтобы помочь оценщику в понимании ОО. Вариант выделения разработчиком подсистем и группирования функций безопасности в рамках каждой подсистемы является важным аспектом полезности проекта верхнего уровня для понимания предполагаемого функционирования ОО. В качестве части данного шага оценивания оценщику следует выполнить оценку приемлемости числа подсистем, представленных разработчиком, а также варианта группирования функций в рамках подсистем. Оценщику следует удостовериться, что декомпозиция ФБО на подсистемы достаточна для того, чтобы он получил высокоуровневое понимание того, каким образом обеспечиваются функциональные возможности ФБО.

Подсистемы, используемые для описания проекта верхнего уровня, не обязательно должны называться «подсистемами», но они должны представлять подобный уровень декомпозиции. Например, при декомпозиции проекта могут использоваться понятия «слои» или «менеджеры».

ADV_HLD.1.4C

ADV_HLD.1-4 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы сделать заключение, содержит ли он описание функциональных возможностей безопасности каждой подсистемы.

Описание режима безопасного функционирования подсистемы – это описание того, что делает подсистема. Оно должно включать описание любых действий, выполнение которых может быть предписано подсистеме, с учетом ее функций и результатов влияния, которое может оказать подсистема на безопасное состояние ОО (например, изменения в субъектах, объектах, базах данных безопасности).

ADV_HLD.1.5C

ADV_HLD.1-5 Оценщик ***должен проверить*** проект верхнего уровня, чтобы сделать заключение, идентифицированы ли в нем все аппаратные, программно-аппаратные и программные средства, требуемые ФБО.

Если ЗБ не содержит требования безопасности для среды ИТ, то рассматриваемый шаг оценивания не применяется.

Если ЗБ содержит необязательное изложение требований безопасности для среды ИТ, оценщик сравнивает перечень требуемых ФБО аппаратных, программно-аппаратных и программных средств, изложенный в проекте верхнего уровня, и изложение требований безопасности для среды ИТ, чтобы сделать заключение, согласованы ли они. Информация в ЗБ характеризует базовую абстрактную машину, на базе которой будет функционировать ОО.

Если проект верхнего уровня включает требования безопасности для среды ИТ, которые не включены в ЗБ, или если они отличаются от требований, включенных в ЗБ, такая несогласованность учитывается оценщиком при выполнении действия ADV_HLD.1.2E.

ADV_HLD.1-6 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы сделать заключение, включает ли он представление функций, предоставляемых поддерживающими механизмами защиты, реализованными в базовых аппаратных, программно-аппаратных и программных средствах.

Если ЗБ не содержит требования безопасности для среды ИТ, то рассматриваемый шаг оценивания не применяется.

Представление функций, предоставляемых базовой абстрактной машиной, на базе которой функционирует ОО, не обязательно должно быть на том же уровне детализации, что и представление функций, являющихся частью ФБО. Представление должно объяснять, каким образом ОО использует функции, предоставленные для поддержки целей безопасности для ОО аппаратными, программно-аппаратными и программными средствами, реализующими требования безопасности для среды ИТ, от которой зависит ОО.

Изложение требований безопасности для среды ИТ может быть абстрактным, особенно, если предполагается возможность их удовлетворения множеством различных комбинаций аппаратных, программно-аппаратных и/или программных средств. В качестве части вида деятельности «Тестирование», когда оценщику предоставляется, по крайней мере, один образец базовой машины, для которой утверждается, что она удовлетворяет требованиям безопасности для среды ИТ, оценщик может сделать заключение, предоставляет ли она необходимые функции безопасности для ОО. Это заключение оценщика не требует тестирования или анализа базовой машины; оно является только заключением, что функции, которые, как предполагается, предоставляются базовой машиной, действительно имеются.

ADV_HLD.1.6C

ADV_HLD.1-7 Оценщик ***должен проверить***, идентифицированы ли в проекте верхнего уровня все интерфейсы подсистем ФБО.

Проект верхнего уровня должен включать для каждой подсистемы имя каждой из ее точек входа.

ADV_HLD.1.7C

ADV_HLD.1-8 Оценщик ***должен проверить***, идентифицировано ли в проекте верхнего уровня, какие интерфейсы подсистем ФБО являются внешне видимыми.

7.5.1.4.2 Действие ADV_HLD.1.2E

ADV_HLD.1-9 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы сделать заключение, является ли он точным отображением функциональных требований

безопасности ОО.

Оценщик анализирует проект верхнего уровня для каждой функции безопасности ОО, чтобы удостовериться, что функция безопасности ОО описана точно. Оценщик также удостоверяется, что функция не имеет зависимостей, которые не были включены в проект верхнего уровня.

Оценщик также анализирует требования безопасности для среды ИТ, изложенные в ЗБ и проекте верхнего уровня, чтобы удостовериться, что они согласованы. Например, если в ЗБ включены функциональные требования безопасности ОО по хранению журнала аудита, а в проекте верхнего уровня изложено, что хранение журнала аудита обеспечивается средой ИТ, то проект верхнего уровня не является точным отображением функциональных требований безопасности ОО.

DV_HLD.1-10 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы сделать заключение, является ли он полным отображением функциональных требований безопасности ОО.

Для того чтобы удостовериться, что все функциональные требования безопасности, определенные в ЗБ, охвачены проектом верхнего уровня, оценщик может построить отображение функциональных требований безопасности ОО на проект верхнего уровня.

7.5.2 Подвид деятельности ADV_HLD.2

7.5.2.1 Цели

Цель данного подвида деятельности – сделать заключение, дано ли в проекте верхнего уровня описание ФБО в терминах основных структурных единиц (т.е., подсистем), описание интерфейсов этих структурных единиц, и является ли проект верхнего уровня корректной реализацией функциональной спецификации.

7.5.2.2 Замечания по применению

Неформальный проект верхнего уровня выражается в терминах последовательностей действий, которые происходят в каждой подсистеме в ответ на инициирующее воздействие на ее интерфейсе. Например, межсетевой экран может состоять из подсистем фильтрации пакетов, удаленного администрирования, аудита, фильтрации на уровне соединения. Проект верхнего уровня межсетевого экрана обычно включает описание предпринимаемых действий, а именно того, какие действия предпринимает каждая подсистема, когда входящий пакет приходит на межсетевой экран.

7.5.2.3 Исходные данные

Безусловными свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) проект верхнего уровня.

Свидетельством оценки для этого подвида деятельности, обусловленным зависимостями из ОК, является функциональная спецификация.

7.5.2.4 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а) ADV_HLD.2.1E;

б) ADV_HLD.2.2E.

7.5.2.4.1 Действие ADV_HLD.2.1E

ADV_HLD.2.1C

ADV_HLD.2-1 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы сделать заключение, содержит ли он весь необходимый неформальный пояснительный текст.

Если весь проект верхнего уровня является неформальным, то рассматриваемый шаг оценивания не применяется.

Для тех частей проекта верхнего уровня, которые трудны для понимания только на основе полуформального или формального описания, необходимо вспомогательное описание в повествовательной форме (например, чтобы сделать понятными значения всех формальных обозначений).

ADV_HLD.2.2C

ADV_HLD.2-2 Оценщик ***должен исследовать*** представление проекта верхнего уровня, чтобы сделать заключение о его внутренней непротиворечивости.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

Оценщик подтверждает правильность спецификаций интерфейсов конкретной подсистемы, удостоверившись, что спецификации интерфейсов согласованы с описанием предназначения данной подсистемы.

ADV_HLD.2.3C

ADV_HLD.2-3 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы сделать заключение, описана ли структура ФБО в терминах подсистем.

Применительно к проекту верхнего уровня, термин *подсистема* относится к большим связанным единицам (таким, как управление памятью, управление файлами, управление процессами). Разбиение проекта на базовые функциональные области способствует пониманию проекта.

Основная цель исследования проекта верхнего уровня состоит в том, чтобы помочь оценщику в понимании ОО. Вариант выделения разработчиком подсистем и группирования функций безопасности в рамках каждой подсистемы является важным аспектом полезности проекта верхнего уровня для понимания предполагаемого функционирования ОО. В качестве части данного шага оценивания оценщику следует выполнить оценку приемлемости числа подсистем, представленных разработчиком, а также варианта группирования функций в рамках подсистем. Оценщику следует удостовериться, что декомпозиция ФБО на подсистемы достаточна для того, чтобы он получил высокоуровневое понимание того, каким образом обеспечиваются функциональные возможности ФБО.

Подсистемы, используемые для описания проекта верхнего уровня, не обязательно должны называться «подсистемами», но они должны представлять подобный уровень декомпозиции. Например, при декомпозиции проекта могут использоваться понятия «слои» или «менеджеры».

Между вариантом выделения подсистем разработчиком и масштабами проводимого оценщиком анализа могут существовать некоторые взаимозависимости. Эти взаимозависимости рассматриваются ниже при описании шага оценивания ADV_HLD.2-10.

ADV_HLD.2.4C

ADV_HLD.2-4 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы сделать заключение, содержит ли он описание функциональных возможностей безопасности каждой подсистемы.

Описание режима безопасного функционирования подсистемы – это описание того, что делает подсистема. Оно должно включать описание любых действий, выполнение которых может быть предписано подсистеме, учитывая ее функции и влияние, которое может оказать подсистема на состояние безопасности ОО (например, изменения в субъектах, объектах, базах данных безопасности).

ADV_HLD.2.5C

ADV_HLD.2-5 Оценщик ***должен проверить*** проект верхнего уровня, чтобы сделать заключение, идентифицированы ли в нем все аппаратные, программно-аппаратные и программные средства, требуемые ФБО.

Если ЗБ не содержит требования безопасности для среды ИТ, то рассматриваемый

шаг оценивания не применяется.

Если ЗБ содержит необязательное изложение требований безопасности для среды ИТ, оценщик сравнивает перечень требуемых ФБО аппаратных, программно-аппаратных и программных средств, изложенный в проекте верхнего уровня, и изложение требований безопасности для среды ИТ, чтобы сделать заключение, согласованы ли они. Информация в ЗБ характеризует базовую абстрактную машину, на базе которой будет функционировать ОО.

Если проект верхнего уровня включает требования безопасности для среды ИТ, которые не включены в ЗБ, или если они отличаются от требований, включенных в ЗБ, такая несогласованность учитывается оценщиком при выполнении действия ADV_HLD.1.2E.

ADV_HLD.2-6 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы сделать заключение, включает ли он представление функций, предоставляемых поддерживающими механизмами защиты, реализованными в базовых аппаратных, программно-аппаратных и программных средствах.

Если ЗБ не содержит требования безопасности для среды ИТ, то рассматриваемый шаг оценивания не применяется.

Представление функций, предоставляемых базовой абстрактной машиной, на базе которой функционирует ОО, не обязательно должно быть на том же уровне детализации, что и представление функций, являющихся частью ФБО. Представление должно объяснять, каким образом ОО использует функции, предоставленные для поддержки целей безопасности для ОО аппаратными, программно-аппаратными и программными средствами, реализующими требования безопасности для среды ИТ, от которой зависит ОО.

Изложение требований безопасности для среды ИТ может быть абстрактным, особенно, если предполагается возможность их удовлетворения множеством различных комбинаций аппаратных, программно-аппаратных и/или программных средств. В качестве части вида деятельности «Тестирование», когда оценщику предоставляется, по крайней мере, один образец базовой машины, для которой утверждается, что она удовлетворяет требованиям безопасности для среды ИТ, оценщик может сделать заключение, предоставляет ли она необходимые функции безопасности для ОО. Это заключение оценщика не требует тестирования или анализа базовой машины; оно является только заключением, что функции, которые, как предполагается, предоставляются базовой машиной, действительно имеются.

ADV_HLD.2.6C

ADV_HLD.2-7 Оценщик ***должен проверить***, идентифицированы ли в проекте верхнего уровня все интерфейсы подсистем ФБО.

Проект верхнего уровня должен включать для каждой подсистемы имя каждой из ее точек входа.

ADV_HLD.2.7C

ADV_HLD.2-8 Оценщик ***должен проверить***, идентифицировано ли в проекте верхнего уровня, какие интерфейсы подсистем ФБО являются внешне видимыми.

Как изложено в описании шагов оценивания ADV_FSP.1-3 и ADV_FSP.2-3, через внешние интерфейсы (т.е. видимые пользователю) можно прямо или косвенно получить доступ к ФБО. Любой внешний интерфейс, через который можно прямо или косвенно получить доступ к ФБО, идентифицируется в целях проведения данного шага оценивания. Внешние интерфейсы, через которые нельзя получить доступ к ФБО, не обязательно должны быть идентифицированы.

ADV_HLD.2.8C

ADV_HLD.2-9 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы

сделать заключение, содержится ли в нем описание назначения и методов использования всех интерфейсов каждой подсистемы, и дается ли при необходимости подробное описание результатов, нештатных ситуаций и сообщений об ошибках.

Проект верхнего уровня должен содержать описание назначения и методов использования для всех интерфейсов каждой подсистемы. Такое описание может быть дано для одних интерфейсов в общих чертах, а для других – более подробно. При определении необходимого уровня детализации результатов, нештатных ситуаций и сообщений об ошибках оценщику следует учитывать цели данного анализа и методы использования интерфейсов ОО. Например, оценщику нужно понять характер взаимодействия между подсистемами, чтобы обрести уверенность в правильности проекта ОО, и, возможно, быть способным понять это только на основе общего описания некоторых интерфейсов между подсистемами. В частности, внутренние точки входа одной подсистемы, которые не используются любой другой подсистемой, как правило, не требуют подробного описания.

Уровень детализации может также зависеть от подхода к тестированию, принятого для удовлетворения требований из семейства ATE_DPT. Например, при использовании подхода к тестированию, предусматривающего тестирование только через внешние интерфейсы, и подхода к тестированию, предусматривающего тестирование и через внешние и через внутренние интерфейсы подсистем, может потребоваться различный уровень детализации.

Детальное описание, как правило, включает подробную информацию обо всех вводимых и выводимых параметрах, влиянии интерфейса, обо всех нештатных ситуациях и сообщениях об ошибках, которые порождает интерфейс. В случае с внешними интерфейсами, требуемое описание, как правило, включается в функциональную спецификацию, а в проекте верхнего уровня вместо повтора может быть использована ссылка на это описание.

ADV_HLD.2.9C

ADV_HLD.2-10 Оценщик ***должен проверить***, содержится ли в проекте верхнего уровня описание разделения ОО на подсистемы, осуществляющие ПБО, и другие подсистемы.

ФБО включают все те части ОО, на которые возложено осуществление ПБО. Поскольку ФБО включают как функции, которые непосредственно осуществляют ПБО, так и функции, которые, хотя непосредственно и не осуществляют ПБО, но косвенным образом вносят вклад в осуществление ПБО, все подсистемы, осуществляющие ПБО, составляют ФБО. Подсистемы, которые не играют никакой роли в осуществлении ПБО, не являются частью ФБО. Если какая-либо часть подсистемы является частью ФБО, то и вся подсистема является частью ФБО.

Как объяснялось на шаге оценивания ADV_HLD.2-3, вариант выделения разработчиком подсистем и группирования функций безопасности в рамках каждой подсистемы является важным аспектом полезности проекта верхнего уровня для понимания предполагаемого функционирования ОО. Однако вариант группирования ФБО в рамках подсистем также влияет на область действия ФБО, так как подсистема с *какой-либо* функцией, которая прямо или косвенно осуществляет ПБО, является частью ФБО. Хотя цель – обеспечить понимание предполагаемого функционирования ОО – важна, также полезным является ограничение объема ФБО в рамках подсистем в целях сокращения масштабов необходимого анализа. Эти две цели – обеспечение понимания и сокращение масштабов анализа – могут иногда противоречить друг другу. Оценщику следует учитывать это при оценке варианта выделения подсистем.

7.5.2.4.2 Действие ADV_HLD.2.2E

ADV_HLD.2-11 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы

сделать заключение, является ли он точным отображением функциональных требований безопасности ОО.

Оценщик анализирует проект верхнего уровня для каждой функции безопасности ОО, чтобы удостовериться, что функция безопасности ОО описана точно. Оценщик также удостоверяется, что функция не имеет зависимостей, которые не были включены в проект верхнего уровня.

Оценщик также анализирует требования безопасности для среды ИТ, изложенные в ЗБ и проекте верхнего уровня, чтобы удостовериться, что они согласованы. Например, если в ЗБ включены функциональные требования безопасности ОО по хранению журнала аудита, а в проекте верхнего уровня изложено, что хранение журнала аудита обеспечивается средой ИТ, то проект верхнего уровня не является точным отображением функциональных требований безопасности ОО.

Оценщику следует подтвердить правильность спецификаций интерфейсов подсистем, удостоверившись, что спецификации интерфейсов согласуются с описанием назначения подсистем.

ADV_HLD.2-12 Оценщик ***должен исследовать*** проект верхнего уровня, чтобы сделать заключение, является ли он полным отображением функциональных требований безопасности ОО.

Для того чтобы удостовериться, что все функциональные требования безопасности, определенные в ЗБ, охвачены проектом верхнего уровня, оценщик может построить отображение функциональных требований безопасности ОО на проект верхнего уровня.

7.6 Оценка реализации

7.6.1 Подвид деятельности ADV_IMP.1

7.6.1.1 Цели

Цель данного подвида деятельности – сделать заключение, является ли представление реализации достаточным для удовлетворения функциональных требований ЗБ и является ли оно корректной реализацией проекта нижнего уровня.

7.6.1.2 Исходные данные

Безусловными свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) подмножество представления реализации.

Свидетельством оценки для этого подвида деятельности, обусловленным зависимостями из ОК, является проект нижнего уровня.

7.6.1.3 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а) ADV_IMP.1.1E;

б) ADV_IMP.1.2E.

7.6.1.3.1 Действие ADV_IMP.1.1E

ADV_IMP.1.1C

ADV_IMP.1-1 Оценщик ***должен исследовать*** 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.

Данный шаг оценивания требует от оценщика подтвердить, что представление реализации пригодно для анализа. Оценщику следует рассмотреть процесс, необходимый для генерации ФБО из предоставленного представления реализации. Если процесс полностью определен и не требует дальнейших проектных решений (например, требуется

только компиляция исходного кода или построение аппаратных средств на основе чертежей аппаратных средств), то представление реализации можно считать пригодным для анализа.

Любые используемые языки программирования должны быть полностью определены, включая однозначное определение всех операторов, а также опций компилятора, используемых для генерации объектного кода. Заключение об этом может уже быть сделано как часть подвида деятельности ALC_TAT.1, если этот подвид деятельности является частью оценки.

ADV_IMP.1-2 Оценщик ***должен исследовать*** представление реализации, предоставленное разработчиком, чтобы сделать заключение, является ли оно достаточно репрезентативным.

От разработчика требуется предоставить представление реализации только для подмножества ФБО. Если в ПЗ или ЗБ специфицировано некоторое избранное подмножество ФБО, то от разработчика также требуется предоставить представление реализации именно для этого специфицированного подмножества ФБО. Разработчик может отобрать и предложить оценщику представление реализации для некоторого исходного подмножества ФБО, но оценщик может дополнительно потребовать предоставления других частей представления реализации или даже представления реализации для других подмножеств ФБО.

Оценщик делает заключение о достаточности и приемлемости подмножества ФБО, используя принципы осуществления выборки.

Руководство по выборке приведено в подразделе 12.2.

Делая заключение о приемлемости подмножества ФБО, оценщик решает, пригодно ли оно для понимания и обретения уверенности в правильности реализации механизмов ФБО.

Делая данное заключение, оценщику следует рассмотреть различные способы представления, используемые разработчиком, с тем, чтобы оценщик был удовлетворен репрезентативностью выбранного подмножества.

Например, для ОО, который реализован в виде традиционной операционной системы, выбранное подмножество исходного кода должно включать выборку исходного кода для ядра, а также выборку за пределами ядра – для команд и прикладных программ. Если известно, что часть исходного кода создана сторонними организациями-разработчиками, выбранное подмножество должно включать выборки исходного кода для каждой сторонней организации-создателя исходного кода. Если исходный код представления реализации включает различные виды языков программирования, то подмножество должно содержать выборки для каждого языка программирования.

В случае, когда представление реализации содержит чертежи аппаратных средств, в подмножество представления реализации должны быть включены несколько различных частей ОО. Например, для ОО, включающего настольный компьютер, выбранное подмножество должно содержать выборки чертежей для контроллеров ввода-вывода, а также для «материнской» платы компьютера.

Имеются и другие факторы, которые могут оказывать влияние на вынесение заключения о репрезентативности подмножества представления реализации:

а) сложность проекта (если сложность проекта в рамках одного ОО варьируется, то в подмножество представления реализации должно включать какие-либо части высокой сложности);

б) требования системы подтверждения соответствия;

в) результаты других подвидов деятельности по анализу проекта (таких, как результаты шагов оценивания, относящихся к проектам нижнего и верхнего уровней), которые могут указывать на те части ОО, для которых в проекте возможна

неоднозначность;

г) суждение оценщика относительно частей представления реализации, которые могут быть полезными для проводимого оценщиком независимого анализа уязвимостей (подвид деятельности AVA_VLA.2, если этот подвид деятельности является частью оценки).

ADV_IMP.1.2C

ADV_IMP.1-3 Оценщик ***должен исследовать*** представление реализации, чтобы сделать заключение о его внутренней непротиворечивости.

Поскольку от разработчика требуется предоставить только подмножество представления реализации, то данный шаг оценивания требует от оценщика заключения о непротиворечивости только для предоставленного подмножества. Оценщик ищет противоречия, сравнивая части представления реализации. В случае с исходным кодом, например, если одна часть исходного кода включает вызов подпрограммы из другой части исходного кода, оценщик проверяет, что аргументы вызывающей программы соответствуют обработке аргументов вызываемой программой. В случае с чертежами аппаратных средств, оценщик проверяет согласованность характеристик на двух концах цепи (например, выполнение требований к уровню напряжения, направлению логики, тактовым сигналам).

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

7.6.1.3.2 Действие ADV_IMP.1.2E

ADV_IMP.1-4 Оценщик ***должен исследовать*** подмножество представления реализации, чтобы сделать заключение, является ли оно точным отображением тех функциональных требований безопасности ОО, которые имеют отношение к подмножеству.

Для тех частей подмножества представления реализации, которые непосредственно предоставляют функции безопасности, оценщик делает заключение, соответствует ли реализация функциональным требованиям безопасности ОО. Остальные части подмножества представления реализации могут поддерживать некоторые функциональные требования ОО. Делая заключение относительно этих остальных частей подмножества представления реализации, оценщик использует проект нижнего уровня, чтобы оценить, отражают ли эти части подмножества представления реализации в комбинации с другими частями, которые описаны в проекте нижнего уровня, функциональные требования безопасности ОО.

Остальные части подмножества представления реализации, если таковые имеются, вообще-то могут быть проигнорированы, потому что они не связаны с каким-либо из функциональных требований безопасности ОО, поддерживаемых подмножеством представления реализации. Тем не менее, оценщику следует быть внимательным, чтобы не пропустить какие-нибудь части, которые играют косвенную роль, неважно насколько малую, в поддержке функций безопасности ОО. Например, в типичных операционных системах исходный код для частей ядра может не играть какую-либо роль в поддержке функции безопасности ОО непосредственно, но способен помешать правильному функционированию тех частей ядра, которые играют такую роль непосредственно. Если в подмножестве предоставленного представления реализации такие части обнаружены, они должны быть оценены на предмет отсутствия с их стороны вмешательства в функционирование тех частей, для которых в ЗБ требуется отсутствие вмешательства.

Данная оценка не потребует того же самого уровня детального исследования, который требуется для тех частей представления реализации, которые играют более непосредственную роль в поддержке функций безопасности ОО.

7.7 Оценка проекта нижнего уровня

7.7.1 Подвид деятельности ADV_LLD.1

7.7.1.1 Цели

Цель данного подвида деятельности – сделать заключение, является ли проект нижнего уровня достаточным для удовлетворения функциональных требований ЗБ и является ли он корректным и эффективным уточнением проекта верхнего уровня.

7.7.1.2 Замечания по применению

Неформальный проект нижнего уровня выражается в терминах последовательностей действий, которые происходят в каждом модуле в ответ на инициирующее воздействие на его интерфейсе. Например, подсистема виртуальной частной сети может состоять из модулей, которые создают сеансовые ключи, шифруют трафик, дешифруют трафик и решают, должен ли трафик шифроваться. Низкоуровневое описание модуля шифрования, как правило, включает описание действий, которые выполняются модулем при получении трафика, подлежащего шифрованию.

7.7.1.3 Исходные данные

Безусловными свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) проект нижнего уровня.

Свидетельствами оценки для этого подвида деятельности, обусловленными зависимостями из ОК, являются:

а) функциональная спецификация;

б) проект верхнего уровня.

7.7.1.4 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а) ADV_LLD.1.1E;

б) ADV_LLD.1.2E.

7.7.1.4.1 Действие ADV_LLD.1.1E

ADV_LLD.1.1C

ADV_LLD.1-1 Оценщик ***должен исследовать*** проект нижнего уровня, чтобы сделать заключение, содержит ли он весь необходимый неформальный пояснительный текст.

Если весь проект нижнего уровня является неформальным, то рассматриваемый шаг оценивания не применяется.

Для тех частей проекта нижнего уровня, которые трудны для понимания только на основе полуформального или формального описания, необходимо вспомогательное описание в повествовательной форме (например, чтобы сделать понятными значения всех формальных обозначений).

ADV_LLD.1.2C

ADV_LLD.1-2 Оценщик ***должен исследовать*** представление проекта нижнего уровня, чтобы сделать заключение о его внутренней непротиворечивости.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

ADV_LLD.1.3C

ADV_LLD.1-3 Оценщик ***должен исследовать*** проект нижнего уровня, чтобы сделать заключение, описана ли структура ФБО в терминах модулей.

Применительно к проекту нижнего уровня термин *модуль* используется в этом подвиде деятельности для обозначения менее абстрактной сущности, чем подсистема. Это означает, что проект нижнего уровня содержит больше подробностей относительно не только цели каждого модуля, но также и относительно способа достижения модулем

своей цели. В идеале в проекте нижнего уровня должна быть представлена вся информация, необходимая для реализации описанных в нем модулей. Последующие шаги оценивания в этом подвиде деятельности требуют проведения конкретного анализа, чтобы сделать заключение, достаточен ли уровень детализации проекта нижнего уровня. На данном шаге оценивания оценщику достаточно верифицировать четкость и однозначность идентификации каждого модуля.

ADV_LLD.1.4C

ADV_LLD.1-4 Оценщик ***должен исследовать*** проект нижнего уровня, чтобы сделать заключение, содержит ли он описание назначения каждого модуля.

Проект нижнего уровня должен содержать описание назначения каждого модуля. Это описание должно быть достаточно четким, чтобы отразить, выполнение каких функций предполагается данным модулем. В данном описании должен даваться краткий обзор назначения модуля, но оно не обязательно должно быть на уровне детализации спецификации интерфейсов модулей.

ADV_LLD.1.5C

ADV_LLD.1-5 Оценщик ***должен исследовать*** проект нижнего уровня, чтобы сделать заключение, определены ли в нем взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.

В целях проведения такого анализа рассматриваются два способа взаимодействия модулей:

а) предоставление услуг друг другу;

б) совместная работа для поддержки функций безопасности.

В проект нижнего уровня должна быть включена конкретная информация об этих взаимосвязях. Например, если модуль выполняет вычисления, которые зависят от результатов вычислений, выполняемых другими модулями, последние должны быть перечислены. Кроме того, если модуль предоставляет услугу, предназначенную для использования другими модулями при поддержке функций безопасности, данная услуга должна быть описана. Возможно, что описание назначения модуля, которое анализируется на предыдущем шаге оценивания, достаточно для того, чтобы предоставить такую информацию.

ADV_LLD.1.6C

ADV_LLD.1-6 Оценщик ***должен исследовать*** проект нижнего уровня, чтобы сделать заключение, содержит ли он описание того, каким образом предоставляется каждая из функций, осуществляющих ПБО.

Функции, осуществляющие ПБО – это те функции из числа ФБО, которые прямо или косвенно осуществляют ПБО.

Рассматриваемое на данном шаге описание, содержащееся в проекте нижнего уровня, является ключевым при оценке того, достаточно ли уточнен проект нижнего уровня, чтобы дать возможность осуществить реализацию. Оценщику следует проанализировать описание с точки зрения реализующего. Если для оценщика, поставившего себя на место реализующего, какой-либо аспект того, каким образом модуль может быть реализован, остается неясным, то рассматриваемое описание считается неполным. Обратите внимание, что не предъявляется требование, чтобы модуль был реализован как отдельная единица (будь это программа, подпрограмма или аппаратный компонент); но проект нижнего уровня может быть достаточно подробным, чтобы дать возможность осуществить такую реализацию.

ADV_LLD.1.7C

ADV_LLD.1-7 Оценщик ***должен проверить***, идентифицированы ли в проекте нижнего уровня все интерфейсы модулей ФБО.

Проект нижнего уровня должен включать для каждого модуля имя каждой из его точек входа.

ADV_LLD.1.8C

ADV_LLD.1-8 Оценщик ***должен проверить***, идентифицировано ли в проекте нижнего уровня, какие интерфейсы модулей ФБО являются внешне видимыми.

Как изложено в описании шагов оценивания ADV_FSP.1-3 и ADV_FSP.2-3, через внешние интерфейсы (т.е. видимые пользователю) можно прямо или косвенно получить доступ к ФБО. Любой внешний интерфейс, через который можно прямо или косвенно получить доступ к ФБО, идентифицируется для проведения данного шага оценивания. Внешние интерфейсы, через которые нельзя получить доступ к ФБО, не обязательно должны быть включены.

ADV_LLD.1.9C

ADV_LLD.1-9 Оценщик ***должен исследовать*** проект нижнего уровня, чтобы сделать заключение, содержится ли в нем описание назначения и методов использования всех интерфейсов каждого модуля, и предоставляется ли при необходимости подробное описание результатов, нештатных ситуаций и сообщений об ошибках.

Описание интерфейсов модулей может быть предоставлено для одних интерфейсов в общих чертах, а для других – более подробно. При определении необходимого уровня детализации описания результатов, нештатных ситуаций и сообщений об ошибках оценщику следует учитывать цели данного анализа и назначение конкретного интерфейса ОО. Например, оценщику нужно понять характер взаимодействия между модулями, чтобы обрести уверенность в правильности проекта ОО и, возможно, быть способным понять это только на основе общего описания некоторых интерфейсов между модулями. В частности, внутренние точки входа, которые не используются каким-либо другим модулем, как правило, не требуют подробного описания.

Данный шаг оценивания может выполняться совместно с проведением оценщиком независимого анализа уязвимостей, который является частью подвида деятельности AVA_VLA.*, если этот подвид деятельности является частью оценки.

Детальное описание, как правило, включает подробную информацию обо всех параметрах ввода-вывода, влиянии интерфейса, обо всех нештатных ситуациях и сообщениях об ошибках, которые порождает интерфейс. В случае с внешними интерфейсами, требуемое описание, как правило, включается в функциональную спецификацию, а в проекте нижнего уровня вместо повтора может быть использована ссылка на это описание.

ADV_LLD.1.10C

ADV_LLD.1-10 Оценщик ***должен проверить***, содержится ли в проекте нижнего уровня описание разделения ОО на модули, осуществляющие ПБО, и другие модули.

ФБО включают все те части ОО, на которые возложено осуществление ПБО. Поскольку ФБО включают, как функции, которые непосредственно осуществляют ПБО, так и функции, которые, хотя непосредственно и не осуществляют ПБО, но косвенным образом вносят вклад в осуществление ПБО, все модули, осуществляющие ПБО, составляют ФБО. Модули, которые не могут оказывать влияния на осуществление ПБО, не являются частью ФБО.

7.7.1.4.2 Действие ADV_LLD.1.2E

ADV_LLD.1-11 Оценщик ***должен исследовать*** проект нижнего уровня, чтобы сделать заключение, является ли он точным отображением функциональных требований безопасности ОО.

Оценщик подтверждает правильность спецификаций интерфейсов модулей, удостоверяясь в том, что:

а) спецификации интерфейсов согласованы с описанием назначения модуля;

б) спецификации интерфейсов согласованы с их использованием другими модулями;

в) взаимосвязи между модулями, необходимые для правильной поддержки каждой функции, осуществляющей ПБО, правильно изложены.

ADV_LLD.1-12 Оценщик ***должен исследовать*** проект нижнего уровня, чтобы сделать заключение, является ли он полным отображением функциональных требований безопасности ОО.

Оценщик удостоверяется, что все функциональные требования из ЗБ отображаются на соответствующие разделы проекта нижнего уровня. Соответствующее заключение следует сделать совместно с выполнением подвида деятельности ADV_RCR.1, если этот подвид деятельности является частью оценки.

Оценщик анализирует проект нижнего уровня, чтобы сделать заключение, полностью ли описана каждая функция безопасности ОО в спецификациях модулей и нет ли таких модулей, от которых зависит функция безопасности ОО, но для которой нет спецификации в проекте нижнего уровня.

7.8 Оценка соответствия представлений

7.8.1 Подвид деятельности ADV_RCR.1

7.8.1.1 Цели

Цель данного подвида деятельности – сделать заключение, правильно ли и полностью ли разработчик реализовал требования ЗБ на всех уровнях абстракции проекта, включенных в свидетельство оценки. Выполнение данного подвида деятельности зависит от того, какие компоненты доверия из класса ADV были включены в пакет доверия. Если в пакет доверия включены компоненты из всех четырех семейств ADV_FSP, ADV_HLD, ADV_LLD, и ADV_IMP, то цель данного подвида деятельности – сделать заключение, правильно ли и полностью ли разработчик реализовал требования ЗБ в функциональной спецификации, проекте верхнего уровня, проекте нижнего уровня и в представлении реализации.

7.8.1.2 Замечания по применению

Необязательно, чтобы неформальная демонстрация соответствия была в повествовательной

форме; достаточным может быть простого двухмерного отображения. Например, матрица с перечисленными по одной оси модулями и перечисленными по другой оси подсистемами, в которой ячейки указывают на соответствие модулей и подсистем, была бы полезна для представления адекватного неформального соответствия между проектом верхнего уровня и проектом нижнего уровня. Так же простого отображения может быть достаточно для демонстрации соответствия между другими представлениями ФБО.

7.8.1.3 Исходные данные

Безусловным свидетельством оценки для этого подвида деятельности является ЗБ. Остальные безусловные свидетельства оценки для этого подвида деятельности зависят от того, какие компоненты из класса ADV были включены в пакет доверия.

Если в пакет доверия включен компонент из семейства ADV_FSP, то безусловные свидетельства оценки для этого подвида деятельности также включают:

а) функциональную спецификацию;

б) материалы анализа соответствия между краткой спецификацией ОО и функциональной спецификацией.

Если кроме этого в пакет доверия включен компонент из семейства ADV_HLD, то безусловные свидетельства оценки для этого подвида деятельности также включают:

а) проект верхнего уровня;

б) материалы анализа соответствия между функциональной спецификацией и проектом верхнего уровня.

Если кроме этого в пакет доверия включен компонент из семейства ADV_LLD, то безусловные свидетельства оценки для этого подвида деятельности также включают:

а) проект нижнего уровня;

б) материалы анализа соответствия между проектом верхнего уровня и проектом нижнего уровня.

Если кроме этого в пакет доверия включен компонент из семейства ADV_IMP, то безусловные свидетельства оценки для этого подвида деятельности также включают:

а) подмножество представления реализации;

б) материалы анализа соответствия между проектом нижнего уровня и подмножеством представления реализации.

7.8.1.4 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ADV_RCR.1.1E.

7.8.1.4.1 Действие ADV_RCR.1.1E

ADV_RCR.1.1C

ADV_RCR.1-1 Оценщик ***должен исследовать*** материалы анализа соответствия между краткой спецификацией ОО и функциональной спецификацией, чтобы сделать заключение, является ли функциональная спецификация корректным и полным представлением функций безопасности ОО.

Если функциональная спецификация не включена в состав свидетельств оценки вследствие того, что ни один из компонентов из семейства ADV_FSP не включен в пакет доверия, то рассматриваемый шаг оценивания не применяется.

Цель оценщика на этом шаге оценивания – сделать заключение, что все функции безопасности, идентифицированные в краткой спецификации ОО, представлены в функциональной спецификации, и что их представление является точным.

Оценщик проверяет соответствие между функциями безопасности ОО в краткой спецификации ОО и в функциональной спецификации. Оценщик ожидает непротиворечивого и точного соответствия. Если материалы анализа соответствия указывают на связь между описанием функции безопасности в краткой спецификации ОО и описанием интерфейса в функциональной спецификации, оценщик верифицирует, что функциональные возможности функции и интерфейса одни и те же. Если функции безопасности в краткой спецификации ОО точно и полно представлены в описании соответствующего интерфейса, рассматриваемый шаг оценивания считается выполненным.

Данный шаг оценивания может быть выполнен совместно с шагами оценивания ADV_FSP.2-8 и ADV_FSP.2-9.

ADV_RCR.1-2 Оценщик ***должен исследовать*** материалы анализа соответствия между функциональной спецификацией и проектом верхнего уровня, чтобы сделать заключение, является ли проект верхнего уровня корректным и полным представлением функциональной спецификации.

Если проект верхнего уровня не включен в состав свидетельств оценки вследствие того, что ни один из компонентов из семейства ADV_HLD не включен в пакет доверия, то рассматриваемый шаг оценивания не применяется.

Оценщик использует материалы анализа соответствия, функциональную спецификацию и проект верхнего уровня, чтобы удостовериться в возможности отобразить каждую функцию безопасности, идентифицированную в функциональной спецификации, на какую-либо подсистему ФБО, описанную в проекте верхнего уровня.

Для каждой функции безопасности материалы соответствия должны указывать, какие подсистемы ФБО предполагают поддержку данной функции безопасности. Оценщик верифицирует, что проект верхнего уровня содержит описание корректной реализации каждой функции безопасности.

ADV_RCR.1-3 Оценщик ***должен исследовать*** материалы анализа соответствия между проектом верхнего уровня и проектом нижнего уровня, чтобы сделать заключение, является ли проект нижнего уровня корректным и полным представлением проекта верхнего уровня.

Если проект нижнего уровня не включен в состав свидетельств оценки вследствие того, что ни один из компонентов из семейства ADV_LLD не включен в пакет доверия, то рассматриваемый шаг оценивания не применяется.

Оценщик использует материалы анализа соответствия, проект верхнего уровня и проект нижнего уровня, чтобы удостовериться в возможности отобразить каждый модуль ФБО, идентифицированный в проекте нижнего уровня, на некоторую подсистему ФБО, описанную в проекте верхнего уровня. Для каждой функции безопасности ОО материалы соответствия должны указывать, какие модули ФБО предполагают поддержку данной функций безопасности. Оценщик верифицирует, что проект нижнего уровня содержит описание правильной реализации каждой функции безопасности.

ADV_RCR.1-4 Оценщик ***должен исследовать*** материалы анализа соответствия между проектом нижнего уровня и подмножеством представления реализации, чтобы сделать заключение, является ли подмножество представления реализации правильным и полным представлением тех частей проекта нижнего уровня, которые уточняются в представлении реализации.

Если подмножество представления реализации не включено в состав свидетельств оценки вследствие того, что ни один из компонентов из семейства ADV_IMP не включен в пакет доверия, то рассматриваемый шаг оценивания не применяется.

Так как оценщик исследует только подмножество представления реализации, этот шаг оценивания выполняется путем проведения оценки материалов анализа соответствия подмножества представления реализации и соответствующих частей проекта нижнего уровня, а не путем осуществления попытки отследить каждую функцию безопасности ОО к представлению реализации. Подмножество может не обеспечить охват некоторых функций безопасности.

7.9 Оценка моделирования политики безопасности ОО

7.9.1 Подвид деятельности ADV_SPM.1

7.9.1.1 Цели

Цель данного подвида деятельности – сделать заключение, описывает ли модель политики безопасности ОО четко и непротиворечиво правила и характеристики политик безопасности ФБ, и соответствует ли это описание описанию функций безопасности в функциональной спецификации.

7.9.1.2 Замечания по применению

Модель описывает политики, осуществляемые теми функциями и услугами безопасности, которые описаны в функциональной спецификации. Неформальная модель – это просто описание политик безопасности, осуществляемых услугами или функциями безопасности, доступными через внешний интерфейс. Например, политики управления доступом обычно описывают защищаемые ресурсы и условия, которые должны быть обеспечены для предоставления доступа; политики аудита обычно описывают потенциально подвергаемые аудиту события ОО, идентифицируя, как те, которые

выбираются администратором, так и те, которые всегда подвергаются аудиту; политики идентификации и аутентификации обычно описывают, как идентифицируются пользователи, как аутентифицируется заявленная идентификационная информация, а также какие-либо правила, влияющие на то, каким образом аутентифицируется идентификационная информация (например, для пользователей корпоративной интранет (внутренней сети) аутентификация не требуется, в то время как внешние пользователи аутентифицируются на основе одноразовых паролей).

7.9.1.3 Исходные данные

Безусловными свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) модель политики безопасности ОО.

Свидетельством оценки для этого подвида деятельности, обусловленным зависимостями из ОК, является функциональная спецификация.

Свидетельствами оценки для этого подвида деятельности, которые требуются для выполнения шагов оценивания, являются:

а) руководство пользователя;

б) руководство администратора.

7.9.1.4 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ADV_SPM.1.1E.

7.9.1.4.1 Действие ADV_SPM.1.1E

ADV_SPM.1.1C

ADV_SPM.1-1 Оценщик ***должен исследовать*** модель политики безопасности ОО, чтобы сделать заключение, содержит ли она весь необходимый неформальный пояснительный текст.

Если вся модель политики безопасности ОО является неформальной, то рассматриваемый шаг оценивания не применяется.

Для тех частей модели политики безопасности ОО, которые трудны для понимания только на основе полуформального или формального описания, требуется вспомогательное описание в повествовательной форме (например, чтобы сделать понятными значения всех формальных обозначений).

ADV_SPM.1.2C

ADV_SPM.1-2 Оценщик ***должен проверить*** модель политики безопасности ОО, чтобы сделать заключение, все ли политики ФБ, которые явным образом включены в ЗБ, смоделированы.

Политика безопасности выражается в ЗБ через совокупность функциональных требований безопасности. Поэтому, чтобы сделать заключение о характере политики безопасности (а, следовательно, о том, какие политики ФБ должны быть смоделированы), оценщик анализирует функциональные требования из ЗБ для тех политик ФБ, которые затребованы явным образом (компонентами требований из семейств FDP_ACC и FDP_IFC, если таковые включены в ЗБ).

В зависимости от ОО, формальное/полуформальное моделирование может быть невозможно даже для управления доступом (например, политика управления доступом для межсетевого экрана, подключенного к Интернету, не может быть надлежащим образом формально смоделирована, потому что состояние Интернета не может быть полностью определено). Любая политика безопасности, для которой создание формальной или полуформальной модели невозможно, должна быть представлена в неформальном виде.

Если ЗБ не содержит явных политик ФБ (вследствие того, что компоненты

требований ни из семейства FDP_ACC, ни из семейства FDP_IFC не включены в ЗБ), то рассматриваемый шаг оценивания не применяется.

ADV_SPM.1-3 Оценщик ***должен исследовать*** модель политики безопасности ОО, чтобы сделать заключение, все ли политики ФБ, представленные функциональными требованиями безопасности, заявленными в ЗБ, смоделированы.

Кроме перечисленных в явном виде политик ФБ (см. шаг оценивания ADV_SPM.1-2), оценщик анализирует функциональные требования безопасности из ЗБ для тех политик ФБ, наличие которых предполагается в связи с другими классами функциональных требований безопасности. Например, включение компонентов требований класса FDP (за исключением FDP_ACC и FDP_IFC) обычно требует описания осуществляемой политики защиты данных; включение компонентов требований класса FIA обычно требует, чтобы в модели политики безопасности ОО было представлено описание политик ФБ идентификации и аутентификации; включение компонентов требований безопасности класса FAU требует описания политик ФБ аудита и т.д. Хотя компоненты функциональных требований безопасности из других семейств обычно не ассоциируются с тем, что понимается как *политики ФБ*, однако они все же обеспечивают выполнение ряда политик ФБ (например, таких как неотказуемость, посредничество при обращениях, приватность и т.д.), которые должны быть включены в модель политики безопасности ОО.

В случаях, когда представление модели политики безопасности ОО является неформальным, все политики ФБ могут быть смоделированы (то есть, описаны) и, таким образом, должны быть включены в модель. Любая политика безопасности, для которой создание формальной или полуформальной модели невозможно, должна быть представлена в неформальном виде.

Если ЗБ не содержит таких подразумеваемых правил, то рассматриваемый шаг оценивания не применяется.

ADV_SPM.1-4 Оценщик ***должен исследовать*** правила и характеристики модели политики безопасности ОО, чтобы сделать заключение, четко ли сформулирован моделируемый режим безопасного функционирования ОО.

Правила и характеристики модели политики безопасности ОО описывают состояние безопасности ОО. Вероятно, что такое описание содержится в оцененном ЗБ сертифицированного ОО. Для того чтобы данное описание считалось четко сформулированным, в нем должно быть определено понятие безопасности для рассматриваемого ОО, идентифицированы атрибуты безопасности сущностей, находящихся под управлением ОО, и идентифицированы действия ОО, которые изменяют значения этих атрибутов. Например, если в политике безопасности предпринята попытка учесть вопросы целостности данных, то, как правило, в модели политики безопасности ОО:

а) определяется понятие целостности для рассматриваемого ОО;

б) идентифицируются типы данных, для которых ОО поддерживает целостность;

в) идентифицируются сущности, которые могут модифицировать данные указанных типов;

г) идентифицируются правила, которые должны выполняться при модификации данных.

ADV_SPM.1.3C

ADV_SPM.1-5 Оценщик ***должен исследовать*** обоснование модели политики безопасности ОО, чтобы сделать заключение, согласован ли смоделированный режим функционирования ОО с правилами, описанными в политиках ФБ (т.е., сформулированными в соответствии с функциональными требованиями из ЗБ).

Делая заключение о непротиворечивости, оценщик верифицирует, что обоснование показывает, что описание каждого правила или характеристики в модели политики

безопасности ОО точно отражает предназначение политик ФБ. Например, если политикой безопасности установлено, что управление доступом необходимо на уровне отдельных пользователей, то модель политики безопасности ОО, описывающая безопасный режим функционирования ОО в контексте управления группами пользователей, не будет считаться согласованной с политикой безопасности. Аналогично, если политикой безопасности установлено, что управление доступом необходимо на уровне групп пользователей, то модель политики безопасности ОО, описывающая безопасный режим функционирования ОО в контексте управления отдельными пользователями, также не будет считаться согласованной с политикой безопасности.

Доверие к безопасности приобретается, исходя из явного или общего изложения политик, лежащих в основе функциональных требований безопасности ОО. Доверие складывается из двух составляющих. Сведение описаний каждой политики ФБ в краткое единое целое помогает в понимании деталей осуществляемых политик. Кроме того, такое сводное описание намного упрощает поиск каких бы то ни было огрехов или противоречий (чего и требуется добиться как части элемента требования ADV_SPM.*.3C) и обеспечивает четкую характеристику безопасных состояний (чего и требуется добиться как части требований элемента ADV_SPM.*.2C).

Рассматриваемое требование к неформальной модели политики безопасности (НМПБ) выполняется путем четкого изложения политики безопасности ОО. Необходимость в оформлении НМПБ в виде отдельного документа не является безусловной, так как для очень простых (очевидных) политик ФБ или политик ФБ, которые очень четко определены в ЗБ, необходимости в отдельном оформлении НМПБ может и не быть. В таких случаях различные разделы ЗБ (например, требования безопасности, краткая спецификация ОО) могут в сочетании друг с другом обеспечить для описания политики безопасности достаточный уровень детализации. Однако, зачастую это не так. Например, требования аудита могут быть разнесены по всем функциональным требованиям безопасности ОО и не обеспечивать четкую модель политики ФБ в целом. Если только в другом разделе ЗБ (возможно в краткой спецификации ОО) все требования аудита не будут собраны во взаимосвязанное целое, то возникает необходимость в отдельном документе НМПБ для того, чтобы иметь возможность обнаружить противоречия в требованиях ЗБ, которые иначе могут остаться необнаруженными.

Когда разработчик утверждает, что требования к НМПБ для некоторых или для всех политик ФБ удовлетворены через ЗБ, оценщику, используя требования компонента ADV_SPM.1, необходимо сделать заключение, что это именно так, то есть, сделать заключение, что политика ясно выражена, и что модель является согласованной с остальными частями ЗБ. В тех случаях, когда разработчик утверждает, что НМПБ полностью отражена в ЗБ, в качестве части обоснования НМПБ надлежащим является, чтобы в обосновании была ссылка на материалы демонстрации пригодности отдельных частей ЗБ и их соответствия друг другу. При выполнении данного шага оценивания оценщик может использовать соответствующие результаты оценки ЗБ.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

ADV_SPM.1-6 Оценщик ***должен исследовать*** обоснование модели политики безопасности ОО, чтобы сделать заключение о полноте смоделированного режима функционирования ОО по отношению к правилам, описанным в политиках ФБ (т.е., сформулированным в соответствии с функциональными требованиями из ЗБ).

Для заключения о полноте обоснования оценщик рассматривает правила и характеристики модели политики безопасности ОО и сопоставляет их с правилами и характеристиками политики безопасности, изложенными в явном виде (т.е., функциональными требованиями). Обоснование должно показать, что для всех политик ФБ, которые должны быть смоделированы, в модели политики безопасности ОО имеется

описание связанных с ними правил или характеристик.

Когда разработчик утверждает, что требования к НМПБ для некоторых или для всех политик ФБ удовлетворены через ЗБ, оценщику, используя требования компонента ADV_SPM.1, необходимо сделать заключение, что это именно так, т.е., сделать заключение, что политика четко выражена, и что модель является полной по отношению к остальным частям ЗБ. При выполнении данного шага оценивания оценщик может использовать соответствующие результаты оценки полноты различных частей ЗБ.

ADV_SPM.1.4C

ADV_SPM.1-7 Оценщик ***должен исследовать*** материалы демонстрации соответствия между моделью политики безопасности ОО и функциональной спецификацией, чтобы сделать заключение, идентифицированы ли в этих материалах все функции безопасности, описанные в функциональной спецификации, которые реализуют какую-либо часть политики безопасности.

Для заключения о полноте оценщик просматривает функциональную спецификацию, определяет, какие из функций непосредственно поддерживают модель политики безопасности ОО, и верифицирует наличие этих функций в материалах демонстрации соответствия функциональной спецификации и модели политики безопасности ОО.

ADV_SPM.1-8 Оценщик ***должен исследовать*** материалы демонстрации соответствия между моделью политики безопасности ОО и функциональной спецификацией, чтобы сделать заключение, согласуется ли описание функций безопасности, идентифицированных в качестве реализации модели политики безопасности ОО, с описанием функций безопасности в функциональной спецификации.

Для демонстрации непротиворечивости оценщик верифицирует, что материалы демонстрации соответствия функциональной спецификации показывают, что описание в функциональной спецификации функций, идентифицированных в качестве реализации политики безопасности, описанной в модели политики безопасности ОО, идентифицирует те же самые атрибуты и характеристики модели политики безопасности и обеспечивает выполнение тех же самых правил, что и модель политики безопасности ОО.

В тех случаях, когда какая-либо политика ФБ осуществляется для администраторов и недоверенных пользователей по-разному, политики ФБ для каждой из этих категорий описываются сообразно соответствующим описаниям режимов функционирования в руководстве администратора и руководстве пользователя. Например, политика ФБ «идентификации и аутентификации», осуществляемая по отношению к удаленным недоверенным пользователям, может быть более строгой, чем осуществляемая по отношению к администраторам, единственная точка доступа которых лежит в пределах физически защищенной зоны; различия в аутентификации должны соответствовать различиям в описании аутентификации в руководствах пользователя и администратора.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

8 Вид деятельности AGD

8.1 Введение

Вид деятельности "Руководства" предназначен для определения достаточности документации, регламентирующей эксплуатацию ОО. Такая документация включает как документацию для доверенных администраторов и не связанных с администрированием пользователей, чьи неправильные действия могли бы отрицательно повлиять на безопасность ОО, так и документацию для недоверенных пользователей, чьи неправильные действия могли бы отрицательно повлиять на безопасность их собственных

данных.

8.2 Цели

Вид деятельности "Руководства" предназначен для определения достаточности документации, регламентирующей эксплуатацию ОО.

8.3 Замечания по применению

Вид деятельности "Руководства" применяется к тем функциям и интерфейсам, которые связаны с безопасностью ОО. Безопасная конфигурация ОО описывается в ЗБ.

8.4 Оценка руководства администратора

8.4.1 Подвид деятельности AGD_ADM.1

8.4.1.1 Цели

Цель данного подвида деятельности – сделать заключение, описано ли в руководстве администратора, как осуществлять безопасное администрирование ОО.

8.4.1.2 Замечания по применению

Термин *администратор* используется для обозначения человека-пользователя, которому доверено выполнение в пределах ОО критичных для безопасности операций, таких, как настройка параметров конфигурации ОО. Данные операции могут влиять на осуществление ПБО, поэтому администратор обладает особыми привилегиями, необходимыми для выполнения таких операций. Роль администратора (роли администраторов) необходимо четко отличать от ролей пользователей ОО, не связанных с администрированием.

В ЗБ могут быть определены несколько различных ролей или групп администраторов, которые признаются объектом оценки и могут взаимодействовать с ФБО, таких как аудитор, администратор или начальник смены. Каждой роли может соответствовать как одна возможность, так и обширный их набор. Возможности этих ролей и связанные с ними привилегии описываются в классе FMT. Различные роли и группы администраторов должны быть рассмотрены в руководстве администратора.

8.4.1.3 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) функциональная спецификация;

в) проект верхнего уровня;

г) руководство пользователя;

д) руководство администратора;

е) процедуры безопасной установки, генерации и запуска;

ж) определение жизненного цикла.

8.4.1.4 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) AGD_ADM.1.1E.

8.4.1.4.1 Действие AGD_ADM.1.1E

AGD_ADM.1.1C

AGD_ADM.1-1 Оценщик ***должен исследовать*** руководство администратора, чтобы сделать заключение, описаны ли в нем относящиеся к администрированию функции

безопасности и интерфейсы, доступные администратору ОО.

В руководстве администратора должен быть помещен краткий обзор функциональных возможностей безопасности, видимых через интерфейсы администратора.

В руководстве администратора должны быть идентифицированы и описаны предназначение, режимы применения и взаимосвязь интерфейсов и функций безопасности, доступных администратору.

Для каждых интерфейса и функции безопасности, доступных администратору, в руководстве администратора должны быть описаны:

а) метод (методы) вызова интерфейса (например, с использованием командной строки, системных вызовов языка программирования, меню, командной кнопки);

б) параметры, которые устанавливаются администратором, их допустимые значения и значения по умолчанию;

в) реакция, сообщения или коды возврата непосредственно от ФБО.

AGD_ADM.1.2C

AGD_ADM.1-2 Оценщик ***должен исследовать*** руководство администратора, чтобы сделать заключение, описан ли в нем безопасный способ администрирования ОО.

В руководстве администратора описывается, как использовать ОО согласно ПБО в среде ИТ, соответствующей ее описанию в ЗБ.

AGD_ADM.1.3C

AGD_ADM.1-3 Оценщик ***должен исследовать*** руководство администратора, чтобы сделать заключение, содержит ли оно предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде эксплуатации.

Конфигурация ОО может позволять пользователям иметь отличающиеся привилегии по использованию различных функций ОО. Это значит, что некоторые пользователи могут быть уполномочены выполнять определенные функции, в то время как другие пользователи могут быть не уполномочены на это. Такие функции и привилегии должны быть описаны в руководстве администратора.

Руководство администратора идентифицирует функции и привилегии, которые необходимо контролировать, требуемые для них способы контроля и основания для такого контроля. Предупреждающие сообщения связаны с ожидаемыми последствиями, возможными побочными эффектами и возможным взаимодействием с другими функциями и привилегиями.

AGD_ADM.1.4C

AGD_ADM.1-4 Оценщик ***должен исследовать*** руководство администратора, чтобы сделать заключение, приведены ли в нем все предположения относительно поведения пользователя, которые связаны с безопасной эксплуатацией ОО.

Предположения относительно действий пользователя могут быть описаны более подробно при изложении среды безопасности ОО в ЗБ. Однако в руководство администратора необходимо включить только ту информацию, которая относится к безопасной эксплуатации ОО.

Примером обязанности пользователей, необходимой для безопасной эксплуатации ОО, является сохранение ими в тайне своих паролей.

AGD_ADM.1.5C

AGD_ADM.1-5 Оценщик ***должен исследовать*** руководство администратора, чтобы сделать заключение, описаны ли в нем все параметры безопасности, контролируемые администратором, с указанием при необходимости их безопасных значений.

Для каждого параметра безопасности в руководстве администратора должны быть приведены предназначение параметра, допустимые значения параметра и его значения по умолчанию, а также безопасные и небезопасные настройки таких параметров, как по

отдельности, так и в сочетании.

AGD_ADM.1.6C

AGD_ADM.1-6 Оценщик ***должен исследовать*** руководство администратора, чтобы сделать заключение, описан ли в нем каждый тип относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО.

Все типы относящихся к безопасности событий детализируются настолько, чтобы администратор знал, какие события могут произойти, и какие действия (если потребуется) он мог бы предпринять для поддержания безопасности. Относящиеся к безопасности события, которые могут произойти в процессе эксплуатации ОО (например, переполнение журнала аудита, полный отказ системы, обновление записей о пользователях, такое, как удаление учетных данных пользователя при его увольнении из организации), определяются в мере, позволяющей при вмешательстве администратора поддерживать безопасность эксплуатации.

AGD_ADM.1.7C

AGD_ADM.1-7 Оценщик ***должен исследовать*** руководство администратора, чтобы сделать заключение о его согласованности со всей другой документацией, представленной для оценки.

В частности, ЗБ может содержать подробную информацию о любых предупреждающих сообщениях администраторам ОО, относящихся к среде безопасности и целям безопасности ОО.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

AGD_ADM.1.8C

AGD_ADM.1-8 Оценщик ***должен исследовать*** руководство администратора, чтобы сделать заключение, описаны ли в нем все требования безопасности ИТ для среды ИТ объекта оценки, которые относятся к администратору.

Если ЗБ не содержит требования безопасности ИТ для среды ИТ, то этот шаг оценивания не подлежит выполнению и считается заведомо удовлетворенным.

Этот шаг оценивания относится только к требованиям безопасности ИТ, а не к каким-либо политикам безопасности организации.

Оценщику следует проанализировать требования безопасности для среды ИТ объекта оценки (являющиеся необязательной частью ЗБ) и сравнить их с руководством администратора, чтобы удостовериться, что все требования безопасности из ЗБ, которые относятся к администратору, надлежащим образом описаны в руководстве администратора.

8.5 Оценка руководства пользователя

8.5.1 Подвид деятельности AGD_USR.1

8.5.1.1 Цели

Цели данного подвида деятельности – сделать заключение, описаны ли в руководстве пользователя функции безопасности и интерфейсы ФБО, и содержит ли данное руководство инструкции и указания по безопасному использованию ОО.

8.5.1.2 Замечания по применению

В ЗБ могут быть определены несколько различных ролей или групп пользователей, которые распознаются объектом оценки и могут взаимодействовать с ФБО. Возможности этих ролей и связанные с ними привилегии описываются в классе FMT. Различные роли и группы пользователей должны быть рассмотрены в руководстве пользователя.

8.5.1.3 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) функциональная спецификация;

в) проект верхнего уровня;

г) руководство пользователя;

д) руководство администратора;

е) процедуры безопасной установки, генерации и запуска.

8.5.1.4 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) AGD_USR.1.1E.

8.5.1.4.1 Действие AGD_USR.1.1E

AGD_USR.1.1C

AGD_USR.1-1 Оценщик ***должен исследовать*** руководство пользователя, чтобы сделать заключение, описаны ли в нем функции безопасности и интерфейсы, доступные пользователям ОО, не связанным с администрированием.

В руководстве пользователя должен быть помещен краткий обзор функциональных возможностей безопасности, видимых через интерфейсы пользователя.

В руководстве пользователя должны быть идентифицированы интерфейсы и функции безопасности и описано их предназначение.

AGD_USR.1.2C

AGD_USR.1-2 Оценщик ***должен исследовать*** руководство пользователя, чтобы сделать заключение, описано ли в нем применение доступных пользователю функций безопасности, предоставляемых ОО.

В руководстве пользователя должны быть идентифицированы и описаны режимы применения и взаимосвязь интерфейсов и функций безопасности, доступных пользователю.

Если пользователю разрешен вызов некоторой функции безопасности ОО, то в руководстве пользователя приводится описание интерфейсов этой функции, доступных пользователю.

Для каждых интерфейса и функции безопасности в руководстве пользователя должны быть описаны:

а) метод (методы) вызова интерфейса (например, с использованием командной строки, системных вызовов языка программирования, меню, командной кнопки);

б) параметры, которые устанавливаются пользователем, их допустимые значения и значения по умолчанию;

в) реакция, сообщения или коды возврата непосредственно от ФБО.

AGD_USR.1.3C

AGD_USR.1-3 Оценщик ***должен исследовать*** руководство пользователя, чтобы сделать заключение, содержит ли оно предупреждения относительно доступных пользователю функций и привилегий, которые следует контролировать в безопасной среде эксплуатации.

Конфигурация ОО может позволять пользователям иметь отличающиеся привилегии по использованию различных функций ОО. Это значит, что некоторые пользователи уполномочены выполнять определенные функции, в то время как другие пользователи могут быть не уполномочены на это. Такие доступные пользователю функции и привилегии описываются в руководстве пользователя.

В руководстве пользователя должны быть идентифицированы функции и привилегии, которые могут применяться, требуемые для них типы команд и объяснения таких команд. В руководстве пользователя должны быть приведены предупреждающие

сообщения относительно использования функций и привилегий, подлежащих контролю.

Предупреждающие сообщения должны быть связаны с ожидаемыми последствиями, возможными побочными эффектами и возможным взаимодействием с другими функциями и привилегиями.

AGD_USR.1.4C

AGD_USR.1-4 Оценщик ***должен исследовать*** руководство пользователя, чтобы сделать заключение, приведены ли в нем все обязанности пользователя, необходимые для безопасной эксплуатации ОО, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности ОО.

Предположения относительно действий пользователя могут быть описаны более подробно при изложении среды безопасности ОО в ЗБ. Однако в руководство пользователя необходимо включить только ту информацию, которая относится к безопасной эксплуатации ОО.

В руководстве пользователя должны быть приведены рекомендации по эффективному использованию функций безопасности (например, описание практических приемов формирования паролей, рекомендуемая периодичность резервного копирования файлов пользователей, предполагаемые последствия изменений привилегий доступа для пользователя).

Примером обязанности пользователей, необходимой для безопасной эксплуатации ОО, является сохранение ими в тайне своих паролей.

В руководстве пользователя должно быть указано, может ли пользователь вызвать функцию, или же для этого ему потребуется помощь администратора.

AGD_USR.1.5C

AGD_USR.1-5 Оценщик ***должен исследовать*** руководство пользователя, чтобы сделать заключение о его согласованности со всей другой документацией, представленной для оценки.

Оценщик удостоверяется, что руководство пользователя и остальная документация, представленная для оценки, не противоречат друг другу. Это особенно актуально, если ЗБ содержит подробную информацию о любых предупреждающих сообщениях пользователям ОО, относящихся к среде безопасности и целям безопасности ОО.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

AGD_USR.1.6C

AGD_USR.1-6 Оценщик ***должен исследовать*** руководство пользователя, чтобы сделать заключение, описаны ли в нем все требования безопасности ИТ для среды ИТ объекта оценки, которые имеют отношение к пользователю.

Если ЗБ не содержит требования безопасности ИТ для среды ИТ, то этот шаг оценивания не подлежит выполнению и считается заведомо удовлетворенным.

Этот шаг оценивания относится только к требованиям безопасности ИТ, а не к каким-либо политикам безопасности организации.

Оценщику следует проанализировать требования безопасности для среды ИТ объекта оценки (являющиеся необязательной частью ЗБ) и сравнить их с руководством пользователя, чтобы удостовериться, что все требования безопасности из ЗБ, которые относятся к пользователю, надлежащим образом описаны в руководстве пользователя.

9 Вид деятельности ALC

9.1 Введение

Вид деятельности "Поддержка жизненного цикла" предназначен для определения

достаточности процедур, применяемых разработчиком во время разработки и сопровождения ОО. Эти процедуры включают меры безопасности во время разработки ОО, модель жизненного цикла, применяемую разработчиком, и инструментальные средства, используемые разработчиком на протяжении жизненного цикла ОО.

9.2 Цели

Вид деятельности "Поддержка жизненного цикла" предназначен для определения достаточности процедур, применяемых разработчиком во время разработки и сопровождения ОО.

9.3 Оценка безопасности разработки

9.3.1 Подвид деятельности ALC_DVS.1

9.3.1.1 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.

9.3.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) 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 их применяют. В частности оценщику может понадобиться исследование документации разработчика по УК (исходные данные подвидов деятельности ACM_CAP.4 и ACM_SCP.2). Также требуется свидетельство, что процедуры применяются.

9.3.1.3 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а) ALC_DVS.1.1E;

б) ALC_DVS.1.2E.

9.3.1.3.1 Действие ALC_DVS.1.1E

ALC_DVS.1.1C

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, особенно из разделов ЗБ об угрозах, политике безопасности организации и предположениях, хотя такая информация может и не быть представлена в явном виде. Изложение в ЗБ целей безопасности для среды также может быть полезно в этом отношении.

Если в ЗБ не имеется такой информации в явном виде, оценщик будет вынужден принять решение о необходимых мерах, основываясь на рассмотрении предполагаемой среды для ОО. В тех случаях, когда меры разработчика признаются недостаточными, должно быть представлено четкое и строгое обоснование для оценки уязвимостей, потенциально пригодных для использования.

При исследовании документации оценщиком рассматриваются следующие типы мер безопасности:

а) *физические*, например средства управления физическим доступом, применяемые для предотвращения несанкционированного доступа к среде разработки ОО (в рабочие часы и в другое время);

б) *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;

в) *относящиеся к персоналу разработчиков*, например, средства контроля или проверки, позволяющие установить, заслуживают ли доверия принимаемые на работу;

г) *прочие меры безопасности*, например, средства логической защиты оборудования разработки.

В документации по безопасности разработки должны быть указаны места разработки и описаны виды выполняемых работ вместе с мерами безопасности, применяемыми в каждом из мест разработки. Например, разработка могла бы происходить в нескольких производственных помещениях внутри одного здания, в нескольких зданиях, расположенных на одной территории, или в нескольких различных местах. К разработке относят такую задачу как тиражирование ОО, когда это применимо. Не следует, чтобы этот шаг оценивания частично перекрывал шаги оценивания из ADO_DEL, но оценщику следует удостовериться, что все аспекты охвачены тем или другим подвидом деятельности.

Кроме того, документация по безопасности разработки может описывать различные меры безопасности, которые могут применяться к различным аспектам разработки с точки зрения их выполнения, требуемых исходных данных и выходных результатов. Например, различные процедуры могут быть применимы к разработке различных частей ОО или к различным стадиям процесса разработки.

ALC_DVS.1-2 Оценщик ***должен исследовать*** политики обеспечения конфиденциальности и целостности при разработке, чтобы сделать заключение о достаточности применявшихся мер безопасности.

Они включают политики управления следующим:

а) какая информация, относящаяся к разработке ОО, нуждается в сохранении конфиденциальности, и кому из персонала разработчиков разрешен доступ к таким материалам;

б) какие материалы должны быть защищены от несанкционированной модификации для сохранения целостности ОО, и кому из персонала разработчиков разрешено модифицировать 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 ACM_CAP. 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, 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.

ALC_DVS.1.2C

ALC_DVS.1-3 Оценщик ***должен проверить*** документацию по безопасности разработки, чтобы сделать заключение, формируется ли документальное свидетельство в результате применения процедур.

При наличии документального свидетельства оценщик просматривает его, чтобы удостовериться в его соответствии процедурам. Примерами подготовленных свидетельств могут служить журналы регистрации входа и журналы аудита. Оценщик может остановиться на выборочной проверке свидетельства.

Руководство по выборке приведено в подразделе 12.2.

9.3.1.3.2 Действие ALC_DVS.1.2E

ALC_DVS.1-4 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:

а) наблюдать применение мер безопасности (например, физических мер);

б) исследовать документальные свидетельства применения процедур;

в) посредством интервью с персоналом разработчиков проверить знание ими политик и процедур безопасности разработки, а также своих обязанностей.

Посещение объекта является полезным способом приобретения уверенности в применяемых мерах. Решение отказаться от такого посещения следует принимать после консультации с органом по подтверждению соответствия.

Руководство по посещению объектов приведено в подразделе 12.5.

9.4 Оценка устранения недостатков

9.4.1 Замечания по применению

Требования семейства ALC_FLR не используются в ОУД, определенных в ОК. Поскольку в ПЗ и ЗБ не обязательно ограничиваться требованиями доверия из ОУД, определенных в ОК, то возможно привлечение и других компонентов доверия, в том числе из семейства ALC_FLR. Это означает, что любой из компонентов ALC_FLR может использоваться как часть ПЗ/ЗБ в сочетании с любым из пакетов доверия из ОК.

Выражение ОО означает объект оценки, но при этом обладает тем свойством, что теряет смысл, как только достигнуты цели оценки. Другими словами, как только оценка объекта завершена, он больше не является объектом для оценки. Но ОК не предлагают никакого иного способа ссылок на ОО по завершении оценки. Требования семейства ALC_FLR, по самой природе относящиеся к событиям "после оценки", приводят к

потребности в дополнительных терминах для периода "после оценки". Дополнительно, для подвидов деятельности, описанных в этом документе, пришлось использовать другие термины с их точным значением. Для этого в Приложении А определены следующие термины:

а) сертифицированный ОО;

б) релиз ОО;

в) отслеживание недостатка безопасности;

г) пользователь ОО;

д) руководства ОО;

е) недостаток безопасности.

Устранение недостатков безопасности выполняется для тех недостатков, которые обнаружены после завершения оценки ОО. (Исправление недостатков безопасности, обнаруженных до начала или во время оценки, является предметом рассмотрения при управлении конфигурацией, анализе уязвимостей, тестировании и т.д.).

Разработчик ОО несет ответственность за *сообщение* о недостатках, которые выявляются в среде ОО; но не за их *исправление*. Например, разработчик доверенного приложения, как правило, идентифицирует базовую операционную систему как среду ИТ. О недостатках, найденных в приложении, разработчик сообщает, а также отслеживает и исправляет их. О недостатках, обнаруженных в операционной системе, разработчику необходимо только сообщить (возможно, в самом кратком виде: "данное приложение не выполняется в такой-то операционной системе"). Тогда пользователям ОО, узнавшим, что операционная система больше не отвечает требованиям, предъявляемым к среде ОО, или предположениям о ней, понадобится другая операционная система, отвечающая упомянутым требованиям/предположениям, на то время, пока недостатки операционной системы не исправлены ее разработчиком. Приведенный сценарий подчеркивает важность осведомленности пользователей ОО о сочетании объектов оценки разных разработчиков.

Следует отметить, что процедуры устранения недостатков из этого подвида деятельности относятся к тем процедурам разработчика, которые требуется выполнять, когда недостатки безопасности найдены в сертифицированных ОО и релизах ОО, но они не содержат никаких предпосылок для верификации следования этим процедурам; некоторые шаги оценивания из ACM_SCP.2 и AMA_EVD.1 могут быть использованы для поддержки этой верификации. Поскольку исправление таких недостатков требует модификации оцененного ОО, то он после исправления не является более сертифицированной версией.

Недостаток безопасности, о котором имеется сообщение, может рассматриваться как всего лишь "предполагаемый" до того времени, пока исследование не завершится заключением: или это не недостаток безопасности (тогда его не требуется далее отслеживать), или это недостаток безопасности (тогда его требуется отслеживать вплоть до момента исправления).

9.4.2 Подвид деятельности ALC_FLR.1

9.4.2.1 Цели

Цель данного подвида деятельности – сделать заключение, установил ли разработчик процедуры устранения недостатков, которые описывают отслеживание недостатков безопасности, идентификацию действий по их исправлению и доведение информации об этих действиях до пользователей ОО.

9.4.2.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является документация процедур устранения недостатков.

9.4.2.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ALC_FLR.1.1E.

9.4.2.3.1 Действие ALC_FLR.1.1E

ALC_FLR.1.1C

ALC_FLR.1-1 Оценщик ***должен исследовать*** документацию процедур устранения недостатков, чтобы сделать заключение, описывает ли она процедуры по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.

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) процедуры устранения недостатков для его дальнейшего отслеживания; только при этом необходимо объяснение, почему недостаток не влияет на безопасность.

В то время как эти требования не обязательно определяют способ широкого оповещения пользователей ОО о недостатках безопасности, они обязывают, чтобы все недостатки безопасности, о которых уже имеется сообщение, отслеживались. Т.е. недостаток безопасности, о котором имеется сообщение, не может игнорироваться просто потому, что оно поступило не из организации разработчика.

ALC_FLR.1.2C

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 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".

ALC_FLR.1-3 Оценщик ***должен исследовать*** процедуры устранения недостатков, чтобы сделать заключение, будет ли идентифицирован при применении этих процедур статус завершения исправления каждого недостатка безопасности.

Процедуры устранения недостатков идентифицируют различные стадии недостатков безопасности. Эта дифференциация, во всяком случае, 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).

ALC_FLR.1.3C

ALC_FLR.1-4 Оценщик ***должен проверить*** процедуры устранения недостатков,

чтобы сделать заключение, будут ли идентифицированы при применении этих процедур действия по исправлению каждого недостатка безопасности.

Действия по исправлению могут заключаться как в коррекции аппаратных средств, программно-аппаратных средств или программ, входящих в ОО, так и в модификации руководств ОО или же включать и то, и другое. Действия по исправлению, приводящие к модификации руководств ОО (например, к детализации процедурных мер, которые необходимо предпринять для нейтрализации недостатка безопасности) включают меры, обеспечивающие как одни лишь промежуточные решения (пока коррекция не закончена), так и окончательное решение (для которого определено, что данная процедурная мера являются наилучшим решением).

Если источником недостатка безопасности является ошибка в документации, то действия по исправлению сводятся к обновлению соответствующего руководства ОО. Если действия по исправлению являются процедурной мерой, то эта мера будет включать обновление соответствующего руководства ОО для отражения этих корректирующих процедур.

ALC_FLR.1.4C

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), предписанных действий по исправлению и соответствующего руководства по реализации исправления.

Такая информация, материалы по исправлению и изменения документации для обновлений могут быть предоставлены пользователям ОО одним из нескольких способов, таких, как размещение их на Web-сайте, рассылка пользователям ОО или заключение соглашения по инсталляции 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 поиску такой информации.

Наиболее подходящая метрика оценки достаточности метода, используемого для предоставления информации, материалов по исправлению и руководств, та, которая дает основания надеяться, что пользователи ОО смогут достать или получить их. Например, рассмотрим метод распространения, при котором необходимые данные размещаются на Web-сайте на один месяц, а пользователи ОО осведомлены, что это произойдет и когда это произойдет. Он может быть не так уж приемлем или эффективен (как, скажем, при постоянном размещении на Web-сайте), но все же позволяет пользователю ОО получить необходимую информацию. С другой стороны, если бы информация была размещена на Web-сайте всего лишь на один час, причем пользователи ОО никак не оповещались об этом и не знали заранее о времени размещения, то получение ими необходимой информации было бы практически невозможно.

9.4.3 Подвид деятельности ALC_FLR.2

9.4.3.1 Цели

Цель данного подвида деятельности – сделать заключение, установил ли разработчик процедуры устранения недостатков, которые описывают отслеживание недостатков безопасности, идентификацию действий по их исправлению 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 и обеспечение уверенности, что исправления не приведут ни к каким новым недостаткам безопасности.

Для того чтобы разработчики имели возможность соответствующим образом реагировать на сообщения пользователей ОО о недостатках безопасности, пользователям ОО необходимо понимать, как представлять сообщения о недостатках безопасности разработчикам, а разработчикам необходимо знать, каким образом получать эти сообщения. 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.

9.4.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

а) документация процедур устранения недостатков;

б) руководство по устранению недостатков.

9.4.3.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ALC_FLR.2.1E.

9.4.3.3.1 Действие ALC_FLR.2.1E

ALC_FLR.2.1C

ALC_FLR.2-1 Оценщик ***должен исследовать*** документацию процедур устранения недостатков, чтобы сделать заключение, описывает ли она процедуры по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.

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) процедуры устранения недостатков для его дальнейшего отслеживания; только при этом необходимо объяснение, почему недостаток не влияет на безопасность.

ALC_FLR.2.2C

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 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".

ALC_FLR.2-3 Оценщик ***должен исследовать*** процедуры устранения недостатков, чтобы сделать заключение, будет ли идентифицирован при применении этих процедур

статус завершения исправления каждого недостатка безопасности.

Процедуры устранения недостатков идентифицируют различные стадии недостатков безопасности. Эта дифференциация, во всяком случае, 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).

ALC_FLR.2.3C

ALC_FLR.2-4 Оценщик ***должен проверить*** процедуры устранения недостатков, чтобы сделать заключение, будут ли идентифицированы при применении этих процедур действия по исправлению каждого недостатка безопасности.

Действия по исправлению могут заключаться как в коррекции аппаратных средств, программно-аппаратных средств или программ, входящих в ОО, так и в модификации руководств ОО или же включать и то, и другое. Действия по исправлению, приводящие к модификации руководств ОО (например, к детализации процедурных мер, которые необходимо предпринять для нейтрализации недостатка безопасности) включают меры, обеспечивающие как одни лишь промежуточные решения (пока коррекция не закончена), так и окончательное решение (для которого определено, что данная процедурная мера являются наилучшим решением).

Если источником недостатка безопасности является ошибка в документации, то действия по исправлению сводятся к обновлению соответствующего руководства ОО. Если действия по исправлению являются процедурной мерой, то эта мера будет включать обновление соответствующего руководства ОО для отражения корректирующих процедур.

ALC_FLR.2.4C

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), предписанных действий по исправлению и соответствующего руководства по реализации исправления.

Такая информация, материалы по исправлению и изменения документации могут быть предоставлены пользователям ОО одним из нескольких способов, таких, как размещение их на Web-сайте, рассылка пользователям ОО или заключение соглашения по инсталляции 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 поиску такой информации.

Наиболее подходящая метрика оценки достаточности метода, используемого для предоставления информации, материалов по исправлению и руководств, та, которая дает основания надеяться, что пользователи ОО смогут достать или получить их. Например, рассмотрим метод распространения, при котором необходимые данные размещаются на Web-сайте на один месяц, а пользователи ОО осведомлены, что это произойдет и когда это произойдет. Он может быть не так уж приемлем или эффективен (как, скажем, при постоянном размещении на Web-сайте), но все же позволяет пользователю ОО получить необходимую информацию. С другой стороны, если бы информация была размещена на

Web-сайте всего лишь на один час, причем пользователи ОО никак не оповещались об этом и не знали заранее о времени размещения, то получение ими необходимой информации было бы практически невозможно.

ALC_FLR.2-6 Оценщик ***должен исследовать*** процедуры устранения недостатков, чтобы сделать заключение, описывают ли они процедуры для разработчика по принятию сообщений о 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.

ALC_FLR.2.5C

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 продвижение в направлении получения окончательного решения.

Процедуры описывают процесс, начиная с момента признания предполагаемого недостатка безопасности реальным до момента принятия решения по нему.

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 каждого недостатка безопасности.

Процедуры описывают процесс, выполняемый от момента принятия решения по недостатку безопасности до момента предоставления описания действий по исправлению. Процедуры для поставки описания действий по исправлению должны быть согласованы с целями безопасности; они не обязательно идентичны процедурам, используемым для поставки ОО, документированным для удовлетворения ADO_DEL при включении компонента этого семейства в требования доверия к ОО. 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.

ALC_FLR.2.6C

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.

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.

Руководство обеспечивают наличие у пользователей ОО 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.

9.4.4 Подвид деятельности ALC_FLR.3

9.4.4.1 Цели

Цель данного подвида деятельности – сделать заключение, установил ли разработчик процедуры устранения недостатков, которые описывают отслеживание недостатков безопасности, идентификацию действий по их исправлению 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 описаний действий по исправлению недостатков.

Для того чтобы разработчики имели возможность соответствующим образом реагировать на сообщения пользователей ОО о недостатках безопасности, пользователям ОО необходимо понимать, как представлять 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.

9.4.4.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

а) документация процедур устранения недостатков;

б) руководство по устранению недостатков.

9.4.4.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ALC_FLR.3.1E.

9.4.4.3.1 Действие ALC_FLR.3.1E

ALC_FLR.3.1C

ALC_FLR.3-1 Оценщик ***должен исследовать*** документацию процедур устранения недостатков, чтобы сделать заключение, описывает ли она процедуры по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.

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) процедуры устранения недостатков для его дальнейшего отслеживания; только при этом необходимо объяснение, почему недостаток не влияет на безопасность.

ALC_FLR.3.2C

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".

ALC_FLR.3-3 Оценщик ***должен исследовать*** процедуры устранения недостатков, чтобы сделать заключение, будет ли идентифицирован при применении этих процедур статус завершения исправления каждого недостатка безопасности.

Процедуры устранения недостатков идентифицируют различные стадии недостатков безопасности. Эта дифференциация, во всяком случае, 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).

ALC_FLR.3.3C

ALC_FLR.3-4 Оценщик ***должен проверить*** процедуры устранения недостатков, чтобы сделать заключение, будут ли идентифицированы при применении этих процедур действия по исправлению каждого недостатка безопасности.

Действия по исправлению могут заключаться как в коррекции аппаратных средств, программно-аппаратных средств или программ, входящих в ОО, так и в модификации руководств ОО или же включать и то, и другое. Действия по исправлению, приводящие к модификации руководств ОО (например, к детализации процедурных мер, которые необходимо предпринять для нейтрализации недостатка безопасности) включают меры, обеспечивающие как одни лишь промежуточные решения (пока коррекция не закончена), так и окончательное решение (для которого определено, что данная процедурная мера являются наилучшим решением).

Если источником недостатка безопасности является ошибка в документации, то действия по исправлению сводятся к обновлению соответствующего руководства ОО. Если действия по исправлению являются процедурной мерой, то эта мера будет включать обновление соответствующего руководства ОО для отражения этих корректирующих процедур.

ALC_FLR.3.4C

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), предписанных действий по исправлению и соответствующего руководства по реализации исправления.

Такая информация, материалы по исправлению и изменения документации могут быть предоставлены пользователям ОО одним из нескольких способов, таких, как размещение их на Web-сайте, рассылка пользователям ОО или заключение соглашения по инсталляции 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 поиску такой информации.

Наиболее подходящая метрика оценки достаточности метода, используемого для предоставления информации, материалов по исправлению и руководств, та, которая дает основания надеяться, что пользователи ОО смогут достать или получить их. Например, рассмотрим метод распространения, при котором необходимые данные размещаются на Web-сайте на один месяц, а пользователи ОО осведомлены, что это произойдет и когда это произойдет. Он может быть не так уж приемлем или эффективен (как, скажем, при постоянном размещении на Web-сайте), но все же позволяет пользователю ОО получить необходимую информацию. С другой стороны, если бы информация была размещена на Web-сайте всего лишь на один час, причем пользователи ОО никак не оповещались об этом и не знали 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.

ALC_FLR.3-6 Оценщик ***должен исследовать*** процедуры устранения недостатков, чтобы сделать заключение, описывают ли они процедуры для разработчика по принятию сообщений о 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.

ALC_FLR.3.5C

ALC_FLR.3-7 Оценщик ***должен исследовать*** процедуры устранения недостатков, чтобы сделать заключение, способствует ли применение этих процедур исправлению 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 продвижение в направлении получения окончательного решения.

Процедуры описывают процесс, начиная с момента признания предполагаемого недостатка безопасности реальным до момента принятия решения по нему.

ALC_FLR.3-8 Оценщик ***должен исследовать*** процедуры устранения недостатков, чтобы сделать заключение, способствует ли применение этих процедур доведению до пользователей ОО действий по исправлению каждого недостатка безопасности.

Процедуры описывают процесс, выполняемый от момента принятия решения по недостатку безопасности до момента предоставления описания действий по исправлению.

Процедуры для поставки описания действий по исправлению должны быть согласованы с целями безопасности; они не обязательно идентичны процедурам, используемым для поставки ОО, документированным для удовлетворения ADO_DEL при включении компонента этого семейства в требования доверия к ОО. 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.

ALC_FLR.3.6C

ALC_FLR.3-9 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.

ALC_FLR.3-10 Оценщик ***должен исследовать*** руководство по устранению недостатков, чтобы сделать заключение, предоставит ли применение этого руководства пользователю ОО способ представления сообщений о предполагаемых недостатках или запросов на исправление таких недостатков.

Руководство обеспечивают наличие у пользователей ОО 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.

ALC_FLR.3.7C

ALC_FLR.3-11 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, 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.

ALC_FLR.3-12 Оценщик ***должен исследовать*** процедуры устранения недостатков, чтобы сделать заключение, будет ли результатом применения этих процедур автоматическое распространение сообщений о недостатках безопасности и материалов по их исправлению зарегистрированным пользователям, для которых эти недостатки могут иметь последствия.

Автоматическое распространение не подразумевает автоматизма, т.е. полного исключения участия человека в распространении. В действительности, метод распространения может состоять полностью из ручных процедур, возможно, с использованием строго контролируемой процедуры, предписывающей усиление мер контроля за недостатками выпуска 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 для всех недостатков безопасности при условии, что это делается автоматически.

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 выполняться как часть стандартных процедур, которым подвергаются пользователи 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 убедиться 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).

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.

9.5 Оценка определения жизненного цикла

9.5.1 Подвид деятельности ALC_LCD.1

9.5.1.1 Цели

Цель данного подвида деятельности - сделать заключение, использовал ли разработчик задокументированную модель жизненного цикла ОО.

9.5.1.2 Исходные данные

Свидетельствами опенки для этого подвида деятельности являются:

а) ЗБ;

б) документация определения жизненного пикта.

9.5.1.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ALC_LCD.1.1E.

9.5.1.3.1 Действие ALC_LCD.1.1E

ALC_LCD.1.1C

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.

Модель жизненного цикла распространяется на процедуры, инструментальные средства и методы, используемые при разработке и сопровождении ОО. В описание модели жизненного цикла должна быть включена информация о процедурах, инструментальных средствах и методах, используемых разработчиком (например, при проектировании, кодировании, тестировании, исправлении ошибок). В ней должны быть описаны общая структура управления применением процедур (например, идентификация и описание персональной ответственности за каждую из процедур, требуемых в процессе разработки и сопровождения ОО согласно модели жизненного цикла). ALC_LCD.1 не содержит требования соответствия используемой модели какой-либо стандартизованной модели жизненного цикла.

ALC_LCD.1.2C

A.LC_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 вид деятельности АСМ). Выявленным недостаткам в модели жизненного цикла следует уделить особое внимание, если можно ожидать, что они приведут к случайному или преднамеренному внесению ошибок в ОО.

ОК не навязывают какой-либо конкретный подход к разработке; следует оценить 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.

9.5.2 Подвид деятельности ALC_LCD.2

9.5.2.1 Цели

Цель данного подвида деятельности - сделать заключение, использовал ли разработчик задокументированную и стандартизованную модель жизненного цикла ОО.

9.5.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) документация определения жизненного цикла.

9.5.2.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ALC_LCD.2.1E.

9.5.2.3.1 Действие ALC_LCD.2.1E

ALC_LCD.2.1C

ALC_LCD.2-1 Оценщик ***должен исследовать*** документированное описание модели используемого жизненного цикла, чтобы сделать заключение, распространяется ли она на процессы разработки и сопровождения ОО.

Модель жизненного цикла распространяется на процедуры, инструментальные средства и методы, используемые при разработке и сопровождении ОО. В описание модели жизненного цикла должна быть включена информация о процедурах, инструментальных средствах и методах, используемых разработчиком (например, при проектировании, кодировании, тестировании, исправлении ошибок). В ней должны быть описаны общая структура управления применением процедур (например, идентификация и описание персональной ответственности за каждую из процедур, требуемых в процессе разработки и сопровождения ОО согласно модели жизненного цикла).

ALC_LCD.2.2C

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 вид деятельности АСМ). Выявленным недостаткам в модели жизненного цикла следует уделить особое внимание, если можно ожидать, что они приведут к случайному или преднамеренному внесению ошибок в ОО.

ОК не навязывают какой-либо конкретный подход к разработке; следует оценить 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.

ALC_LCD.2.3C

ALC_LCD.2-3 Оценщик ***должен исследовать*** документацию определения жизненного цикла, чтобы сделать заключение, содержит ли она объяснение, почему выбрана именно эта модель.

Оценщику следует исследовать документацию определения жизненного цикла, чтобы сделать заключение, представлены ли в ней основания для принятия выбранной модели жизненного цикла. Такие основания могут включать, например, соответствие политике организации или же отражать предполагаемые преимущества использования конкретной модели жизненного цикла.

ALC_LCD.2.4C

ALC_LCD.2-4 Оценщик ***должен исследовать*** документацию определения жизненного цикла, чтобы сделать заключение, содержит ли она объяснение, как применяется стандартизованная модель при разработке и сопровождении данного ОО.

В то время как требования в ALC_LCD.1 ограничены описанием используемой модели жизненного цикла, элемент ALC_LCD.2.4C из ОК содержит требование, чтобы разработчик объяснил, как применяется модель к оцениваемому ОО. Необходимо, чтобы это объяснение охватило любую адаптацию стандартизованной модели для удовлетворения требований конкретного ОО или организационных требований.

ALC_LCD.2.5C

ALC_LCD.2_5 Оценщик ***должен исследовать*** документацию определения жизненного цикла, чтобы сделать заключение, демонстрирует ли она соответствие используемой модели жизненного цикла стандартизованной модели.

В документации определения жизненного цикла должны быть соотнесены аспекты стандартизованной модели и конкретных процедур разработки и сопровождения для данного ОО так, чтобы соответствие стандартизованной модели могло быть легко подтверждено оценщиком. Свидетельство соответствия может, например, содержать отображение детальных шагов и ролей, определенных для организации, из стандартизованной модели в отдельных процедурах разработки и ролях или персонале из среды разработки.

По завершении шага оценивания ALC_LCD.2_4 и данного шага оценивания, оценщик должен получить ясное понимание того, как применяется стандартизованная модель, и что она применяется корректно.

9.6 Оценка инструментальных средств и методов

9.6.1 Подвид деятельности ALC_TAT.1

9.6.1.1 Цели

Цель данного подвида деятельности - сделать заключение, использовал ли разработчик для разработки, анализа и реализации ОО полностью определенные инструментальные средства, которые дают непротиворечивые и предсказуемые результаты.

9.6.1.2 Исходные данные

Свидетельством опенки для этого подвида деятельности является документация инструментальных средств.

9.6.1.3 Замечания по применению

Эта работа может выполняться в сочетании с видом деятельности ADV при условии применения соответствующих требований доверия, в особенности в отношении определения того, какие свойства инструментальных средств окажут влияние на предоставленное представление.

9.6.1.4 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ALC_TAT.1.1E.

9.6.1.4.1 Действие ALC_TAT.1.1E

ALC_TAT.1.1C

ALC_TAT.1-1 Оценщик ***должен исследовать*** документацию, инструментальных средств, чтобы сделать заключение, все ли инструментальные средства, используемые для разработки, анализа и реализации ОО, полностью определены. Это требование относится ко всем используемым инструментальным средствам. В их число включены инструментальные средства для разработки проекта верхнего уровня, проекта нижнего уровня и представления реализации.

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.

ALC_TAT.1.2C

ALC_TAT.1-2 Оценщик ***должен исследовать*** документацию инструментальных средств, чтобы сделать заключение, однозначно ли определены в ней значения всех конструкций, используемых в представлении реализации.

В документации инструментальных средств разработки (например, в спецификациях языка программирования и в руководствах пользователя) должны быть охвачены все конструкции, используемые в представлении реализации ОО, и для каждой такой конструкции должно быть предоставлено 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.1 (при условии заявления соответствующих требований доверия). Главные усилия оценщика следует направить на выяснение того, действительно ли документация достаточно ясна для понимания представления реализации. Например, документация не должна предполагать, что читатель является экспертом по используемому языку программирования.

В большинстве широко используемых языков программирования, хотя и тщательно спроектированных, не исключено наличие некоторых проблемных конструкций. Если

язык реализаций определен "почти" полностью, но при этом в нем все же имеются некоторые проблемные конструкции, то не следует делать определенного заключения до проведения исследования исходного текста.

ALC_TAT.1.3C

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 должны быть включены определения опций, обусловленных реализацией, которые могут повлиять на выполняемый код, и тех, которые отличаются от стандарта используемого языка. В случаях, когда оценщику предоставляется исходный текст, ему также должна быть предоставлена информация по используемым опциям компиляции и сборки.

В документации инструментальных средств проектирования и разработки аппаратных средств должно быть описано использование всех опций, которые влияют на результаты применения инструментальных средств (например, детальные аппаратные спецификации или сами аппаратные средства).

ALC_TAT.1-4 Оценщик ***должен исследовать*** документацию инструментальных средств, чтобы сделать заключение, поддерживают ли инструментальные средства разработки корректную реализацию ОО.

На этом шаге оценивания от оценщика не требуется проведения непосредственного исследования самого инструментального средства. Оценщик может провести анализ представления реализации в сочетании с подвидом деятельности ADV_IMP.*. При анализе правильности представления реализации этот шаг оценивания может быть выполнен в сочетании с видом деятельности АТЕ.

9.6.2 Подвид деятельности ALC_TAT.2

9.6.2.1 Цели

Цель данного подвила деятельности - сделать заключение, использовал ли разработчик для разработки, анализа и реализации ОО полностью определенные инструментальные средства, которые лают непротиворечивые и предсказуемые результаты, и использовались ли стандарты реализации.

9.6.2.2 Исходные данные

Свидетельством опенки для этого подвида деятельности являются:

а) документация инструментальных средств;

б) описание стандартов реализации;

в) предоставленное представление реализации ФБО.

9.6.2.3 Замечания по применению

Эта работа может выполняться в сочетании с видом деятельности ADV при условии применения соответствующих требований доверия, в особенности в отношении определения того, какие свойства инструментальных средств окажут влияние на предоставленное представление.

9.6.2.4 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а) ALC_TAT.2.1E;

б) ALC_TAT.2.2E.

9.6.2.4.1 Действие ALC_TAT.2.1E

ALC_TAT.2.1C

ALC_TAT.2-1 Оценщик ***должен исследовать*** документацию инструментальных средств, чтобы сделать заключение, все ли инструментальные средства, используемые для

разработки, анализа и реализации ОО, полностью определены.

Это требование относится ко всем используемым инструментальным средствам. В их число включены инструментальные средства для разработки проекта верхнего уровня, проекта нижнего уровня и представления реализации.

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.

ALC_TAT.2.2C

ALC_TAT.2-2 Оценщик ***должен исследовать*** документацию инструментальных средств, чтобы сделать заключение, однозначно ли определены в ней значения всех конструкций, используемых в представлении реализации.

В документации инструментальных средств разработки (например, в спецификациях языка программирования и в руководствах пользователя) должны быть охвачены все конструкции, используемые в представлении реализации ОО, и для каждой такой конструкции должно быть предоставлено 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.1 (при условии заявления соответствующих требований доверия). Главные усилия оценщика следует направить на выяснение того, действительно ли документация достаточно ясна для понимания представления реализации. Например, документация не должна предполагать, что читатель является экспертом по используемому языку программирования.

В большинстве широко используемых языков программирования, хотя и тщательно спроектированных, не исключено наличие некоторых проблемных конструкций. Если язык реализаций определен "почти" полностью, но при этом в нем все же имеются некоторые проблемные конструкции, то до проведения исследования исходного текста следует сделать лишь предварительное заключение.

ALC_TAT.2.3C

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 должны быть включены определения опций, обусловленных реализацией, которые могут повлиять на выполняемый код, и тех, которые отличаются от стандарта используемого языка. В случаях, когда оценщику предоставляется исходный текст, ему также должна быть предоставлена информация по используемым опциям компиляции и сборки.

В документации инструментальных средств проектирования и разработки аппаратных средств должно быть описано использование всех опций, которые влияют на результаты применения инструментальных средств (например, детальные аппаратные спецификации или сами аппаратные средства).

ALC_TAT.2-4 Оценщик ***должен исследовать*** документацию инструментальных средств, чтобы сделать заключение, поддерживают ли инструментальные средства разработки и стандарты реализации корректную реализацию ОО.

На этом шаге оценивания от оценщика не требуется проведения непосредственного исследования самого инструментального средства. Оценщик может провести анализ представления реализации в сочетании с подвидом деятельности ADV_IMP.*. При анализе правильности представления реализации этот шаг оценивания может быть выполнен в сочетании с видом деятельности ATE.

9.6.2.4.2 Действие ALC_TAT.2.2E

ALC_TAT.2-5 Оценщик ***должен исследовать*** предоставленное представление реализации, чтобы сделать заключение, применялись ли стандарты реализации.

Оценщик сравнивает предоставленное представление реализации с описанием применявшихся стандартов реализации и верифицирует их использование. На этом уровне не требуется, чтобы предоставленное представление реализации всех ФБО базировалось на стандартах реализации. Требуется всего лишь, чтобы те стандарты реализации, на которые ссылался разработчик, действительно применялись. Если упомянутые стандарты реализации не применялись, по меньшей мере, к части предоставленного представления реализации, то по этому шагу оценивания делается отрицательное заключение.

Этот шаг оценивания может быть выполнен в сочетании с подвидами деятельности ADV_IMP.*.

9.6.3 Подвид деятельности ALC_TAT.3

9.6.3.1 Цели

Цель данного подвида деятельности - сделать заключение, использовал ли разработчик для разработки, анализа и реализации ОО полностью определенные инструментальные средства, которые дают непротиворечивые и предсказуемые результаты, и применялись ли стандарты реализации ко всем ФБО.

9.6.3.2 Исходные данные

Свидетельством опенки для этого подвида деятельности являются:

а) документация инструментальных средств;

б) описание стандартов реализации;

в) предоставленное представление реализации ФБО.

9.6.3.3 Замечания по применению

Эта работа может выполняться в сочетании с видом деятельности ADV при условии применения соответствующих требований доверия, в особенности в отношении определения того, какие свойства инструментальных средств окажут влияние на предоставленное представление.

9.6.3.4 Действия оценщика

Этот подвид деятельности включает три элемента действий оценщика из части 3 ОК:

а) ALC_TAT.3.1E;

б) ALC_TAT.3.2E;

в) Подразумеваемое действие оценщика, основанное на ALC_TAT.3.3Д.

9.6.3.4.1 Действие ALC_TAT.3.1E

ALC_TAT.3.1C

ALC TAT.3-1 Оценщик ***должен исследовать*** документацию инструментальных средств, чтобы сделать заключение, все ли инструментальные средства, используемые для разработки, анализа и реализации ОО. полностью определены.

Это требование относится ко всем используемым инструментальным средствам. В их число включены инструментальные средства для разработки проекта верхнего уровня, проекта нижнего уровня и представления реализации.

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.

ALC_TAT.3.2C

ALC_TAT.3-2 Оценщик ***должен исследовать*** документацию инструментальных средств, чтобы сделать заключение, однозначно ли определены в ней значения всех конструкций, используемых в представлении реализации.

В документации инструментальных средств разработки (например, в спецификациях языка программирования и в руководствах пользователя) должны быть охвачены все конструкции, используемые в представлении реализации ОО, и для каждой такой конструкции должно быть предоставлено 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.1. (при условии заявления соответствующих требований доверия). Главные усилия оценщика следует направить на выяснение того, действительно ли документация достаточно ясна для понимания представления реализации. Например, документация не должна предполагать, что читатель является экспертом по используемому языку программирования.

В большинстве широко используемых языков программирования, хотя и тщательно спроектированных, не исключено наличие некоторых проблемных конструкций. Если язык реализаций определен "почти" полностью, но при этом в нем все же имеются некоторые проблемные конструкции, то до проведения исследования исходного текста следует сделать лишь предварительное заключение.

ALC_TAT.3.3C

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 должны быть включены определения опций, обусловленных реализацией, которые могут повлиять на выполняемый код, и тех, которые отличаются от стандарта используемого языка. В случаях, когда оценщику предоставляется исходный текст, ему также должна быть предоставлена информация по используемым опциям компиляции и сборки.

В документации инструментальных средств проектирования и разработки аппаратных средств должно быть описано использование всех опций, которые влияют на результаты применения инструментальных средств (например, детальные аппаратные спецификации или сами аппаратные средства).

ALC_TAT.3-4 Оценщик ***должен исследовать*** документацию инструментальных средств, чтобы сделать заключение, поддерживают ли инструментальные средства разработки и стандарты реализации корректную реализацию ОО.

На этом шаге оценивания от оценщика не требуется проведения непосредственного исследования самого инструментального средства. Оценщик может провести анализ представления реализации в сочетании с подвидом деятельности ADV_IMP.*. При анализе правильности представления реализации этот шаг оценивания может быть выполнен в сочетании с видом деятельности ATE.

9.6.3.4.2 Действие ALC_TAT.3.2E

ALC_TAT.3-5 Оценщик ***должен исследовать*** предоставленное представление реализации, чтобы сделать заключение, применялись ли стандарты реализации.

Оценщик сравнивает предоставленное представление реализации с описанием применявшихся стандартов реализации и верифицирует их использование. На этом уровне не требуется, чтобы предоставленное представление реализации всех ФБО базировалось на стандартах реализации. Требуется всего лишь, чтобы те стандарты реализации, на которые ссылался разработчик, действительно применялись. Если упомянутые стандарты реализации не применялись, по меньшей мере, к части предоставленного представления реализации, то по этому шагу оценивания делается отрицательное заключение.

Этот шаг оценивания может быть выполнен в сочетании с подвидами деятельности ADV_IMP.*.

9.6.3.4.3 Подразумеваемое действие оценщика

9.6.3.4.4 ALC_TAT.3.3Д

A1C_TAT.3-6 Оценщик ***должен исследовать*** представление реализации, чтобы сделать заключение, применялись ли стандарты реализации к полной совокупности ФБО.

Оценщик сравнивает представление реализации с описанием применявшихся стандартов реализации и верифицирует их использование. На этом уровне требуется, чтобы полное представление реализации ФБО базировалось на тех стандартах реализации, на которые сослался разработчик.

Оценщику следует удостовериться, что конструкции, запрещенные указанными стандартами, не используются. Любые отклонения от стандартов приводят к отрицательному заключению по этому шагу оценивания.

Этот шаг оценивания может быть выполнен в сочетании с подвидами деятельности ADV_IMP.*.

10 Вид деятельности ATE

10.1 Введение

Вид деятельности «Тестирование» позволяет сделать заключение, функционирует ли ОО в соответствии с тем, как определено в проектной документации, и в соответствии с функциональными требованиями безопасности ОО, определенными в ЗБ.

10.2 Цели

Вид деятельности «Тестирование" предназначен для того, чтобы сделать заключение, функционирует ли ОО в соответствии с тем, как определено в проектной документации и в соответствии с функциональными требованиями безопасности ОО. определенными в ЗБ. Данная цель достигается путем вынесения заключения о проведении разработчиком тестирования ФБО на их соответствие функциональной спецификации, проекту верхнего уровня и проекту нижнего уровня, повышая уверенность в результатах тестирования путем выборочного выполнения тестов разработчика, а также путем проведения независимого тестирования некоторого подмножества ФБО.

10.2.1 Комментарии по применению

Объем и состав подмножества тестов оценщика зависят от нескольких факторов, рассматриваемых в подвидах деятельности, связанных с независимым тестированием. Один из таких факторов, оказывающих влияние на состав подмножества тестов - это известные из общедоступных источников слабые места, к информации о которых оценщику необходимо получить доступ (например, в рамках системы подтверждения соответствия).

Для повышения гибкости применения компонентов семейств в ОК вопросы покрытия тестами и глубины тестирования рассмотрены отдельно от функциональных тестов. Тем не менее, требования соответствующих семейств предназначены для совместного применения в пенях подтверждения, что ФБО выполняются согласно их спецификации. Такая тесная связь семейств привела к некоторому дублированию работы оценщика по подвидам деятельности. Настоящие замечания по применению используются для минимизации повторения текста при описании подвидов деятельности одного и того же вида деятельности.

10.2.1.1 Понимание ожидаемого режима функционирования ОО

Прежде, чем адекватность 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,

В какой то момент времени оценщик может сосредоточиться на одной функции ФБО. Для каждой функции безопасности оценщик исследует конкретное требование ЗБ и соответствующие части функциональной спецификации, проекта верхнего уровня и руководств для понимания ожидаемого режима функционирования ОО.

Понимая ожидаемый режим функционирования ОО, оценщик исследует план тестирования, чтобы понять подход к тестированию. В большинстве случаев подход к тестированию будет предусматривать инициирование выполнения некоторой функции безопасности через внешние или внутренние интерфейсы и наблюдение ее реакции. Тем не менее, могут быть случаи, когда функция безопасности 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.

10.2.1.2 Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности

В тех случаях, когда практически нецелесообразно или несоразмерно осуществлять тестирование через интерфейс, в плане тестирования должен быть определен альтернативный подход к верификации ожидаемого режима выполнения. Сделать заключение о пригодности альтернативного подхода - обязанность оценщика. Оценивая пригодность альтернативных подходов, следует учесть, что:

а) приемлемым альтернативным подходом является анализ представления реализации, для заключения, что требуемый режим функционирования будет демонстрироваться ОО. Это может означать экспертизу кода для программного ОО или возможно экспертизу фотошаблона (маски) микросхем для аппаратного ОО.

б) приемлемым является использование свидетельства помодульного или интегрированного тестирования разработчиком, даже если это не соизмеримо с представленными на оценку проектом нижнего уровня пли реализацией. 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 потребуется 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. Такая альтернатива дает возможность разработчику минимизировать затраты (времени и/или денег) на тестирование при описанных выше обстоятельствах: она не предназначена для того, чтобы дать оценщику большую свободу требовать произвольную дополнительную информацию относительно ОО, а также для того, чтобы вообще заменить тестирование.

10.2.1.3 Верификация адекватности тестов

Для тестов необходимо заранее установить требуемые начальные условия их выполнения. Они могут быть определены через параметры, которые должны быть установлены, или через упорядочение 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 смешению наблюдаемых результатов тестирования по отношению 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 из себя представляют. Оценщик должен сделать заключение о согласованности шагов тестирования и ожидаемых результатов тестирования с функциональной спецификацией и проектом верхнего уровня. Тесты должны верифицировать задокументированный в этих спецификациях режим выполнения. Это означает, что для каждой характеристики режима выполнения функции безопасности, явным образом описанной в функциональной спецификации и проекте верхнего уровня, следует иметь тесты и описание ожидаемых результатов тестирования, чтобы верифицировать данный режим выполнения.

Несмотря на то, что все ФБО должны тестироваться разработчиком, исчерпывающее тестирование интерфейсов спецификации не требуется. Основная цель данного вида деятельности состоит в том, чтобы сделать заключение о достаточности тестирования каждой функции безопасности на соответствие заявленным в функциональной спецификации и проекте верхнего уровня режимам выполнения. Процедуры тестирования должны обеспечить понимание того, каким образом разработчиком в ходе тестирования опробовались функции безопасности. Оценщик будет использовать данную информацию при разработке дополнительных тестов для независимого тестирования ОО.

10.3 Оценка обеспеченности

10.3.1 Подвид деятельности ATE_COV.1

10.3.1.1 Цели

Цель данного подвида деятельности - сделать заключение, показывает ли свидетельство разработчика о достаточности тестов разработчика и соответствие их тестам, идентифицированным в тестовой документации и функциональной спецификации.

10.3.1.2 Замечания по применению

Материалы анализа покрытия тестами, представляемые разработчиком, требуются для того, чтобы показать соответствие между тестами, предоставленными в качестве свидетельства опенки, и функциональной спецификацией. Однако нет необходимости в том, чтобы в материалах анализа покрытия демонстрировалось, что все функции безопасности были подвергнуты тестированию, или, что все внешние интерфейсы ФБО были подвергнуты тестированию. Подобные недостатки, если они имеют место, рассматриваются оценщиком в процессе выполнения подвида деятельности по независимому тестированию.

10.3.1.3 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

а) функциональная спецификация:

б) тестовая документация;

в) свидетельство о покрытии тестами.

10.3.1.4 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК: а)ATE_COV.1.1E.

10.3.1.4.1 Действие ATE_COV.1.1E

ATE_COV.1.1C

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 функциональной спецификацией.

Соответствие может принимать форму таблицы или матрицы. Свидетельство о покрытии тестами, требуемое для рассматриваемого компонента, скорее должно показать степень покрытия тестами, а не его полноту. В тех случаях, когда показана недостаточность покрытия, оценщику, чтобы это компенсировать, следует повысить уровень независимого тестирования.

На рисунке 10.1 отражена концептуальная структура соответствия между функциями безопасности, описанными в функциональной спецификации, и тестами, выделенными в тестовой документации для тестирования этих функций. Тесты могут затрагивать одну или несколько функций безопасности, что может быть обусловлено зависимостями тестов или общей целью выполняемого теста.

Идентификация тестов и функций безопасности, представленных в свидетельстве о покрытии тестами, должна быть однозначной, обеспечивая четкое соответствие между идентифицированными тестами и функциональной спецификацией тестируемых функций безопасности.

На рисунке 10.1 функция безопасности ФБ-3 не сопоставлена с какими бы то ни было тестами: следовательно, относительно функциональной спецификации покрытие тестами является неполным. Неполное покрытие, тем не менее, не будет влиять на заключение по рассматриваемому подвиду деятельности, поскольку свидетельство о покрытии тестами не обязательно должно показывать полное покрытие тестами идентифицированных в функциональной спецификации функций безопасности.

10.3.2 Подвид деятельности ATE_COV.2

10.3.2.1 Цель

Цель данного подвида деятельности - сделать заключение, является ли тестирование (как это документально зафиксировано) достаточным, чтобы установить, что ФБО были систематическим метолом протестированы на соответствие функциональной спецификации.

10.3.2.2 Исходные данные

а) ЗБ;

б) функциональная спецификация;

в) тестовая документация;

г) материалы анализа покрытия тестами.

10.3.2.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ATE_COV.2.1E.

10.3.2.3.1 Действие ATE_COV.2.1E

ATE_COV.2.1C

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 функциональной спецификацией.

Соответствие может принимать форму таблицы или матрицы. В некоторых случаях, чтобы показать соответствие тестов может оказаться достаточным наличие такого отображения. В других случаях может потребоваться некоторое обоснование (на естественном языке) для того, чтобы дополнить материалы анализа соответствия, представленные разработчиком.

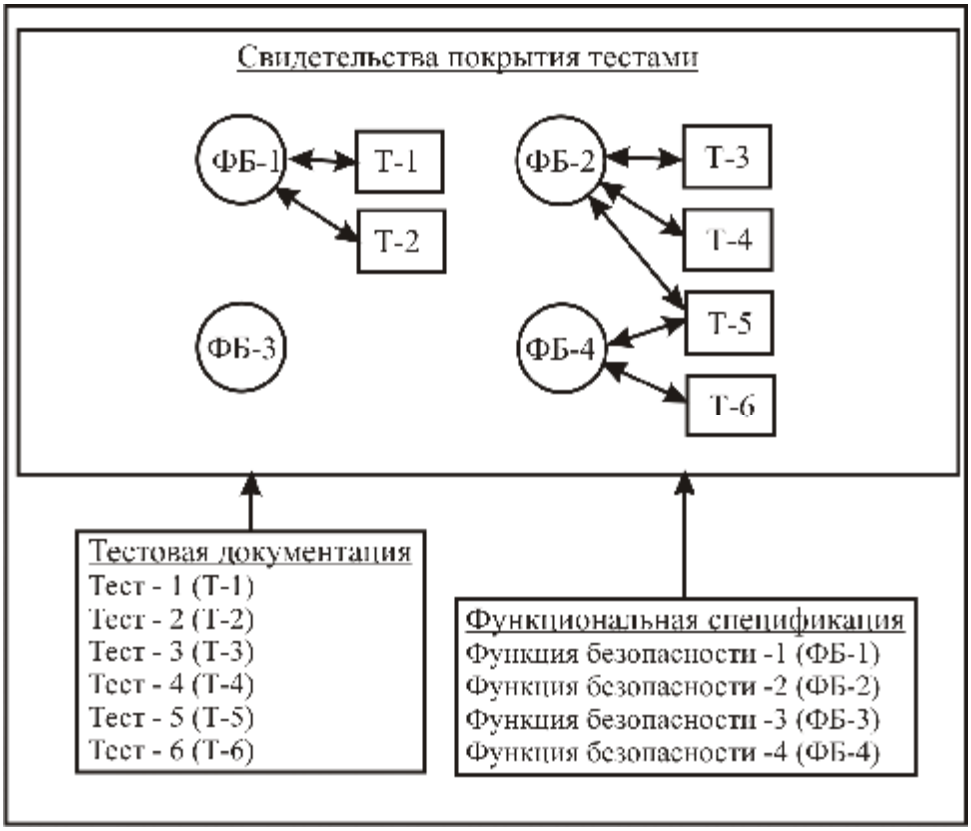


Рисунок 10.1 -Концептуальная структура свидетельства покрытия тестами

На рисунке 10.2 отражена концептуальная структура соответствия между функциями безопасности, описанными в функциональной спецификации, и тестами, выделенными в тестовой документации для тестирования этих функций. Тесты могут затрагивать одну или несколько функции безопасности, что может быть обусловлено зависимостями тестов или общей целью выполняемого теста.

Идентификация тестов и функций безопасности, представленных в материалах анализа покрытия тестами, должна быть однозначной. Материалы анализа покрытия тестами должны позволить оценщику сопоставить идентифицированные тесты с тестовой документацией, а тестируемые функции безопасности - с функциональной спецификацией.

ATE_COV.2-2 Оценщик ***должен исследовать*** план тестирования, чтобы сделать заключение, является ли подход к тестированию каждой функции безопасности ФБО пригодным для демонстрации ожидаемого режима ее выполнения.

Руководство по выполнению этого шага оценивания можно найти в следующих Замечаниях по применению:

а) Понимание ожидаемого режима функционирования ОО (см. 10.2.1.1);

б) Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности (см. 10.2.1.2).

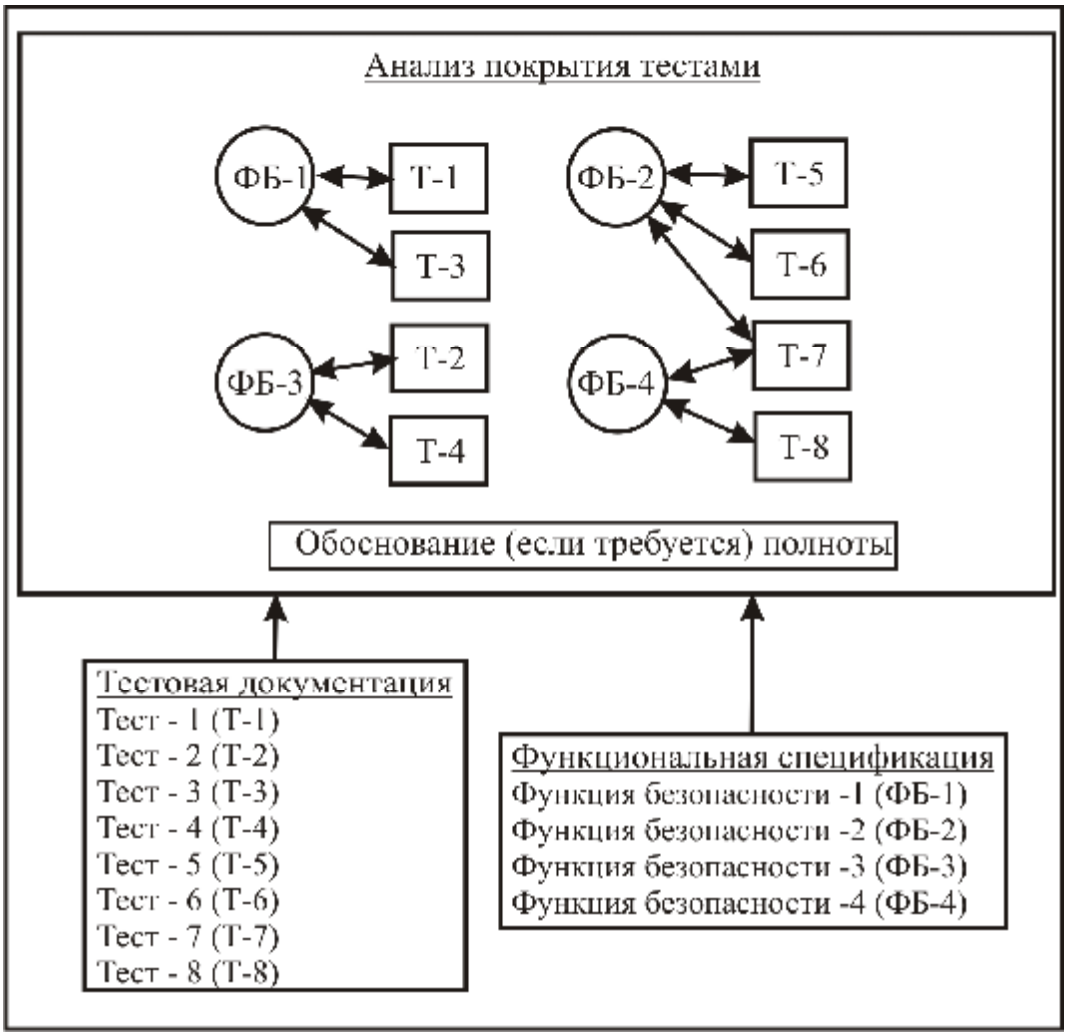


Рисунок 10.2 - Концептуальная структура анализа покрытия тестами

ATE_COV.2-3 Оценщик ***должен исследовать*** процедуры тестирования, чтобы сделать заключение, адекватно ли описание предварительных условий тестирования, шагов тестирования и ожидаемого результата (ожидаемых результатов) для тестирования каждой функции безопасности.

Руководство по выполнению этого шага оценивания, который относится к функциональной спецификации, можно найти в Замечаниях по применению «Верификация адекватности тестов» (см. 10.2.1.3).

ATE_COV.2.2C

ATE_COV.2-4 Оценщик ***должен исследовать*** материалы анализа покрытия тестами, чтобы сделать заключение о полноте соответствия между ФБО, описанными в функциональной спецификации, и тестами, идентифицированными в тестовой документации.

Все функции безопасности и 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. Как показано на рисунке 10.2, для всех функций безопасности имеются относящиеся к ним тесты, а, следовательно, в данном примере продемонстрировано полное покрытие тестами. Неполнота покрытия была бы очевидна,

если бы некоторая функция безопасности была идентифицирована в материалах анализа покрытия тестами, но никакие тесты не могли быть к ней отнесены.

10.4 Оценка глубины

10.4.1 Подвид деятельности ATE_DPT.1

10.4.1.1 Цели

Цель данного подвида деятельности - сделать заключение, тестировал ли разработчик ФБО на соответствие проекту верхнего уровня.

10.4.1.2 Исходные данные

а) ЗБ;

б) функциональная спецификация;

в) проект верхнего уровня;

г) тестовая документация;

д) материалы анализа глубины тестирования.

10.4.1.3 Действия оценщика

Этот подвид деятельности включает одни элемент действий оценщика из части 3 ОК:

а) ATE_DPT.1.1E

10.4.1.3.1 Действие ATE_DPT.1.1E

ATE_DPT.1.1C

ATE_DPT.1-1 Оценщик ***должен исследовать*** материалы анализа глубины тестирования на предмет сопоставления тестов, идентифицированных в тестовой документации, и проекта верхнего уровня.

В материалах анализа глубины тестирования идентифицируются все подсистемы, описанные в проекте верхнего уровня, и представляется сопоставление тестов с этими подсистемами. Соответствие может принимать форму таблицы или матрицы. В некоторых случаях, чтобы показать соответствие тестов может оказаться достаточным наличие такого отображения. В других случаях может потребоваться некоторое обоснование (на естественном языке) для того, чтобы дополнить материалы анализа соответствия, представленные разработчиком.

Все детали проекта, специфицированные в проекте верхнего уровня, сопоставленные с требованиями безопасности ОО и удовлетворяющие им, являются предметом тестирования, а, следовательно, должны быть сопоставлены с тестовой документацией. На рисунке 10.3 отражена концептуальная структура сопоставления подсистем, описанных в проекте верхнего уровня, и тестов, изложенных в тестовой документации ОО и используемых для их тестирования. Тесты могут затрагивать одну или несколько функций безопасности, что может быть обусловлено зависимостями между тестами или обшей целью выполняемого теста.

ATE_DPT.1-2 Оценщик ***должен исследовать*** план тестирования разработчика, чтобы сделать заключение, является ли подход к тестированию каждой функции безопасности ФБО пригодным для демонстрации ожидаемого режима ее выполнения.

Руководство по выполнению этого шага оценивания можно найти в следующих Замечаниях по применению:

а) Понимание ожидаемого режима функционирования ОО (см. 10.2.1.1);

б) Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности (см. 10.2.1.2).

Тестирование ФБО может быть выполнено 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 строгое обоснование, остается за оценщиком.

ATE_DPT.1-3 Оценщик ***должен исследовать*** процедуры тестирования, чтобы сделать заключение, адекватно ли описание предварительных условий тестирования, шагов тестирования и ожидаемого результата (ожидаемых результатов) для тестирования каждой функции безопасности.

Руководство по выполнению этого шага оценивания, который относится к проекту верхнего уровня, можно найти в Замечаниях по применению «Верификация адекватности тестов» (см. 10.2.1.3).

ATE_DPT.1-4 Оценщик ***должен проверить*** материалы анализа глубины тестирования, чтобы удостовериться, что ФБО в том виде, в котором они определены в проекте верхнего уровня, полностью сопоставлены с тестами, представленными в тестовой документации.

Материалы анализа глубины тестирования обеспечивают полное изложение соответствия между проектом верхнего уровня, планом и процедурами тестирования. Все подсистемы и внутренние интерфейсы, описанные в проекте верхнего уровня, должны быть представлены в материалах анализа глубины тестирования. Для всех подсистем и внутренних интерфейсов, представленных в материалах анализа глубины тестирования, должны иметься сопоставленные с ними тесты для того, чтобы можно было утверждать о полноте. Как показано на рисунке 10.3, для всех подсистем и внутренних интерфейсов имеются относящиеся к ним тесты, а, следовательно, в данном примере продемонстрирована полнота глубины тестирования. Неполнота тестирования была бы очевидна, если бы подсистема или внутренний интерфейс были идентифицированы в материалах анализа глубины тестирования, но никакие тесты не могли быть к ним отнесены.

10.4.2 Подвид деятельности ATE_DPT.2

10.4.2.1 Цели

Цель данного подвида деятельности - сделать заключение, тестировал ли разработчик ФБО а соответствие проекту верхнего уровня и проекту нижнего уровня.

10.4.2.2 Исходные данные

а) ЗБ;

б) функциональная спецификация;

в) проект верхнего уровня;

г) проект нижнего уровня;

д) тестовая документация;

е) материалы анализа глубины тестирования.

10.4.2.3 Действия оценщика

Этот подвид деятельности включает один элемент действий оценщика из части 3 ОК:

а) ATE_DPT.2.1E.

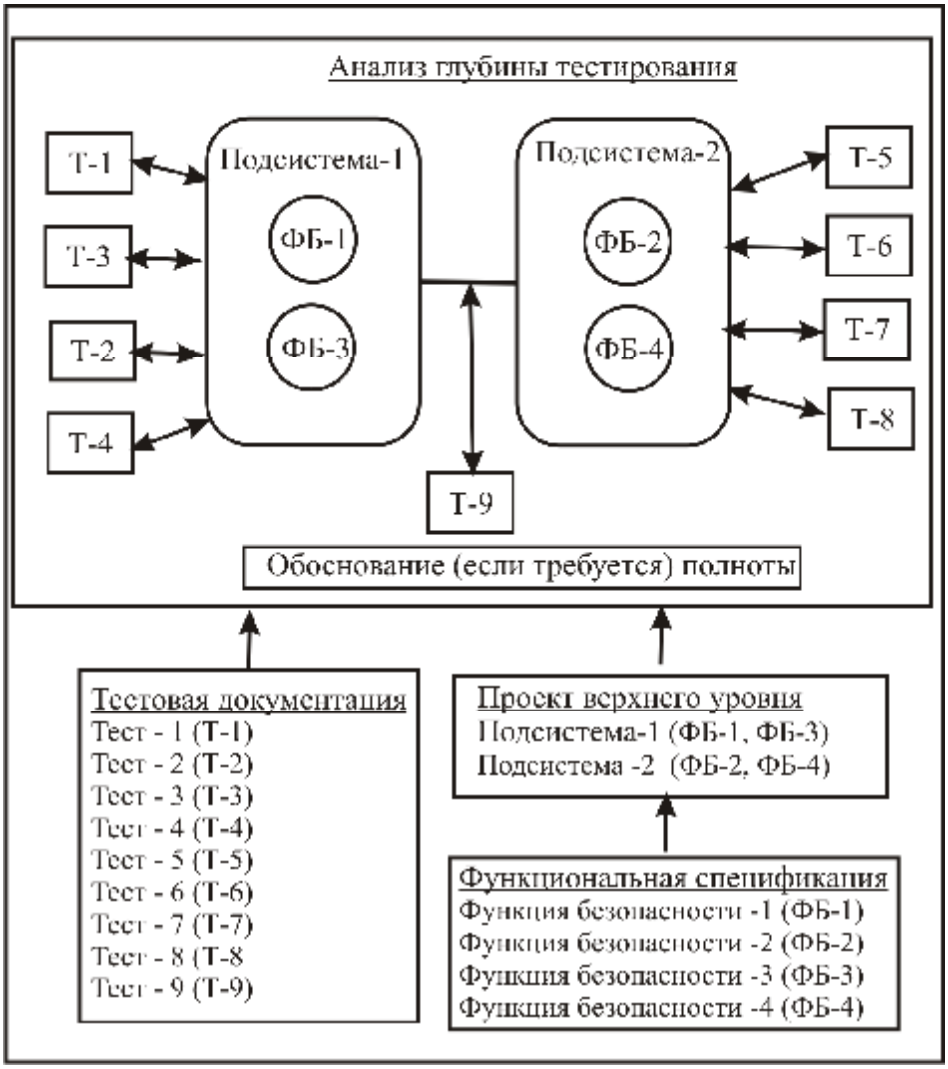


Рисунок 10.3 - Концептуальная структура анализа глубины тестирования

10.4.2.3.1 Действие ATE_DPT.2.1E

ATE_DPT.2.1C

ATE_DPT.2-1 Оценщик ***должен исследовать*** материалы анализа глубины тестирования для сопоставления тестов, идентифицированных в тестовой документации, проекта верхнего уровня и проекта нижнего уровня.

В материалах анализа глубины тестирования идентифицируются все подсистемы, определенные в проекте верхнего уровня, и все модули, описанные в проекте нижнего уровня, и демонстрируется сопоставление тестов с этими подсистемами и модулями. Соответствие может принимать форму таблицы или матрицы. В некоторых случаях, чтобы показать соответствие тестов может оказаться достаточным наличие такого отображения. В других случаях может потребоваться некоторое обоснование (на естественном языке) для того, чтобы дополнить материалы анализа соответствия, представленные разработчиком.

Все детали проекта, специфицированные в проекте верхнего уровня и проекте нижнего уровня, сопоставленные с требованиями безопасности ОО и удовлетворяющие им, являются предметом тестирования, а, следовательно, должны быть сопоставлены с тестовой документацией. На рисунке 10.4 отражена концептуальная структура

сопоставления подсистем, описанных в проекте верхнего уровня, модулей, описанных в проекте нижнего уровня, и тестов, изложенных в тестовой документации ОО и используемых для их тестирования. Тесты могут затрагивать одну или несколько функций безопасности, что может быть обусловлено зависимостями между тестами или общей целью выполняемого теста.

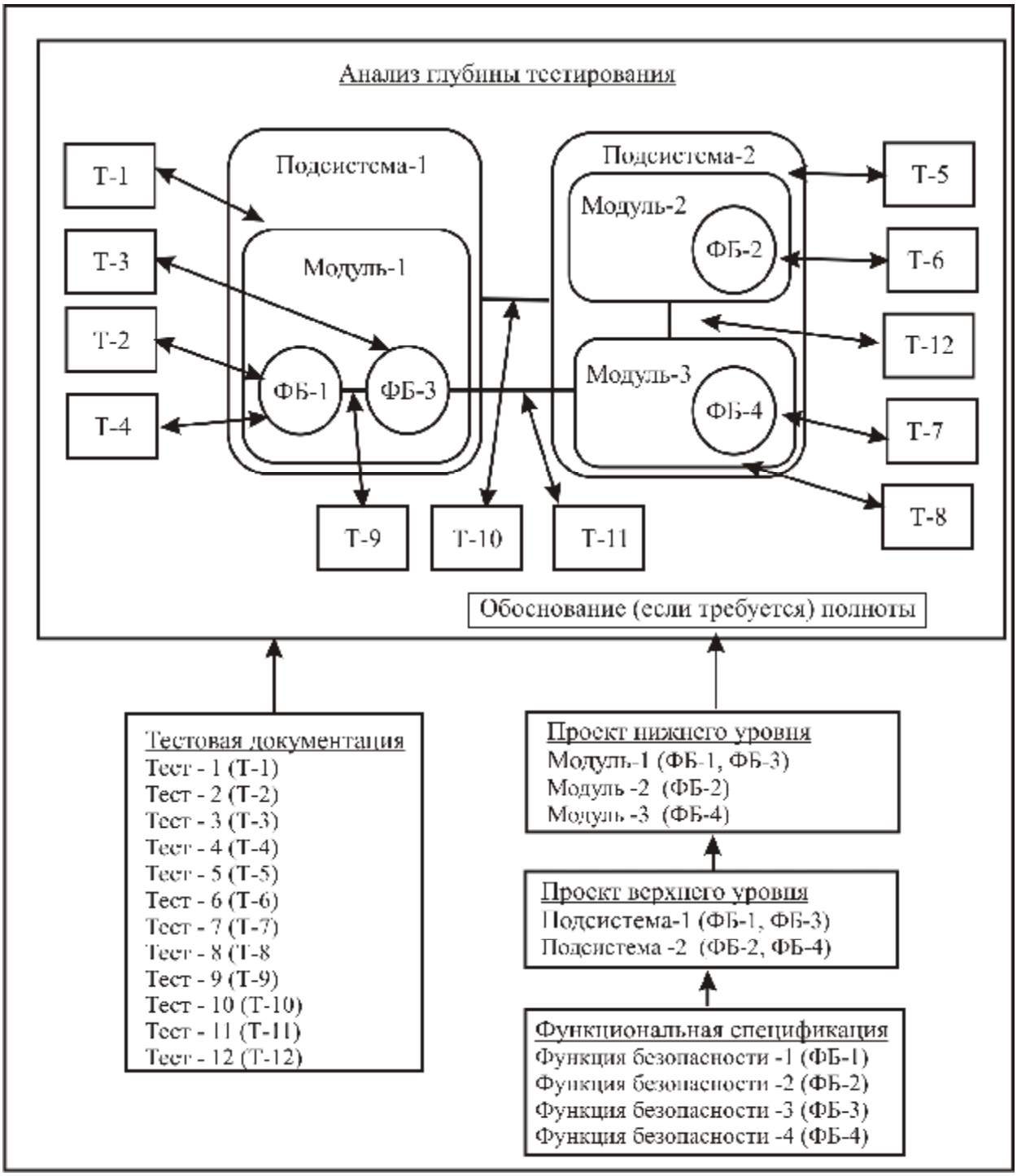


Рисунок 10.4 - Концептуальная структура анализа глубины тестирования

ATE_DPT.2-2 Оценщик ***должен исследовать*** план тестирования разработчика, чтобы сделать заключение, является ли подход к тестированию каждой функции

безопасности ФБО пригодным для демонстрации ожидаемого режима ее выполнения.

Руководство по выполнению этого шага оценивания можно найти в следующих Замечаниях по применению:

а) Понимание ожидаемого режима функционирования ОО (см. 10.2.1.1);

б) Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности (см. 10.2.1.2).

Тестирование ФБО может быть выполнено 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 функции безопасности необходимым, или эти внутренние интерфейсы могут быть надлежащим образом протестированы (хотя и неявным образом) с использованием внешних интерфейсов. Это решение, как и его строгое обоснование, остается за оценщиком.

ATE_DPT.2-3 Оценщик ***должен исследовать*** процедуры тестирования, чтобы сделать заключение, адекватно ли описание предварительных условий тестирования, шагов тестирования и ожидаемого результата (ожидаемых результатов) для тестирования каждой функции безопасности.

Руководство по выполнению этого шага оценивания, который относится к проекту верхнего уровня и проекту нижнего уровня, можно найти в Замечаниях по применению «Верификация адекватности тестов» (см. 10.2.1.3).

ATE_DPT.2-4 Оценщик ***должен проверить*** материалы анализа глубины тестирования, чтобы удостовериться, что ФБО в том виде, в котором они определены в проекте верхнего уровня, полностью сопоставлены с тестами, представленными в тестовой документации.

Материалы анализа глубины тестирования обеспечивают полное изложение соответствия между проектом верхнего уровня, планом и процедурами тестирования. Все подсистемы и внутренние интерфейсы, описанные в проекте верхнего уровня, должны быть представлены в материалах анализа глубины тестирования. Для всех подсистем и внутренних интерфейсов, представленных в материалах анализа глубины тестирования, должны иметься сопоставленные с ними тесты для того, чтобы можно было утверждать о полноте. Как показано на рисунке 10.4 для всех подсистем и внутренних интерфейсов имеются относящиеся к ним тесты, а, следовательно, в данном примере продемонстрирована полнота глубины тестирования. Неполнота тестирования была бы очевидна, если бы некоторая подсистема или внутренний интерфейс были идентифицированы в материалах анализа глубины тестирования, но никакие тесты не могли быть к ним отнесены.

ATE_DPT.2-5 Оценщик ***должен проверить*** материалы анализа глубины тестирования, чтобы удостовериться, что ФБО в том виде, в котором они определены в проекте нижнего уровня, полностью сопоставлены с тестами, представленными в тестовой документации.

Материалы анализа глубины тестирования обеспечивают полное изложение соответствия между проектом нижнего уровня, планом и процедурами тестирования. Все модули и внутренние интерфейсы, описанные в проекте нижнего уровня, должны присутствовать в материалах анализа глубины тестирования. Для всех модулей и внутренних интерфейсов, представленных в материалах анализа глубины тестирования, должны иметься сопоставленные с ними тесты для того, чтобы можно было утверждать о полноте. Как показано на рисунке 10.4, для всех модулей и внутренних интерфейсов имеются относящиеся к ним тесты, а, следовательно, в данном примере продемонстрирована полнота глубины тестирования. Неполнота тестирования была бы

очевидна, если бы некоторый модуль или внутренний интерфейс был идентифицирован в материалах анализа глубины тестирования, но никакие тесты не могли быть к нему отнесены.

10.5 Оценка функциональных тестов

10.5.1 Подвид деятельности ATE_FUN.1

10.5.1.1 Цели

Цель данного подвида деятельности - сделать заключение, является ли документация функциональных тестов разработчика достаточной для демонстрации того, что функции безопасности выполняются в соответствии со спецификациями

10.5.1.2 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 повторными, и определяет степень возможности использования тестов разработчика при проведении оценщиком независимого тестирования. Любую функцию безопасности, для которой результаты тестирования разработчиком указывают, что она может не выполняться в соответствии со спецификациями, оценщику следует подвергнуть независимому тестированию, чтобы сделать заключение, выполняется ли она в соответствии со спецификациями или нет.

10.5.1.3 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) функциональная спецификация,

в) тестовая документация,

г) процедуры тестирования.

10.5.1.4 Действия оценщика

Этот подвид деятельности включает одни элемент действий оценщика из части 3 ОК:

а) ATE_FUN.1.1E.

10 5.1.4.1 Действие ATE_FUN.1.1E

ATE_FUN.1.1C

ATE_FUN.1-1 Оценщик ***должен проверить***, что тестовая документация включает планы тестирования, описание процедур тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.

ATE_FUN.1.2C

ATE_FUN.1-2 Оценщик ***должен проверить***, что в плане тестирования идентифицированы подлежащие тестированию функции безопасности.

Одним из методов, который может быть использован для идентификации проверяемой функции безопасности, является ссылка на соответствующую часть (части) функциональной спецификации, в которой определена конкретная функция безопасности.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке приведено в подразделе 12.2.

ATE_FUN.1-3 Оценщик ***должен исследовать*** план тестирования, чтобы сделать заключение, содержит ли он описание целей выполняемых тестов.

План тестирования предоставляет информацию о том, каким образом тестируются функции безопасности, а также информацию о тестируемой конфигурации ОО,

используемой при проведении тестирования.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке приведено в подразделе 12.2.

ATE_FUN.1-4 Оценщик ***должен исследовать*** план тестирования, чтобы сделать заключение, согласована ли тестируемая конфигурация ОО с той конфигурацией, которая идентифицирована для оценки в ЗБ

ОО, упомянутый в плане тестирования разработчика, должен иметь ту же самую уникальную маркировку, которая установлена системой УК.

В ЗБ может быть определено несколько подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию на соответствие ЗБ. Оценщик верифицирует, что в тестовой документации разработчика определены тестируемые конфигурации, и они согласованы соответственно с каждой из оцениваемых конфигураций, описанных в ЗБ.

Оценщику следует рассмотреть описанные в ЗБ предположения относительно аспектов безопасности среды ОО, которые могут касаться среды тестирования. В ЗБ могут быть и другие предположения, которые не касаются среды тестирования. Например, предположение относительно допусков пользователей может не касаться среды тестирования, однако, предположение относительно единой точки подключения к сети, как правило, касается среды тестирования.

ATE_FUN.1-5 Оценщик ***должен исследовать*** план тестирования, чтобы сделать заключение, согласован ли он с описанием процедур тестирования.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке приведено в подразделе 12.2.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

ATE_FUN.1.3C

ATE_FUN.1-6 Оценщик ***должен проверить***, что в описании процедур тестирования идентифицирован каждый из подлежащих тестированию режимов выполнения функций безопасности.

Одним из методов, который может использоваться для идентификации подлежащего тестированию режима выполнения функции безопасности, является ссылка на соответствующую часть (части) спецификации проекта, которая определяет конкретный подлежащий тестированию режим выполнения функции безопасности

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке приведено в подразделе 12.2.

ATE_FUN.1-7 Оценщик ***должен исследовать*** описание процедур тестирования, чтобы сделать заключение представлены ли достаточные инструкции для того, чтобы установить воспроизводимые начальные условия выполнения тестов, включая зависимости, связанные с порядком следования, при их наличии.

Для того чтобы установить начальные условия выполнения тестов, возможно, потребуется выполнить некоторые шаги. Например, необходимо добавить учетные записи пользователей прежде, чем их можно будет удалить Пример зависимостей, связанных с порядком следования тестов, от результатов других тестов - необходимость тестирования функции аудита прежде, чем полагаться на нее при создании записей аудита для другого механизма безопасности, такого как управления доступом. Другой пример зависимости, связанной с порядком следования тестов, - при выполнении одного теста генерируется файл данных, используемых в качестве исходных данных для набора других тестов

Для выполнения данного шага оценивания оценщик может избрать стратегию

выборки.

Руководство по выборке приведено в подразделе 12.2.

ATE_FUN 1-8 Оценщик ***должен исследовать*** описание процедур тестирования, чтобы сделать заключение, представлены ли достаточные инструкции для того, чтобы иметь воспроизводимый способ инициирования выполнения функции безопасности и наблюдения за режимом их выполнения.

Инициирующее воздействие обычно обеспечивается внешним по отношению к функции безопасности способом через ИФБО. После того, как входные данные (инициирующее воздействие) предоставлены ИФБО, через ИФБО можно наблюдать режим выполнения функции безопасности. Воспроизводимость не обеспечивается, если процедуры тестирования не содержат достаточных подробностей для однозначного описания инициирующего воздействия и режима выполнения, ожидаемого в результате инициирующего воздействия.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке приведено в подразделе 12.2.

ATE_FUN 1-9 Оценщик ***должен исследовать*** описание процедур тестирования, чтобы сделать заключение об их согласованности с процедурами тестирования.

Если описание процедур тестирования - это собственно процедуры тестирования, то рассматриваемый шаг оценивания не применяется.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке смотри в подразделе 12.2.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

ATE_FUN.1.4C

ATE_FUN 1-10 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 достаточно, если оно однозначно и согласуется с ожидаемым режимом выполнения ФБО, обусловленным подходом к тестированию.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке приведено в подразделе 12.2.

ATE_FUN.1.5C

ATE_FUN.1-11 Оценщик ***должен проверить,*** что ожидаемые результаты тестирования в тестовой документации согласуются с представленными фактическими результатами тестирования.

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 сначала будет выполнено некоторое преобразование или синтез данных. В подобных случаях в тестовой документации разработчика должен быть описан процесс преобразования или синтеза фактических данных.

Например, разработчику может потребоваться проверить содержимое буфера сообщений после того, как имело место сетевое соединение, чтобы определить содержимое буфера. 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 высокого уровня должно быть достаточно подробно описано разработчиком, чтобы позволить оценщику выполнить процесс преобразования (то есть, необходимо описать, используется синхронный или асинхронный метод передачи данных, 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.

Руководство по выборке приведено в подразделе 12.2.

Если ожидаемые и фактические результаты тестирования для любого теста не совпадают, то правильность выполнения функции безопасности не продемонстрирована. Такая ситуация окажет влияние на усилия оценщика по независимому тестированию, выражающееся в необходимости тестирования соответствующей функции безопасности. Оценщику также следует рассмотреть вопрос об увеличении выборки свидетельств, на основе которых выполняется рассматриваемый шаг оценивания.

ATE_FUN 1-12 Оценщик ***должен привести*** в отчете информацию об усилиях разработчика по тестированию, выделив подход к тестированию, конфигурацию, глубину тестирования, покрытие тестами и результаты тестирования.

Информация о тестировании разработчиком, зафиксированная в ТОО, позволяет оценщику передать общий подход к тестированию и усилия, затраченные разработчиком на тестирование ОО. Смысл предоставления этой информации состоит в том, чтобы дать содержательный краткий обзор усилий разработчика по тестированию. Не имеет смысла, 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 органа по подтверждению соответствия 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, которую обычно можно найти в соответствующем разделе ТОО, включает:

а) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые тестировались;

б) подход к тестированию. Описание общей стратегии тестирования, которую применил разработчик;

в) объем тестирования, выполненного разработчиком. Описание степени покрытия тестами и глубины тестирования разработчиком;

г) результаты тестирования. Описание общих результатов тестирования разработчиком.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, связанной с усилиями разработчика по тестированию, которую следует представить в ТОО.

10.6 Оценка путем независимого тестирования

10.6.1 Подвид деятельности ATE_IND.1

10.6.1.1 Цели

Цель данного подвида деятельности состоит в том, чтобы путем независимого

тестирования подмножества ФБО сделать заключение, выполняются ли ФБО в соответствии со спецификациями.

10.6.1.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

а) ЗБ,

б) функциональная спецификация;

в) руководство пользователя;

г) руководство администратора;

д) процедуры безопасной установки, генерации и запуска;

е) ОО, пригодный для тестирования.

10.6.1.3 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из части 3 ОК:

а)ATE_IND.1.1E;

б)ATE_IND.1.2E.

10.6.1.3.1 Действие ATE_IND.1.1E

ATE_IND.1.1C

ATE_IND.1-1 Оценщик ***должен исследовать*** ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, используемый оценщиком для тестирования, должен иметь ту же самую уникальную маркировку, которая установлена системой УК.

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 предположения относительно аспектов безопасности среды ОО, которые могут относиться к среде тестирования. В ЗБ могут быть и другие предположения, которые не относятся к среде тестирования. Например, предположение относительно допусков пользователей может не относиться к среде тестирования, однако, предположение относительно единой точки подключения к сети, как правило, относится к среде тестирования.

При использовании каких бы то ни было средств тестирования (например, измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика

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 AD0_IGS.1 позволит считать выполненным данный шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был должным образом 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 шаг оценивания ADO_IGS.1-2.

10.6.1.3.2 Действие ATE_IND.1.2E

ATE_IND.1-3 Оценщик ***должен продумать*** тестируемое подмножество ФБО.

Оценщик выбирает тестируемое подмножество и стратегию тестирования, которая является приемлемой для ОО. Одна, крайняя, стратегия тестирования предусматривает наличие тестируемого подмножества ФБО, содержащего как можно большее количество функций безопасности, тестируемых с небольшой строгостью. Другая стратегия тестирования предусматривает наличие тестируемого подмножества, содержащего небольшое количество функций безопасности, исходя из их осознанной значимости, и строгое тестирование этих функций.

Как правило, подход к тестированию, принятый оценщиком, должен находиться где-то между этими двумя крайностями. Оценщику следует проверить выполнение большинства определенных в ЗБ функциональных требований безопасности, используя, по крайней мере, один тест для каждого требования, но при этом нет необходимости, чтобы тестирование продемонстрировало исчерпывающую проверку спецификаций.

При выборе подмножества тестируемых ФБО оценщику следует рассмотреть следующие факторы:

а) число функций безопасности, из которых необходимо сформировать тестируемое подмножество. В тех случаях, когда у ОО только небольшое число функций безопасности, может быть практичным строгое тестирование всех функций безопасности. Для ОО с большим числом функций безопасности это будет нерентабельно и потребуется осуществление выборки;

б) поддержание некоторого баланса между видами деятельности по оценке. Тестирование, как правило, занимает 20-30 % усилий оценщика в течение оценки.

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:

а) известные из общедоступных источников слабые места безопасности, обычно ассоциируемые с конкретным типом ОО (например, с операционной системой, межсетевым экраном). Известные из общедоступных источников слабые места, ассоциируемые с конкретным типом ОО, будут влиять на процесс выбора тестируемого подмножества. Оценщику следует включить в тестируемое подмножество те функции безопасности, которые связаны с известными из общедоступных источников слабыми местами для данного типа ОО (известные из общедоступных источников слабые места в данном случае относятся не к уязвимостям как таковым, а к несоответствиям или проблемным вопросам, которые были обнаружены для данного конкретного типа ОО). Если такие слабые места не известны, то может быть более приемлемым более общий подход, связанный с выбором широкого диапазона функции безопасности;

б) значимость функции безопасности. Те функции безопасности, которые более значимы, чем другие, с точки зрения целей безопасности для ОО, следует включить в тестируемое подмножество;

в) сложность функции безопасности. Для сложных функции безопасности может потребоваться выполнение сложных тестов налагающих обременительные требования на разработчика или оценщика, которые, в свою очередь, не будут способствовать рентабельным оценкам. С другой стороны, сложные функции безопасности - это вероятная область поиска ошибок и подходящие кандидаты для включения в подмножество. Оценщику необходимо достигнуть баланса между этими соображениями;

г) 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 функции безопасности. Некоторые интерфейсы обычно могут использоваться для обеспечения нескольких функциональных возможностей

безопасности, и их следует сделать объектом эффективного подхода к тестированию;

д) 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;

е) инновационные или необычные функции. В тех случаях, когда в ОО включены инновационные или необычные функции безопасности, которые могут широко быть представлены в маркетинговой литературе, они должны быть прямыми кандидатами на тестирование.

В данном руководстве сформулированы факторы, которые необходимо рассмотреть в процессе выбора приемлемого тестируемого подмножества ФБО, но они ни в коем случае не являются исчерпывающими

Руководство по выборке приведено в подразделе 12.2.

ATE_IND.1.4 Оценщик ***должен разработать*** тестовую документацию для тестируемого подмножества ФБО, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов.

Уяснив из ЗБ и функциональной спецификации ожидаемый режим выполнения функции безопасности, оценщик должен определить наиболее подходящий способ тестирования данной функции. Оценщик, в особенности, рассматривает:

а) подход, который будет использоваться, например, будет ли функция безопасности тестироваться через внешний интерфейс, внутренний интерфейс с использованием каких-либо средств автономного тестирования или будет использован альтернативный тестированию подход (например, в исключительных обстоятельствах - экспертиза кода);

б) интерфейс(ы) функции безопасности, который(е) будет(ут) использоваться для инициирования выполнения функции безопасности и наблюдения ее реакции;

в) начальные условия, которые будут необходимы для выполнения теста (т.е., какие бы то ни было конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

г) 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 практичным тестировать каждую функцию безопасности, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования очень специфичного аспекта ожидаемого режима выполнения функции безопасности.

В тестовой документации оценщика следует определить происхождение каждого теста, прослеживая его к соответствующей спецификации проекта и, если необходимо, к ЗБ.

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 течение тестирования. Эти новые тесты записываются в тестовую документацию

ATE_IND.1-6 Оценщик ***должен зафиксировать*** следующую информацию о тестах, которые составляют подмножество тестов:

а) идентификационную информацию тестируемого режима выполнения функции безопасности;

б) инструкции по подключению и установке всего требуемого оборудования для тестирования, как это требуется для проведения конкретного теста;

в) инструкции по установке всех предварительных условий выполнения теста;

г) инструкции по инициированию функции безопасности;

д) инструкции по наблюдению режима поведения функции безопасности;

е) описание всех ожидаемых результатов и необходимого анализа, который выполняется по отношению к наблюдаемому режиму выполнения для сравнения с ожидаемыми результатами;

ж) инструкции по завершению тестирования и установке необходимого пост-тестового состояния ОО;

з) 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 строгое обоснование, остается за оценщиком.

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 строгое обоснование, остается за оценщиком.

ATE_IND.1-8 Оценщик ***должен привести*** в ТОО информацию об усилиях по тестированию, вкратце изложив подход к тестированию, тестируемую конфигурацию, глубину и результаты тестирования.

Информация оценщика о тестировании, приводимая в ТОО, позволяет оценщику передать общин подход к тестированию и усилия, затраченные в течение оценки на вид деятельности по тестированию. Смысл предоставления этой информации состоит в том, чтобы дать содержательный краткий обзор усилии 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 органа по подтверждению соответствия 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, которую обычно можно найти в соответствующем разделе ТОО, включает:

а) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые тестировались;

б) выбранный размер подмножества Количество протестированных в течение оценки функции безопасности и строгое обоснование этого размера;

в) критерии выбора для функции безопасности, которые составляют тестируемое подмножество. Краткое изложение факторов, рассмотренных при отборе функций безопасности для включения в подмножество;

г) протестированные функции безопасности Краткий перечень функций безопасности, обоснованно включенных в подмножество;

д) заключение 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 дать некоторое представление о типе информации, касающейся тестирования, выполненного оценщиком в течение оценки, которую следует представить в ТОО.

10.6.2 Подвид деятельности ATE_IND.2

10.6.2.1 Цели

Цель данного подвида деятельности состоит в том, чтобы путем независимого тестирования подмножества ФБО сделать заключение, соответствует ли спецификациям режим функционирования ОО, и повысить уверенность в результатах тестирования разработчиком путем выполнения выборки тестов разработчика.

10.6.2.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

а) ЗБ;

б) функциональная спецификация;

в) руководство пользователя;

г) руководство администратора;

д) процедуры безопасной установки, генерации и запуска;

е) тестовая документация;

ж) материалы анализа покрытия тестами;

з) материалы анализа глубины тестирования;

и) ОО, пригодный для тестирования.

10.6.2.3 Действия оценщика

Этот подвид деятельности включает три элемента действии оценщика из части 3 ОК:

а)ATE_IND.2.1E;

б)ATE_IND.2.2E;

в) ATE_IND 2.3E.

10.6.2.3.1 Действие ATE_IND.2.1E

ATE_IND.2 1C

ATE_IND.2-1 Оценщик ***должен исследовать*** ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, используемый оценщиком для тестирования, должен иметь ту же самую уникальную маркировку, которая установлена системой УК.

В ЗБ может быть определено более одной подлежащих оценке конфигурации 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 предположения относительно аспектов безопасности среды ОО, которые могут касаться среды тестирования. В ЗБ могут быть и другие предположения, которые не относятся к среде тестирования. Например, предположение относительно допусков пользователей может не относиться к среде тестирования, однако, предположение относительно единой точки подключения к сети, как правило, относится к среде тестирования.

При использовании каких бы то ни было средств тестирования (например, измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика.

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 ADO_IGS.1 удовлетворит этот шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был должным образом 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 шаг оценивания ADO_IGS. 1-2.

ATE_IND.2.2C

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 может, кроме всего прочего, включать доступное лабораториям и специальное испытательное оборудование. Ресурсы, которые не являются идентичными ресурсам, использовавшимся разработчиком, должны быть эквивалентны нм с точки зрения любого влияния, которое они могут оказать на результаты тестирования.

10.6.2.3.2 Действие ATE_IND.2.2E

ATE_IND.2-4 Оценщик ***должен продумать*** тестируемое подмножество ФБО.

Оценщик выбирает тестируемое подмножество и стратегию тестирования, которая является приемлемой для ОО. Одна, крайняя, стратегия тестирования предусматривает наличие тестируемого подмножества ФБО, содержащего как можно большее количество функций безопасности, тестируемых с небольшой строгостью. Другая стратегия тестирования предусматривает наличие тестируемого подмножества, содержащего небольшое количество функций безопасности, исходя из их осознанной значимости, и строгое тестирование этих функций.

Как правило, подход к тестированию, принятый оценщиком, должен находиться где-то между этими двумя крайностями. Оценщику следует проверить выполнение большинства определенных в ЗБ функциональных требований безопасности, используя, по крайней мере, один тест для каждого требования, но при этом нет необходимости, чтобы тестирование продемонстрировало исчерпывающую проверку спецификаций. При выборе подмножества тестируемых ФБО оценщику следует рассмотреть следующие факторы:

а) свидетельства тестирования разработчиком. Свидетельства тестирования разработчиком включают: анализ покрытия тестами, анализ глубины тестирования и тестовую документацию. Свидетельства тестирования разработчиком должны обеспечить понимание того, каким образом разработчиком в ходе тестирования опробовались функции безопасности. Оценщик будет использовать данную информацию при разработке новых тестов для независимого тестирования ОО. Оценщику следует, в особенности, рассмотреть:

1) усиление тестирования, выполненного разработчиком, для определенной функции (функции) безопасности. Оценщик может захотеть выполнить большее количество тестов того же самого типа, чтобы путем изменения параметров более строго протестировать функцию безопасности;

2) дополнение стратегии тестирования, применявшейся разработчиком, для определенной функции (функции) безопасности. Оценщик может захотеть изменить подход к тестированию определенной функции безопасности, тестируя ее с использованием другой стратегии тестирования;

б) число функций безопасности, из которых необходимо сформировать тестируемое подмножество. В тех случаях, когда у ОО только небольшое число функций безопасности, может быть практичным строгое тестирование всех функции безопасности. Для ОО с большим числом функций безопасности это будет нерентабельно и потребуется осуществление выборки;

в) поддержание некоторого баланса между видами деятельности по оценке. Усилия оценщика, затраченные на вид деятельности по тестированию, должны быть соразмерны с усилиями, затраченными на любой другой вид деятельности 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:

а) строгость тестирования разработчиком функций безопасности. Все функции безопасности идентифицированные в функциональной спецификации, должны иметь относящиеся к ним свидетельства тестирования разработчиком, как это требуется в ATE_COV.2. Те функции безопасности, которые оценщик определил как требующие дополнительного тестирования, следует включить в тестируемое подмножество ФБО;

б) результаты тестирования разработчиком. Если результаты тестов разработчика заставляют оценщика сомневаться в том, что функция безопасности или ее аспект, выполняются в соответствии со спецификациями, то оценщику следует включить подобные функции безопасности в тестируемое подмножество;

в) известные из общедоступных источников слабые места безопасности, обычно ассоциируемые с конкретным типом ОО (например, с операционной системой, межсетевым экраном). Известные из общедоступных источников слабые места, ассоциируемые с конкретным типом ОО. будут влиять на процесс выбора тестируемого подмножества. Оценщику следует включить в тестируемое подмножество те функции безопасности, которые связаны с известными из общедоступных источников слабыми местами для данного типа ОО (известные из общедоступных источников слабые места в данном случае относятся не к уязвимостям как таковым, а к несоответствиям или проблемным вопросам, которые были обнаружены для данного конкретного типа ОО). Если такие слабые места не известны, то может быть более приемлемым более общий подход, связанный с выбором широкого диапазона функций безопасности;

г) значимость функций безопасности. Те функции безопасности, которые более значимы, чем другие, с точки зрения целей безопасности для ОО, следует включить в тестируемое подмножество;

д) утверждение о СФБ, сделанное в ЗБ. Все функции безопасности, для которых было сделано конкретное утверждение о СФБ, следует включить в тестируемое подмножество ФБО;

е) сложность функции безопасности. Для сложных функции безопасности может потребоваться выполнение сложных тестов, налагающих обременительные требования на разработчика или оценщика, которые, в свою очередь, не будут способствовать рентабельным оценкам. С другой стороны, сложные функции безопасности - это вероятная область поиска ошибок и подходящие кандидаты для включения в подмножество. Оценщику необходимо достигнуть баланса между этими соображениями;

ж) 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;

з) 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;

и) инновационные или необычные функции. В тех случаях, когда в ОО включены инновационные или необычные функции безопасности, которые могут широко быть представлены в маркетинговой литературе, они должны быть прямыми кандидатами на тестирование.

В данном руководстве сформулированы факторы, которые необходимо рассмотреть в процессе выбора приемлемого тестируемого подмножества ФБО, но они ни в коем случае не являются исчерпывающими.

Руководство по выборке приведено в подразделе 12.2.

ATE_IND.2-5 Оценщик ***должен разработать*** тестовую документацию для тестируемого подмножества ФБО, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов. Уяснив из ЗБ и функциональной спецификации ожидаемый режим выполнения функции безопасности, оценщик должен определить наиболее подходящий способ тестирования данной функции. Оценщик, в особенности, рассматривает:

а) подход, который будет использоваться, например, будет ли функция безопасности тестироваться через внешний интерфейс, внутренний интерфейс с использованием каких-либо средств автономного тестирования или будет использован альтернативный тестированию подход (например, в исключительных обстоятельствах - экспертиза кода);

б) интерфейс(ы) функции безопасности, который(е) будет(ут) использоваться для инициирования выполнения функции безопасности и наблюдения ее реакции;

в) начальные условия, которые будут необходимы для выполнения теста (т.е., какие бы то ни было конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

г) 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 практичным тестировать каждую функцию безопасности, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования очень специфичного аспекта ожидаемого режима выполнения функции безопасности.

В тестовой документации оценщика следует определить происхождение каждого теста, прослеживая его к соответствующей спецификации проекта и, если необходимо, к ЗБ.

ATE_IND.2-6 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 течение тестирования. Эти новые тесты записываются в тестовую документацию.

ATE_IND.2-7 Оценщик ***должен зафиксировать*** следующую информацию о тестах, которые составляют подмножество тестов:

а) идентификационную информацию тестируемого режима выполнения функции

безопасности;

б) инструкции по подключению и установке всего требуемого оборудования для тестирования, как это требуется для проведения конкретного теста;

в) инструкции по установке всех предварительных условии выполнения теста;

г) инструкции по инициированию функции безопасности;

д) инструкции по наблюдению режима поведения функции безопасности;

е) описание всех ожидаемых результатов и необходимого анализа, который выполняется по отношению к наблюдаемому режиму выполнения для сравнения с ожидаемыми результатами;

ж) инструкции по завершению тестирования и установке необходимого пост-тестового состояния ОО;

з) 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 строгое обоснование, остается за оценщиком.

ATE_IND.2-8 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 строгое обоснование, остается за оценщиком.

10.6.2.3.3 Действие ATE_IND.2.3E

ATE_IND.2-9 Оценщик ***должен провести*** тестирование, используя выборку тестов, находящихся в плане и процедурах тестирования разработчика.

Общая цель данного шага оценивания состоит в выполнении тестов разработчика в количестве, достаточном для подтверждения правильности результатов тестирования разработчиком. Оценщик должен определиться с размером выборки и тестами разработчика, которые составят данную выборку.

Принимая во внимание общие усилия оценщика в целом по виду деятельности, связанному с тестированием, обычно следует выполнить около 20% тестов разработчика, хотя этот процент может варьироваться в соответствии с характером ОО и представленных свидетельств тестирования.

Все тесты разработчика могут быть сопоставлены с конкретными функциями безопасности. Следовательно, факторы, которые необходимо рассмотреть при выборе тестов для включения в выборку, подобны тем, которые перечислены на шаге оценивания ATE_IND.2-4 для выбора тестируемого подмножества ФБО. Дополнительно, для выбора тестов разработчика, включаемых в выборку, оценщик может избрать метод случайной выборки.

Руководство по выборке приведено в подразделе 12.2.

ATE_IND.2-10 Оценщик ***должен проверить***, что все фактические результаты

тестирования согласуются с ожидаемыми результатами тестирования.

Противоречия между ожидаемыми результатами тестирования разработчиком и фактическими результатами тестирования заставляют оценщика разрешать эти несоответствия. Противоречия, с которыми столкнулся оценщик, могут быть разрешены разработчиком путем убедительного объяснения и разрешения противоречий.

Если удовлетворительное объяснение или разрешение противоречий не может быть достигнуто, то уверенность оценщика в результатах тестирования разработчиком может уменьшиться, у оценщика даже может возникнуть необходимость в увеличении объема выборки, чтобы восстановить уверенность в результатах тестирования разработчиком. Если увеличение объема выборки не оправдает ожиданий оценщика, может потребоваться повторение всей совокупности тестов разработчика. В конечном счете, для адекватного тестирования подмножества ФБО, идентифицированного на шаге оценивания ATE_IND_2-4, недостаточность тестов разработчика приведет к необходимости корректировки тестов разработчика или разработки оценщиком новых тестов.

ATE_IND.2-11 Оценщик ***должен привести*** в ТОО информацию об усилиях по тестированию, вкратце 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 дать содержательный краткий обзор усилии 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 органа по подтверждению соответствия 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, которую обычно можно найти в соответствующем разделе ТОО, включает:

а) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые тестировались;

б) выбранный размер подмножества. Количество протестированных в течение оценки функций безопасности и строгое обоснование этого размера;

в) критерии выбора для функций безопасности, которые составляют тестируемое подмножество. Краткое изложение факторов, рассмотренных при отборе функций безопасности для включения в подмножество;

г) протестированные функции безопасности. Краткий перечень функций безопасности, обоснованно включенных в подмножество;

д) выполненные тесты разработчика. Количество выполненных тестов разработчика и краткое описание критериев, использовавшихся для выбора данных тестов;

е) заключение 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 дать некоторое представление о типе информации, касающейся тестирования, выполненного оценщиком в течение оценки, которую следует представить в ТОО.

10.6.3 Подвид деятельности ATE_IND.3

10.6.3.1 Цели

Цель данного подвида деятельности состоит в том, чтобы путем независимого тестирования подмножества ФБО сделать заключение, соответствует ли спецификациям режим функционирования ОО, и повысить уверенность в результатах тестирования разработчиком путем выполнения тестов разработчика

10.6.3.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

а) ЗБ;

б) функциональная спецификация;

в) руководство пользователя;

г) руководство администратора;

д) процедуры безопасной установки, генерации и запуска;

е) тестовая документация;

ж) материалы анализа покрытия тестами;

з) материалы анализа глубины тестирования;

и) ОО, пригодный для тестирования.

10.6.3.3 Действия оценщика

Этот подвид деятельности включает три элемента действии оценщика из части 3 ОК:

а) ATE_IND.3.1E;

б) ATE_IND.3.2E;

в) ATE_IND.3.3E;

10.6.3.3.1 Действие ATE_IND.3.1E

ATE_IND.3.1C Оценщик ***должен исследовать*** ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, используемый оценщиком для тестирования, должен иметь ту же самую уникальную маркировку, которая установлена системой УК.

В ЗБ может быть определено более одной подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализации, 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 предположения относительно аспектов безопасности среды ОО, которые могут касаться среды тестирования. В ЗБ могут быть и другие предположения, которые не касаются среды тестирования. Например, предположение относительно допусков пользователей может не откоситься к среде тестирования, однако, предположение относительно единой точки подключения к сети, как правило, относится к среде тестирования.

При использовании, каких бы то ни было средств тестирования (например, измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика.

ATE_IND.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 ADO_IGS.1 удовлетворит этот шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был должным образом 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 шаг оценивания ADO_IGS.1-2.

ATE_IND.3.2C

ATE_IND.3-3 Оценщик ***должен исследовать*** набор ресурсов, предоставленных разработчиком, чтобы сделать заключение, эквивалентны ли они набору ресурсов, использовавшимся разработчиком для функционального тестирования ФБО.

Рассматриваемый набор ресурсов может, кроме всего прочего, включать доступное лабораториям и специальное испытательное оборудование. Ресурсы, которые не являются идентичными ресурсам, использовавшимся разработчиком, должны быть эквивалентны им с точки зрения любого влияния, которые они могут оказать на результаты тестирования.

10.6.3.3.2 Действие ATE_IND.3.2E

ATE_IND.3-4 Оценщик ***должен продумать*** тестируемое подмножество ФБО.

Оценщик выбирает тестируемое подмножество и стратегию тестирования, которая является приемлемой для ОО. Одна, крайняя стратегия тестирование предусматривает наличие тестируемого подмножества ФБО содержащего как можно большее количество функций безопасности тестируемых с небольшой строгостью. Другая стратегия тестирования предусматривает наличие тестируемого подмножества содержащего небольшое количество функций безопасности, исходя из их осознанной значимости и строгое тестирование этих функций.

Как правило, подход к тестированию, принятый оценщиком должен находиться где-то между этими двумя крайностями. Оценщику следует проверить выполнение большинства определенных в ЗБ функциональных требований безопасности, используя, по крайней мере, один тест для каждого требования но при этом нет необходимости, чтобы тестирование продемонстрировало исчерпывающую проверку спецификаций.

При выборе подмножества тестируемых ФБО оценщику следует рассмотреть следующие факторы:

а) свидетельство тестирования разработчиком. Свидетельства тестирования разработчиком включают анализ покрытия тестами анализ глубины тестирования и тестовую документацию. Свидетельства тестирования разработчиком должны обеспечить понимание того, каким образом разработчиком в ходе тестирования опробовались функции безопасности. Оценщик будет использовать данную информацию при разработке новых тестов для независимого тестирования ОО. Оценщику следует в особенности, рассмотреть:

1) усиление тестирования выполненного разработчиком, для определенной функции (функций) безопасности. Оценщик может захотеть выполнить большее количество тестов того же самого типа, чтобы путем изменения параметров более строго протестировать функцию безопасности;

2) дополнение стратегии тестирования применяющейся разработчиком, для определенной функции (функций) безопасности. Оценщик может захотеть изменить подход к тестированию определенной функции безопасности, тестируя ее с использованием другой стратегии тестирования;

б) число функций безопасности, из которых необходимо сформировать тестируемое подмножество. В тех случаях, когда в ОО только небольшое число функций безопасности может быть практичным строгое тестирование всех функций безопасности. Для ОО с большим числом функций безопасности это будет нерентабельно и потребуется осуществление выборки;

в) поддержание некоторого баланса между видами деятельности по оценке. Усилия

оценщика, затраченные на вид деятельности по тестированию, должны быть соразмерны с усилиями, затраченными на любой другой вид деятельность 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:

а) строгость тестирования разработчиком функций безопасности. Все функции безопасности, идентифицированные в функциональной спецификации, должны иметь относящиеся к ним свидетельства тестирования разработчиком к ним, как это требуется в ATE_COV.2. Те функции безопасности, которые оценщик определил как требующие дополнительного тестирования, следует включить в тестируемое подмножество ФБО;

б) результаты тестирования разработчиком. Если результаты тестов разработчика заставляют оценщика сомневаться в том, что функция безопасности или ее аспект, выполняется в соответствии со спецификациями, то оценщику следует включить подобные функции безопасности в тестируемое подмножество;

в) известные из общедоступных источников слабые места безопасности, обычно ассоциируемые с конкретным типом ОО (например, с операционной системой межсетевым экраном). Известные из общедоступных источников слабые места, ассоциируемые *с* конкретным типом ОО, будут влиять на процесс выбора тестируемого подмножества. Оценщику следует включить в тестируемое подмножество те функции безопасности, которые связаны с известными из общедоступных источников слабыми местами для данного типа ОО (известные из общедоступных источников слабые места в данном случае относятся не к уязвимостям как таковым, а к несоответствиям или проблемным вопросам, которые были обнаружены для данного конкретного типа ОО). Если такие слабые места не известны, то может быть, более приемлемым общий подход, связанный с выборов широкого диапазона функций безопасности;

г) значимость функций безопасности. Те функции безопасности, которые более значимы, чем другие с точки зрения целей безопасности для ОО, следует включить в тестируемое подмножество;

д) утверждение о СФБ, сделанное в ЗБ. Все функции безопасности, для которых было сделано конкретное утверждение о СФБ, следует включить в тестируемое подмножество ФБО;

е) сложность функции безопасности. Для сложных функций безопасности может потребоваться выполнение сложных тестов налагающих обременительные требования на разработчика или оценщика, которые, в свою очередь не будут способствовать рентабельным оценкам. С другой стороны сложные функции безопасности - это вероятная область поиска ошибок и подходящие кандидаты для включения в подмножество. Оценщику необходимо достигнуть баланса между этими соображениями;

ж) 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;

з) 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;

и) инновационные или необычные функции. В тех случаях, когда в ОО включены инновационные или необычные функции безопасности, которые могут широко быть представлены в маркетинговой литературе, они должны быть прямыми кандидатами на

тестирование.

В данном руководстве сформулированы факторы, которые необходимо рассмотреть в процессе выбора приемлемого тестируемого подмножества ФБО, но они ни в коем случае не являются исчерпывающими.

Руководство по выборке приведено в подразделе 12.2.

ATE_IND.3-5 Оценщик ***должен разработать*** тестовую документацию для тестируемого подмножества ФБО, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов.

Уяснив из ЗБ и функциональной спецификации ожидаемый режим выполнения функции безопасности оценщик должен определить наиболее подходящий способ тестирования данной функции. Оценщиц и особенности рассматривает:

а) подход, который будет использоваться например, будет ли функция безопасности тестироваться через внешний интерфейс, внутренний интерфейс с использованием каких-либо средств автономного тестирования или будет использован альтернативный тестированию подход (например, в исключительных обстоятельствах - экспертиза кода);

б) интерфейс(ы) функции безопасности, который(е) будет(ут) использоваться для инициирования выполнения функции безопасности к наблюдения ее реакции;

в) начальные условия, которые будут необходимы для выполнения теста (т.е., какие бы то ни было конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

г) 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 практичным тестировать каждую функцию безопасности, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования очень специфичного аспекта ожидаемого режима выполнения функции безопасности.

В тестовой документации оценщика следует определить происхождении каждого теста, прослеживая его к соответствующей спецификации проекта и если необходимо к ЗБ.

ATE_IND.3-6 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 течение тестирования. Эти новые тесты записываются в тестовую документацию.

ATE_IND.3-7 Оценщик ***должен зафиксировать*** следующую информацию о тестах, которые составляют подмножество тестов:

а) идентификационную информацию тестируемого режима выполнения функции безопасности;

б) инструкции по подключению и установке всего требуемого оборудования для тестирования, как это требуется для проведения конкретного теста;

в) инструкции по установке всех предварительных условий выполнения теста;

г) инструкции по инициированию функций безопасности;

д) инструкции по наблюдению режима поведения функции безопасности;

е) описание всех ожидаемых результатов и необходимого анализа, который выполняется по отношению к наблюдаемому режиму выполнения дня сравнения с ожидаемыми результатами;

ж) инструкции по завершению тестирования и установке необходимого пост-

тестового состояния ОО;

з) 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). Это решение, как и его строгое обоснования остается за оценщиком.

ATE_IND.3-8 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 ее соответствии со спецификацией либо о том, что тестовая документация оценщика может быть некорректной. Не ожидаемые 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.

Решение опустить эту информацию, как в его строгое обоснование, остается за оценщиком.

10.6.3.3.3 Действие ATE_IND.3.3E

ATE_IND.3-9 Оценщик ***должен провести*** тестирование по всем тестам, находящимся в плане и процедурах тестирования разработчика.

Общая цель данного шага оценивания состоит в выполнении всех тестов разработчика, чтобы подтвердить правильность результатов тестирования разработчиком.

ATE_IND.3-10 Оценщик ***должен проверить,*** что все фактические результаты тестирования согласуются с ожидаемыми результатами тестирования.

Противоречия между ожидаемыми результатами тестирования разработчиков и фактическими результатами тестирования заставляют оценщица разрешать эти несоответствия. Противоречия, с которыми столкнулся оценщик, могут быть разрешены разработчиком путем убедительного объяснения и разрешения противоречий.

ATE_IND.3-11 Оценщик ***должен привести*** в ТОО информацию об усилиях по тестированию, вкратце 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 дать 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 органа по подтверждению соответствия получить некоторое понимание выбранного подхода к тестированию, объема выполненного оценщиком тестирования, объема выполненного разработчиков, тестирования, тестируемых конфигураций ОО и общих результатов вида деятельности по тестированию.

Информация, относящаяся к усилиям оценщика по тестированию, которую обычно можно найти в соответствующем разделе ТОО, включает:

а) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые

тестировались;

б) выбранный размер подмножества. Количество протестированных в течение оценки функций безопасности и строгое обоснование этого размера;

в) критерии выбора для функций безопасности, которые составляют тестируемое подмножество. Краткое изложение факторов, рассмотренных при отборе функций безопасности для включения в подмножество;

г) протестированные функции безопасности. Краткий перечень функций безопасности, включенных в подмножество;

д) выполняемые тесты разработчика. Указание на то, что выполнены все тесты разработчика;

е) заключение 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 дать некоторое представление о типе информации, касающейся тестирования, выполненного оценщиком в течение оценки, которую следует представить в ТОО.

11 Вид деятельности AVA

11.1 Введение

Вид деятельности. «Оценка уязвимостей» позволяет сделать заключение о существовании и пригодности для использования в предопределенной среде недостатков или слабых мест в ОО. Это заключение основывается на анализе, выполненном разработчиком и оценщиком, и поддерживается тестированием, выполненным оценщиком.

11.2 Цели

Вид деятельности «Оценка уязвимостей» предназначен для того, чтобы сделать заключение о существовании и пригодности для использования в предопределенной среде недостатков или слабых мест в ОО.

11.3 Замечания по применению, относящиеся к стойкости функций безопасности и анализу уязвимостей

Сравнение показывает, что между анализом стойкости функций безопасности ОО и анализом уязвимостей (поисков потенциальных уязвимостей, приводящим к тестированию уязвимостей) имеется как существенное сходство, так и существенные различия.

Существенное сходство основано на использовании потенциала нападения. Для обоих видов анализа оценщик определяет минимальный потенциал нападения, требуемый нарушителю, чтобы осуществить нападение, и приходит к заключению относительно возможностей ОО противостоять нападению. В таблице 11.1 и таблице 11.2 демонстрируются и далее описываются взаимосвязи между этими видами анализа и потенциалом нападения.

Таблица 11.1 - Тестирование уязвимостей и потенциал нападения

Компонент анализа уязвимостей	ОО противостоит нарушителю с потенциалом нападения:	Остаточные уязвимости способен использовать только нарушитель с потенциалом нападения:
VLA.4	высокий	Не применимо - успешное нападение за пределами практически возможного
VLA.3	умеренный	высокий
VLA.2	низкий	умеренный

Таблица 11.2 - Стойкость функции безопасности и потенциал нападения

Уровень СФБ	Адекватная защита от нарушителя с потенциалом нападения:	Недостаточная защита от нарушителя с потенциалом нападения:
высокая СФБ	высокий	Не применимо - успешное нападение за пределами практически возможного
средняя СФБ	умеренный	высокий
базовая СФБ	низкий	умеренный

Существенные различия между этими видами анализа основаны на природе функции безопасности ОО, а также на характере нападения. Анализ стойкости функции безопасности ОО выполняется только для функции безопасности реализуемых вероятностными или перестановочными механизмами за исключением тех из них, которые основаны на криптографии. Более того, при анализе предполагается, что вероятностный или перестановочный механизм безопасности реализован безупречно и что функция безопасности используется при нападении с учетом ограничений ее проекта и реализации. Как показано в таблице 11.2 уровень СФБ также отражает нападение, описанное в терминах потенциала нападения для защиты от которого спроектирована функция безопасности, реализуемая вероятностными или перестановочными механизмами.

Анализ уязвимостей применяется ко всем некриптографическим функциям безопасности ОО, включая те из них, механизмы реализации которых, по своей природе являются вероятностными или перестановочными. Не делается никаких предположений относительно корректности проекта и реализации функции безопасности а также не накладывается ограничений на метод нападения или взаимодействие нарушителя с ОО - если нападение возможно, то оно рассматривается в процессе анализа уязвимостей. Как показано в таблице 11.1 успешная оценка в соответствии с компонентом доверия, связанным с анализом уязвимостей отражает уровень источника угрозы, описанный в терминах потенциала нападения для защиты, от которого спроектированы и реализованы все функция безопасности ОО.

11.3.1 Потенциал нападения

11.3 1.1 Применение потенциала нападения

Потенциал нападения является функцией от компетентности, ресурсов и мотивации нарушителя. Потенциал нападения специально рассматривается оценщиком двумя различными способами в процессе оценки ЗБ и при выполнении действий по оценке уязвимостей. В процессе оценки ЗБ оценщик делает заключение, является ли выбор компонентов требовании доверия в особенности компонентов класса оценки уязвимостей, соразмерным с потенциалом нападения источника угроз (приведено ASE_REQ.1.4C).

Случаи, когда требования доверия не соразмерны, могут означать, что-либо оценка не будет обеспечивать достаточное доверие, либо оценка будет излишне трудоемкой в процессе оценки уязвимостей, оценщик использует потенциал нападения, как способ определения возможности использования идентифицированных уязвимостей в предопределенной среде.

11.3.1.2 Трактовка мотивации

Мотивация является фактором потенциала нападения, который может использоваться, чтобы описать различные аспекты, относящиеся 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 или что вследствие немотивированней угрозы нападение не ожидается. Однако за исключением этих двух крайних уровней мотивации, затруднительно нехотя из мотивации, установить вероятность осуществления нападения.

Во-вторых, мотивация может подразумевать определенную ценность актива в денежном или ином выражении для нарушителя или владельца актива. Более ценный актив обусловит, вероятно, белее 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 ценности владелец актива.

В-третьих, мотивация может подразумевать определенную компетентность и ресурсы, с которыми нарушитель намеревается произвести нападение. Можно предполагать, что нарушитель с высокой мотивацией, вероятно, приобретет достаточную компетентность и ресурсы, чтобы преодолеть меры защиты актива. И наоборот, можно предполагать, 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 обеспечит доверие к способности ОО помешать усилиям нарушителя. Когда предопределенная 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 предопределенной среде, чтобы помешать нарушителям с идентифицированной компетентностью и ресурсами.

11.3.2 Вычисление потенциала нападения

В этом подразделе исследуются факторы, которые определяют потенциал нападения, и предоставляется руководство, способствующее устранению некоторой субъективности этого аспекта процесса оценивание. Данный подход следует выбрать, если оценщик не

сделает заключение, что он не является надлежащим, в последнем случае требуется строгое обоснование правильности альтернативного подхода.

11.3.2.1 Идентификация и использование

Чтобы нарушитель использовал уязвимость, ее необходимо сначала идентифицировать, а затем использовать. Это разделение может показаться тривиальным, но является существенным. Чтобы проиллюстрировать это, рассмотрите уязвимость, которая обнаружена после месяцев анализа экспертом, и простой метод нападения, опубликованный в Интернете. Сравните это с уязвимостью, которая широко известна, но требует огромного времени и ресурсов для использования. Понятно, что такие факторы, как время необходимо в этих случаях трактовать по-разному.

Для анализа СФБ проблема использование обычно более важна, так как уязвимости в вероятностных или перестановочных механизмах будут зачастую сами по себе очевидны. Заметьте, однако, что так случается не всегда. Для криптографических механизмов, например, знание неочевидных уязвимостей может значительно влиять на эффективность нападения “грубой силой”. Знание того, что пользователи системы имеют склонность выбирать имена людей в качестве паролей, будет иметь подобный результат. Для оценки уязвимости выше, чем по AVA_VLA.1 начальная идентификация уязвимостей приобретет гораздо более важное значение, так как существование трудных для раскрытия уязвимостей может быть обнародовано, зачастую делая использование тривиальным.

11.3.2.2 Учитываемые факторы

В ходе анализа потенциала нападения требуемого для использования уязвимости, необходимо учитывать следующие факторы:

а) Идентификация:

1) время, затрачиваемое на идентификацию уязвимости;
2) техническая компетентность специалиста;
3) знание проекта и функционирования ОО;
4) доступ к ОО;
5) аппаратные средства/программное обеспечение ИТ или другое оборудование, требуемое для анализа;

б) Использование:

1) время, затрачиваемое на использование уязвимости;
2) техническая компетентность специалиста;
3) знание проекта и функционирования ОО;
4) доступ к ОО;
5) 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.

Время — это время, обычно затрачиваемое нарушителем на непрерывной основе, чтобы идентифицировать или использовать уязвимость. В целях данного обсуждения, *за минуты* означает, что при нападении идентификация и использование уязвимости занимает менее получаса, *за часы* означает нападение, которое может быть успешным менее чем за день; *за дни* означает, что нападение может быть успешным менее чем за месяц, и *за месяцы* означает, что успешное нападение требует, по меньшей мере, месяца.

Компетентность специалиста относится к уровню общих знаний прикладной области или типа продукта (например, операционной системы Unix, протоколов Интернета).

Идентифицированными уровнями являются следующие:

а) *Эксперты* хорошо знакомы с основными алгоритмами, протоколами, аппаратными средствами, структурами и т.п., реализованными в типе продукта или системы, а также с применяемыми принципами и концепциями безопасности;

б) *Профессионалы* хорошо осведомлены, в том, что касается режима безопасности продукта или системы данного типа;

в) *Непрофессионал* слабо осведомлен, по сравнению с экспертом или профессионалом, и не обладает специфической компетентностью.

Знание ОО указывает на определенный уровень знаний об ОО. Оно отличается от общей компетентности, хотя и связано с ней. Идентифицированными уровнями являются следующие:

а) *Отсутствие информации* об ОО кроме его назначения;

б) *Общедоступная информация* об ОО (например, полученная из руководства пользователя);

в) *Чувствительная информация* об ОО (например, сведения о внутреннем содержании проекта).

Здесь следует проявить внимательность, чтобы отделить информацию, необходимую для идентификации уязвимости, от информации, необходимой для ее использования, особенно в области чувствительной информации. Требовать чувствительную информацию об использовании уязвимости было бы необычно.

Доступ к ОО также является важным обстоятельством и имеет отношение к фактору "время". Идентификация или использование уязвимости могут требовать продолжительного доступа к ОО, что может увеличить вероятность обнаружения. Некоторые нападения могут требовать значительных автономных усилий и лишь краткого доступа к ОО для использования уязвимости. Доступ также может быть необходим непрерывный или в виде нескольких сеансов. В целях данного обсуждения, *за минуты* означает, что требуется доступ менее получаса; *за часы* означает, что требуется доступ менее, чем день; *за дни* означает, что требуется доступ менее, чем месяц; и *за месяцы* означает, что требуется доступ, по меньшей мере, в течение месяца. Когда доступ к ОО не увеличивает вероятность обнаружения (например, смарт-карта в распоряжении нарушителя), этот фактор следует игнорировать.

Аппаратные средства/программное обеспечение ИТ или другое оборудование, указывает на оборудование, которое требуется для идентификации или использования уязвимости.

а) *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 или простые сценарии нападения);

б) *Специализированное* оборудование не легко доступно нарушителю, но может быть приобретено без значительных усилий. Оно может включать покупку небольшого количества оборудования (например, анализатора протоколов) или разработку более сложных сценариев и программ нападения;

в) *Заказное оборудование* не легко доступно широкому кругу, поскольку либо может потребоваться его специальная разработка (например, очень сложное программное обеспечение), либо оборудование настолько специализировано, что его распространение контролируется и, возможно, даже ограничено. Или же оборудование может быть очень дорогим. Использование сотен персональных компьютеров связанных через Интернет, как правило, относится к этой категории.

Компетентность специалиста и *знание ОО* связаны с информацией, необходимой

нарушителям, чтобы быть способными к нападению на ОО. Существует неявная зависимость между компетентностью нарушителя и его способностью эффективно использовать оборудование при нападении. Чем ниже компетентность нарушителя, тем ниже потенциал использования 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 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.

11.3.2.3 Подход к вычислению

В предыдущем пункте определены факторы, подлежащие рассмотрению. Однако для проведения стандартной оценки требуется дальнейшее руководство. Для поддержки этого процесса предусмотрен следующий подход. Должны быть представлены конкретные числа с целью достижения уровней, которые согласуются с соответствующими уровнями оценки.

В таблице 11.3 идентифицируются факторы, обсуждавшиеся в предыдущем пункте, и им поставлены в соответствие числовые значения по двум аспектам: идентификации и использованию уязвимости. При определении потенциала нападения для данной уязвимости из каждого столбца для каждого фавора следует выбрать определенное значение (10 значений). При выборе значении должна учитываться предопределенная среда ОО. Выбранные 10 значений суммируются, давая итоговое значение. Это значение затем сверяется с таблицей 11.4 для определения рейтинга.

Когда значение фактора оказывается близким к границе диапазона, то оценщику следует подумать об использовании значения, усредняющего табличные. Например, если для использования уязвимости требуется доступ к ОО в течение одного часа или если доступ обнаруживается очень быстро, то для этого фактора может быть выбрано значение между 0 и 4.

Таблица 11.3 предназначена для руководства.

Для конкретной уязвимости может возникнуть необходимость сделать несколько проходов таблицы для различных сценариев нападения (например, попеременно использовать разные значения компетентности в сочетании со значениями факторов времени или оборудования). Наименьшее значение, полученное для этих проходов, следует сохранить.

В случае уязвимости, которая уже идентифицирована и информация о которой общедоступна, идентифицируемые значения для нарушителя следует выбирать, исходя из раскрытия этой уязвимости в общедоступных источниках, а не из начальной ее идентификации нарушителем.

Затем для получения рейтинга уязвимости следует использовать таблицу 11.4.

Подобный подход не позволяет учесть все обстоятельства и факторы, но должен давать лучшее указание на уровень противодействия нападениям, требуемый для достижения рейтингов, приведенных в таблице 11.4. Другие факторы, такие, как расчет на малую вероятность случайных воздействий или вероятность обнаружения атаки до того как она может быть завершена, не включены в базовую модель, но могут использоваться оценщиком как строгое обоснование для рейтинга иного, чем тот, на который может указывать базовая модель.

В случаях, когда, например, определяется рейтинг механизма пароля, а реализация ОО такова, что допускается очень мало попыток до ограничения нападения, рейтинг стойкости становится почти полностью связанным с вероятностью правильного отгадывания в течение этих немногочисленных попыток. Такие меры ограничения обычно

рассматриваются как часть функции управления доступом и в то время как сам механизм пароля может получить, например, только рейтинг «средняя СФБ», для функции управления доступом может быть вынесено суждение о рейтинге «высокая СФБ».

Следует отметить, что в то время как ряд уязвимостей, оцененных по отдельности, могут указывать на высокое противодействие нападениям, наличие других уязвимостей может изменять табличные значении так, что комбинация уязвимостей будет свидетельствовать о применимости более низкого общего рейтинга. Другими словами, наличие одной уязвимости может упростить использование другой. Предполагается, что такая оценка является частью анализа уязвимостей разработчиком и оценщиком.

Таблица 11.3 - Вычисление потенциала нападения

Название фактора	Диапазон	Значение при идентификации уязвимости	Значение при использовании уязвимости
Затрачиваемое время	< 0.5 часа	0	0
	< 1 день	2	3
	< 1месяц	3	5
	> 1месяц	5	8
	Не практично	*	*
Компетентность	Непрофессионал	0	0
	Профессионал	2	2
	Эксперт	5	4
Знание ОО	Отсутствие информации	0	0
	Общедоступная информация	2	2
	Чувствительная информация	5	4
Доступ к ОО	< 0.5 часа или не обнаруживаемый доступ	0	0
	< 1 день	2	4
	< 1 месяц	3	б
	> 1 месяц	4	9
	Не практично	*	*
Оборудование	Отсутствует	0	0
	Стандартнее	1	2
	Специализированное	3	4
	Заказное	5	6
* Означает что нападение невозможно в пределах тех временных рамок, которые были бы приемлемы для нарушителя. Любое значение «*» указывает на «высокий» рейтинг			

Таблица 11.4 - Рейтинг уязвимостей

Диапазон значений	ОО противостоит нарушителю с потенциалом нападения:
<10	Нет рейтинга
10-17	Низкий
18-24	Умеренный

> 25	Высокий

11.3.3 Пример анализа стойкости функции

Ниже представлен анализ СФБ для гипотетического механизма цифрового пароля.

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:

а) цифровой пароль должен быть не менее четырех и не более шести цифр длиной;

б) последовательные числовые ряды (типа 7,6,5,4,3) не допускаются;

в) 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:

а) Шаблоны, используемые людьми являются важным обстоятельством, которое может влиять на подход к поиску возможных значений цифровых паролей и таким образом влиять на СФБ Допуская самый плохой вариант сценария когда пользователь выбирает число, состоящее только из четырех цифр число перестановок цифрового пароля, предполагая, что каждая цифра уникальна, равно:

$$7(8)(9)(10) = 5040$$

б) Число возможных увеличивающихся рядов - семь, как и число убывающих рядов После сбрасывания этих рядов число возможных значений цифровых паролей равно:

$$5040\text{-}14=5026$$

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:

$$\frac{2513 \text{ìèí}}{60 \frac{\text{ìèí}}{\div \text{àñ}}} \approx 42 \div \text{àñà}$$

Используя подход, описанный в предыдущем подразделе, следует выбирать значения факторов при идентификации, минимальные из каждой категории (все 0), так как существование уязвимости в такой функции очевидно. Основываясь на приведенных выше вычислениях, для непрофессионала является возможным нанести поражение

механизму в пределах дней (при получении доступа к ОО) без использования какого-либо оборудования и без знания ОО что по таблице 11.3 (для использования уязвимостей) дает значение 11. Получив результирующую сумму – 11, потенциал нападения, требуемый для осуществления успешной атаки, определяется, по меньшей мере, как умеренный. Уровни СФБ определены в терминах потенциала нападения в Глоссарии (подраздел 2.3 части 1 ОК). Поскольку для того чтобы утверждать о базовой СФБ, механизм должен противодействовать нарушителю с низким потенциалом нападения, и поскольку механизм цифрового пароля является стойким к нарушителю с низким потенциалом, то этот механизм цифрового пароля, в лучшем случае, соответствует уровню «базовая СФБ».

11.4 Оценка неправильного применения

11.4.1 Подвид деятельности AVA_MSU.1

11.4.1.1 Цели

Цель данного подвида деятельности - сделать заключение, не являются пи руководства вводящими в заблуждение необоснованными или противоречивыми, были ли учтены процедуры безопасности для всех режимов функционирования, и будет ли использование руководств способствовать предотвращению и обнаружению небезопасных состоянии ОО.

11.4.1.2 Замечания по применению

Использование термина *руководства* в этом подвиде деятельности относится к руководству пользователя, руководству администратора и процедурам безопасной инсталляции, генерации и запуска. Здесь к процедурам инсталляции, генерации и запуска относятся все процедуры перевода ОО из состояния при поставке в состояние функционирования, ответственным за выполнение которых является администратор.

11.4.1.3 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

а) ЗБ;

б) функциональная спецификация;

в) руководство пользователя;

г) руководство администратора;

д) процедуры безопасной инсталляции, генерации и запуска.

11.4 1.4 Действия оценщика

Этот подвид деятельности включает три элемента действий оценщика из части 3 ОК:

а) AVA_MSU.1.1E;

6) AVA_MSU.1.2E;

в) AVA_MSU.1.3E.

11.4.1.4.1 Действие AVA_MSU.1.1E

AVA_MSU.1.1C

AVA_MSU_1-1 Оценщик ***должен исследовать*** руководства и другие свидетельства оценки, чтобы сделать заключение, идентифицированы ли в руководства все возможные режимы эксплуатации ОО (включая, если применимо, функционирование после сбоя или ошибки в работе), их последствия и значение для поддержания безопасной эксплуатации.

Другие свидетельства оценки, в особенности функциональная спецификация, представляют источник информации, который оценщику следует использовать, чтобы сделать заключение, содержат ли руководства достаточную руководящую информацию.

Если в пакет доверия включена тестовая документация, то информация, представленная в этом свидетельстве, может также быть использована, чтобы сделать заключение, содержат ли руководства достаточную руководящую информацию. Детали,

представленные в описании шагов тестирования, могут быть использованы для подтверждения того, достаточны ли предоставленные руководства для использования и администрирования ОО.

Оценщику следует сосредоточиться одновременно на одной функции безопасности, сопоставляя руководства для безопасного использования данной функции безопасности с другими свидетельствами оценки, чтобы сделать заключение, достаточны ли руководства в части, относящейся к данной функции безопасности, для ее безопасного использования (т.е., согласовано ли оно с ПБО). Оценщику следует также рассмотреть соотношения между функциями, осуществляя поиск потенциальных конфликтов.

AVA_MSU.1.2C

AVA_MSU.1-2 Оценщик ***должен исследовать*** руководства, чтобы сделать заключение, являются ли они понятными и внутренне непротиворечивыми.

Руководства являются непонятными, если они так или иначе могут быть неправильно истолкованы администратором или пользователем и использоваться путем, причиняющим ущерб ОО или безопасности, обеспечиваемой ОО.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

AVA_MSU.1-3 Оценщик ***должен исследовать*** руководства и другие свидетельства оценки, чтобы сделать заключение, являются ли руководства полными и обоснованными.

Оценщику следует использовать знакомство с ОО, приобретенное при выполнении других видов деятельности по оценке, чтобы сделать заключение, являются ли руководства полными.

В частности, оценщику следует рассмотреть функциональную спецификацию и краткую спецификацию ОО. Предполагается, что все функции безопасности, описанные в этих документах, описываются в руководствах надлежащим образом, чтобы дать возможность их безопасного администрирования и использования. Оценщик может в качестве вспомогательного средства подготовить неформальное отображение между руководствами и этими документами. Какие-либо пропуски в этом отображении могут указывать на неполноту.

Руководства являются необоснованными, если они содержат требования к использованию ОО или среде функционирования, которые противоречат ЗБ или являются чрезмерно обременительными для поддержания безопасности.

Оценщику следует обратить внимание, что результаты, полученные в процессе выполнения шагов оценивания подвида деятельности AGD_ADM, предоставят полезные исходные данные для этого исследования.

AVA_MSU.1.3C

AVA_MSU.1-4 Оценщик ***должен исследовать*** руководства, чтобы сделать заключение, все ли предположения относительно предопределенной среды четко сформулированы.

Оценщик анализирует предположения ЗБ относительно предопределенной среды безопасности ОО и сравнивает их с руководствами, чтобы удостовериться, все ли предположения из ЗБ относительно предопределенной среды безопасности ОО, которые имеют отношение к администратору или пользователю, соответствующим образом описаны в руководствах.

AVA_MSU.1.4C

AVA_MSU.1-5 Оценщик ***должен исследовать*** руководства, чтобы сделать заключение, все ли требования для внешних мер безопасности четко сформулированы.

Оценщик анализирует руководства, чтобы удостовериться, перечислены ли в них все внешние процедурные меры, меры физической защиты, управления персоналом и связностью. Цели безопасности в ЗБ для не-ИТ среды указывают на то, что требуется.

11.4.1.4.2 Действие AVA_MSU.1.2E

AVA_MSU.1-6 Оценщик ***должен выполнить*** все процедуры администратора и пользователя (если применимо), необходимые для конфигурирования и установки ОО, чтобы сделать заключение, может ли ОО быть безопасно сконфигурирован и использован с применением только представленных руководств.

Конфигурация и инсталляция требуют, чтобы оценщик перевел ОО из состояния при поставке в состояние в котором ОО функционирует и осуществляет ПБО, согласованную с целями безопасности, специфицированными в ЗБ.

Оценщику необходимо следовать только процедурам разработчика, задокументированным в руководствах пользователя и администратора, которые обычно поставляются потребителю ОО. Любые встретившиеся трудности в процессе такого применения процедур могут указывать на неполноту, непонятность, противоречивость или необоснованность руководств.

Обратите внимание, что работа, выполненная для удовлетворения данного шага оценивания, может также способствовать удовлетворению действия оценщика ADO_IGS.1.2E.

11.4.1.4.3 Действие AVA_MSU.1.3E

AVA_MSU.1-7 Оценщик ***должен исследовать*** руководства, чтобы сделать заключение, предоставлены ли потребителю руководства, достаточные, чтобы эффективно администрировать и использовать функции безопасности ОО, а также обнаруживать небезопасные состояния.

ОО могут использовать разнообразные способы содействия потребителю в эффективном, с точки зрения безопасности, использовании ОО. Один ОО может использовать функциональные возможности (характеристики), чтобы предупредить потребителя, когда ОО находится в небезопасном состоянии, в то время как другие ОО могут поставляться с расширенными руководствами, содержащими предложения, советы, процедуры и т.д. по наиболее эффективному использованию существующих характеристик безопасности; например, с руководством по использованию характеристики аудита как вспомогательного средства при обнаружении небезопасных состояний.

Чтобы вынести вердикт для этого шага оценивания, оценщик рассматривает функциональные возможности ОО, его назначение и предопределенную среду, а также предположения о его использовании или о пользователях. Оценщику следует прийти к заключению, что, если возможен переход ОО в небезопасное состояние, то имеется ли обоснованное ожидание, что использование руководства позволит своевременно обнаружить небезопасное состояние. Заключение о потенциальной возможности перехода ОО в небезопасные состояния может быть сделано с использованием поставляемых для оценки материалов, таких как ЗБ, функциональная спецификация и какие-либо другие представления проекта, предоставленные в качестве свидетельств для компонентов, включенных в пакет доверия для ОО (например, проект верхнего уровня ФБО, если в пакет доверия включен компонент из семейства ADV_HLD).

11.4.2 Подвид деятельности AVA_MSU.2

11.4 2.1 Цели

Цель данного подвида деятельности - сделать заключение, не являются ли руководства вводящими в заблуждение, необоснованными или противоречивыми, были ли учтены процедуры безопасности для всех режимов функционирования, и будет ли использование руководств способствовать предотвращению и обнаружению небезопасных состояний ОО.

11.4.2.2 Замечания по применению

Использование термина *руководства* в этом подвиде деятельности относится к руководству пользователя, руководству администратора и процедурам безопасной инсталляции, генерации и запуска. Здесь к процедурам инсталляции, генерации и запуска относятся все процедуры перевода ОО из состояния при поставке в состояние функционирования, ответственным за выполнение которых является администратор.

Этот компонент включает требование к анализу, выполняемому разработчиком, которое не присутствует в AVA_MSU.1. Проверку правильности этого анализа не следует использовать как замену собственного исследования оценщиком руководств, но следует использовать, чтобы предоставить свидетельство, что разработчик также явным образом учел проблему неправильного применения

11.4.2.3 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

а) ЗБ

б) функциональная спецификация;

в) руководство пользователя;

г) руководство администратора;

д) процедуры безопасной инсталляции, генерации и запуска;

е) материалы анализа неправильного применения руководств;

11.4 2.4 Действия оценщика

Этот подвид деятельности включает четыре элемента действий оценщика из части 3 ОК:

а) AVA_MSU.2.1E;

б) AVA_MSU.2.2E;

в) AVA_MSU.2.3E;

г) AVA_MSU.2.4E.

11.4.2.4.1 Действие AVA_MSU.2 1E

AVA_MSU.2.1C

AVA_MSU.2-1 Оценщик ***должен исследовать*** руководства и другие свидетельства оценки, чтобы сделать заключение, идентифицированы ли в руководствах все возможные режимы эксплуатации ОО (включая, если применимо, функционирование после сбоя или ошибки в работе), их последствия и значение для поддержания безопасной эксплуатации.

Другие свидетельства оценки, в особенности функциональная спецификация, представляют источник информации, который оценщику следует использовать, чтобы сделать заключение, содержат ли руководства достаточную руководящую информацию.

Если в пакет доверия включена тестовая документация, то информация представленная в этом свидетельстве, может также быть использована, чтобы сделать заключение, содержат ли руководства достаточную руководящую информацию. Детали, представленные в описании шагов тестирования, могут быть использованы для подтверждения того, достаточны ли предоставленные руководства для использования и администрирования ОО.

Оценщику следует сосредоточиться одновременно на одной функции безопасности, сопоставляя руководство для безопасного использования данной функции безопасности с другими свидетельствами оценки, чтобы сделать заключение, достаточны ли руководства в части, относящейся к данной функции безопасности, для ее безопасного использования (т.е., согласовано ли оно с ПБО). Оценщику следует также рассмотреть соотношения между функциями, осуществляя поиск потенциальных конфликтов.

AVA_MSU.2.2C

AVA_MSU.2-2 Оценщик ***должен исследовать*** руководства, чтобы сделать заключение, являются ли они понятными и внутренне непротиворечивыми.

Руководства являются непонятными, если они так или иначе могут быть

неправильно истолкованы администратором или пользователем и использоваться путем, причиняющим ущерб ОО или безопасности, обеспечиваемой ОО.

Руководство по анализу непротиворечивости приведено в подразделе 12.3.

AVA_MSU.2-3 Оценщик ***должен исследовать*** руководства и другие свидетельства оценки, чтобы сделать заключение, являются ли руководства полными и обоснованными.

Оценщику следует использовать знакомство с ОО, приобретенное при выполнении других видов деятельности по оценке, чтобы сделать заключение, являются ли руководства полными.

В частности, оценщику следует рассмотреть функциональную спецификацию и краткую спецификацию ОО. Предполагается, что все функции безопасности, описанные в этих документах, описываются в руководствах надлежащим образом, чтобы дать возможность их безопасного администрирования и использования. Оценщик может в качестве вспомогательного средства подготовить неформальное отображение между руководствами и этими документами. Какие-либо пропуски в этом отображении могут указывать на неполноту.

Руководства являются необоснованными, если они содержат требования к использованию ОО или среде функционирования, которые противоречат ЗБ или являются чрезмерно обременительными для поддержания безопасности.

Оценщику следует обратить внимание, что результаты, полученные в процессе выполнения шагов оценивания подвида деятельности AGD_ADM, предоставят полезные исходные данные для этого исследования.

AVA_MSU.2.3C

AVA_MSU.2-4 Оценщик ***должен исследовать*** руководства, чтобы сделать заключение, все ли предположения относительно предопределенной среды четко сформулированы.

Оценщик анализирует предположения ЗБ относительно предопределенной среды безопасности ОО и сравнивает их с руководствами, чтобы удостовериться, все ли предположения из ЗБ относительно предопределенной среды безопасности ОО, которые имеют отношение к администратору или пользователю, соответствующим образом описаны в руководствах.

AVA_MSU.2.4C

AVA_MSU.2-5 Оценщик ***должен исследовать*** руководства, чтобы сделать заключение, все ли требования для внешних мер безопасности четко сформулированы.

Оценщик анализирует руководства, чтобы удостовериться, перечислены ли в нем все внешние процедурные меры, меры физической защиты, управления персоналом и связностью. Цели безопасности в ЗБ для не-ИТ среды указывают на то, что требуется.

AVA_MSU.2.5C

AVA_MSU.2-6 Оценщик ***должен исследовать*** материалы анализа, выполненного разработчиком, чтобы сделать заключение, предпринял ли разработчик соответствующие меры для обеспечения полноты руководств.

Материалы анализа, выполненного разработчиком, могут включать отображения ЗБ или функциональной спецификации на руководства, чтобы продемонстрировать, что руководства являются полными. Какие бы ни были предоставлены разработчиком свидетельства для демонстрации полноты, оценщику следует оценить материалы анализа, выполненного разработчиком, с учетом любых недостатков, обнаруженных в ходе выполнения шагов оценивания с AVA_MSU.2-1 по AVA_MSU.2-5, а также AVA_MSU.2-7.

11.4.2.4.2 Действие AVA_MSU.2.2E

AVA_MSU.2-7 Оценщик ***должен выполнить*** все процедуры администратора и пользователя (если применимо), необходимые для конфигурирования и установки ОО,

чтобы сделать заключение, может ли ОО быть безопасно сконфигурирован и использован с применением только представленных руководств.

Конфигурация и инсталляция требуют, чтобы оценщик перевел ОО из состояния при поставке в состояние, в котором ОО функционирует и осуществляет ПБО, согласованную с целями безопасности, специфицированными в ЗБ.

Оценщику необходимо следовать только процедурам разработчика, задокументированным в руководствах пользователя и администратора, которые обычно поставляются потребителю ОО. Любые встретившиеся трудности в процессе такого применения процедур могут указывать на неполноту, непонятность, противоречивость или необоснованность руководств.

Обратите внимание, что работа, выполненная для удовлетворения данного шага оценивания, может также способствовать удовлетворению действия оценщика ADO_IGS.1.2E.

AVA_MSU.2-8 Оценщик ***должен выполнить*** другие относящиеся к безопасности процедуры, специфицированные в руководствах, чтобы сделать заключение, может ли ОО быть безопасно сконфигурирован и использован с применением только представленных руководств.

Оценщику необходимо следовать только процедурам разработчика, задокументированным в руководствах пользователя, и администратора, которые обычно поставляются потребителю ОО.

Оценщику следует осуществить выборку при выполнении данного шага оценивания. При осуществлении выборки оценщику следует принять во внимание:

а) ясность руководства. Любое потенциально непонятное руководство следует включить в выборку;

б) руководство, которое будет использоваться наиболее часто. Редко используемое руководство обычно не следует включать в выборку;

в) сложность руководства. Сложное руководство следует включать в выборку;

г) серьезность ошибки. Процедуры, для которых ошибка влияет очень серьезным образом на безопасность, следует включать в выборку;

д) характер ОО. Руководство, связанное с нормальным или наиболее вероятным использованием ОО, следует включать в выборку.

Руководство по выборке приведено в подразделе 12.2.

11.4.2.4.3 Действие AVA_MSU.2 3E

AVA_MSU.2-9 Оценщик ***должен исследовать*** руководства, чтобы сделать заключение, предоставлены ли потребителю руководства, достаточные, чтобы эффективно администрировать и использовать функции безопасности ОО, а также обнаруживать небезопасные состояния.

ОО могут использовать разнообразные способы содействия потребителю в эффективном с точки зрения безопасности использовании ОО. Один ОО может использовать функциональные возможности (характеристики), чтобы предупредить потребителя, когда ОО находится в небезопасном состоянии, в то время как другие ОО могут поставляться с расширенными руководствами, содержащими предложения, советы, процедуры и т.д. по наиболее эффективному использованию существующих характеристик безопасности; например, с руководством по использованию характеристики аудита как вспомогательного средства при обнаружении небезопасных состояний.

Чтобы вынести вердикт для этого шага оценивания, оценщик рассматривает функциональные возможности ОО, его назначение и предопределенную среду, а также предположения о его использовании или о пользователях. Оценщицу следует прийти *к* заключению, что, если возможен переход ОО в небезопасное состояние, то имеется ли

обоснованное ожидание, что использование руководства позволит своевременно обнаружить небезопасное состояние. Заключение о потенциальной возможности перехода ОО в небезопасные состояния может быть сделано с использованием поставляемых для оценки материалов, таких как ЗБ, функциональная спецификация и какие-либо другие представления проекта, предоставленные в качестве свидетельств для компонентов, включенных в пакет доверия для ОО (например, проект верхнего уровня ФБО, если в пакет доверия включен компонент из семейства ADV_HLD).

11.4.2.4.4 Действие AVA_MSU.2.4E

AVA_MSU.2-10 Оценщик ***должен исследовать*** материалы анализа руководств, выполненного разработчиком, чтобы сделать заключение, предоставлено ли руководство по безопасному функционированию во всех режимах функционирования ОО.

Результаты действия по оценке AVA_MSU.2.1E обеспечивают основу для оценки материалов анализа, выполненного разработчиком. Оценивая возможность неправильного применения руководств, оценщику следует быть способным сделать заключение, отвечает ли анализ неправильного применения, выполненный разработчиком, целям этого подвида деятельности.

11.5 Оценка стойкости функций безопасности ОО

11.5.1 Подвид деятельности AVA_SOF.1

11.5.1.1 Цель оценки

Цель данного подвида деятельности - сделать заключение, сделаны ли в ЗБ утверждения о СФБ для всех вероятностных или перестановочных механизмов, и поддержаны ли утверждения о СФБ, сделанные разработчиком в ЗБ, корректным анализом.

11.5.1.2 Замечания по применению

Анализ СФБ выполняется для механизмов, которые по своей природе являются вероятностными или перестановочными, таких как механизм пароля или биометрия. Хотя криптографические механизмы по своей природе являются также вероятностными и зачастую описываются в терминах *стойкости*, AVA_SOF.1 не применим к криптографическим механизмам. Для таких механизмов оценщику следует руководствоваться указаниями системы подтверждения соответствия.

Хотя анализ СФБ выполняется на базе отдельных механизмов, общее заключение о СФБ базируется на функциях. Когда для обеспечения некоторой функции безопасности применяется более одного вероятностного или перестановочного механизма, проанализирован должен быть каждый отдельный механизм. Способ объединения этих механизмов для обеспечения функции безопасности определит общий уровень СФБ для этой функции. Оценщику необходима информация о проекте, чтобы понять, как механизмы работают вместе, чтобы обеспечить функцию, и минимальный уровень для такой информации предоставляется через зависимость от ADV_HLD.1. Фактическая проектная информация, доступная оценщику, определяется ОУД, и эту доступную информацию, когда требуется, следует использовать для поддержки анализа, выполняемого оценщиком.

Обсуждение СФБ в отношении многодоменных ОО приведено в 6.4.6.

11.5.1.3 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются

а) ЗБ;

б) функциональная спецификация;

в) проект верхнего уровня;

г) материалы анализа стойкости функций безопасности ОО.

11.5.1.4 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из часта 3 ОК:

а) AVA_SOF.1.1E;

6) AVA_SOF.1.2E.

11.5.1.4.1 Действие AVA_SOF.1.1E

AVA_SOF.1.1C

AVA_SOF.1-1 Оценщик ***должен проверить***, предоставил ли разработчик материалы анализа СФБ для каждого механизма безопасности, для которого в ЗБ имеется утверждение о СФБ, выраженное как уровень СФБ.

Если утверждения о СФБ выражены исключительно в метрике СФБ, то данный шаг оценивания не применяется.

Уровень СФБ выражается как базовая СФБ, средняя СФБ или высокая СФБ, которые определены в терминах потенциала нападения – см. Глоссарий части 1 ОК. Минимальное общее требование СФБ, выраженное как некоторый уровень, применяется ко всем некриптографическим вероятностным или перестановочным механизмам безопасности. Однако для отдельных механизмов может иметься утверждение о СФБ как некотором уровне, который превышает общее требование СФБ.

Руководство по определению потенциала нападения, необходимого для осуществления нападения, и, следовательно, определению СФБ как некоторого уровня приведено в 11.3.2.

Материалы анализа СФБ включают строгое обоснование утверждения о СФБ, сделанного в ЗБ.

AVA_SOF.1.2C

AVA_SOF.1-2 Оценщик ***должен проверить***, предоставил ли разработчик материалы анализа СФБ для каждого механизма безопасности, для которого имеется утверждение о СФБ в ЗБ, выраженное в некоторой метрике.

Если утверждения о СФБ выражены исключительно как уровни СФБ, то данный шаг оценивания не применяется.

Минимальное общее требование СФБ, выраженное как некоторый уровень, применяется ко всем некриптографическим вероятностным или перестановочным механизмам безопасности. Однако для отдельных механизмов может иметься утверждение о СФБ в метрике, которая удовлетворяет или превосходит общее требование СФБ.

Анализ СФБ включает строгое обоснование утверждения о СФБ, сделанного в ЗБ.

AVA_SOF.1.1C и **AVA_SOF.1.2C**

AVA_SOF.1-3 Оценщик ***должен исследовать*** материалы анализа СФБ, чтобы сделать заключение, являются ли обоснованными любые утверждения или предположения, поддерживающие анализ.

Например, может быть неверным предположение, что конкретная реализация генератора псевдослучайных чисел будет обладать требуемой энтропией, необходимой для отбора данного механизма безопасности в число тех, для которых уместен анализ СФБ.

Ожидается, что предположения, сопровождающие анализ СФБ, отражают *самый плохой случай*, за исключением *случая*, являющегося в соответствии с ЗБ несостоятельным. Когда существует ряд различных возможных сценариев, и они зависят от поведения человека-пользователя или нарушителя, следует предположить сценарий, который представляет самую низкую стойкость, если этот сценарий не был признан ранее несостоятельным.

Например, утверждение о стойкости, основанное на максимальной теоретически

возможной области значений пароля (т.е. комбинаций всех печатных символов ASCII), обычно не является самым плохим случаем, потому что человеку свойственно использовать пароли на естественном языке, существенно уменьшая область значений пароля и ассоциированную с ней стойкость. Однако такое предположение может быть приемлемым, если в конкретном ОО применяются меры ИТ, идентифицированные в ЗБ, такие как фильтры паролей, чтобы минимизировать использование паролей на естественном языке.

AVA_SOF.1-4 Оценщик ***должен исследовать*** материалы анализа СФБ, чтобы сделать заключение, корректны ли любые алгоритмы, принципы, характеристики и вычисления, поддерживающие анализ.

Характер данного шага оценивания сильно зависит от типа рассматриваемого механизма. В 11.3.3 представлен пример анализа СФБ для функции идентификации и аутентификации, которая реализована с использованием механизма пароля; при анализе рассматривается максимальная область значений пароля, чтобы, в конечном счете, прийти к некоторому уровню СФБ. Для биометрии при анализе рассматривается разрешающая способность и другие факторы, влияющие на чувствительность механизма к обману.

СФБ, выраженная как некоторый уровень, основана на минимальном потенциале нападения, требуемом, чтобы нанести поражение механизму безопасности. Уровни СФБ определены в терминах потенциала нападения в Глоссарии части 1 ОК.

Руководство по определению потенциала нападения приведено в 11.3.1.

AVA_SOF.1-5 Оценщик ***должен исследовать*** материалы анализа СФБ, чтобы сделать заключение, каждое ли утверждение о СФБ удовлетворено или превышено.

Руководство по ранжированию утверждений о СФБ приведено в 11.3.1.

AVA_SOF.1-6 Оценщик ***должен исследовать*** материалы анализа СФБ, чтобы сделать заключение, все ли функции с заявленной СФБ удовлетворяют минимальному уровню стойкости, определенному в ЗБ.

11.5.1.4.2 Действие AVA_SOF.1.2E

AVA_SOF.1-7 Оценщик ***должен исследовать*** свидетельства проекта, представленные для оценки, чтобы сделать заключение, для всех ли вероятностных или перестановочных механизмов имеется утверждение о СФБ.

Идентификация разработчиком функций безопасности, которые реализованы вероятностными или перестановочными механизмами, верифицируется в процессе оценки ЗБ. Однако, поскольку краткая спецификация ОО может быль единственным свидетельством, доступным при выполнении этих действий, идентификация таких механизмов может быть неполной. Дополнительные свидетельства оценки, требуемые в качестве исходных данных для этого подвида деятельности, (функциональная спецификация и проект верхнего уровня) и какие-либо другие свидетельства (например, проект нижнего уровня, руководства) могут идентифицировать дополнительные вероятностные или перестановочные механизмы, ранее не идентифицированные в ЗБ. Если это так, то ЗБ должно быть соответствующим образом обновлено, чтобы отразить дополнительные утверждения о СФБ, а разработчику будет необходимо представить материалы дополнительного анализа, в которых строго обосновываются утверждения о СФБ. в качестве исходных данных для действия оценщика AVA SOF.1.1E.

AVA_SOF 1-8 Оценщик ***должен исследовать*** утверждения о СФБ, чтобы сделать заключение, являются ли они корректными.

Когда материалы анализа СФБ включают утверждения или предположения (например, о возможном количестве попыток аутентификации в минуту), оценщику следует независимо подтвердить, что они корректны. Это может быть достигнуто путем тестирования или независимого анализа.

11.6 Оценка анализа уязвнмостей

11.6.1 Замечания по применению

Использование термина *руководства* в этом подвиде деятельности относится к руководству пользователя, руководству администратора и процедурам безопасной инсталляции, генерации и запуска.

Рассмотрение пригодных для использования уязвимостей определяется целями безопасности и функциональными требованиями в ЗБ. Например, если меры по предотвращению обхода функций безопасности не требуются в ЗБ (FPT_PHP, FPT_RVM и FPT_SEP отсутствуют), то уязвимости, на которых базируется обход, рассматривать не следует.

Уязвимости могут быть или не быть идентифицированы в общедоступных источниках и могут требовать или не требовать навыка для их использования. Эти два аспекта являются связанными, но различными. Не следует предполагать, что уязвимость может быть легко использована просто потому, что она идентифицирована в общедоступных источниках.

Следующие термины используются в данном руководстве с конкретным значением:

а) уязвимость - слабость в ОО, которая может быть использована, чтобы нарушить политику безопасности в некоторой среде;

б) анализ уязвимостей - систематический поиск уязвимостей в ОО и оценка найденных уязвимостей, чтобы сделать заключение об их значимости для предопределенной среды ОО;

в) явная уязвимость - уязвимость, которая является открытой для использования, требующего минимума понимания ОО, технических познаний и ресурсов;

г) потенциальная уязвимость – уязвимость, существование которой в ОО предполагается (на основании теоретически допускаемого маршрута нападения), но не подтверждено;

д) пригодная для использования уязвимость - уязвимость ОО, которая может быть использована в предопределенной среде;

е) непригодная для использования уязвимость - уязвимость ОО, которая не может быть использована в предопределенной среде;

ж) остаточная уязвимость - непригодная для использования уязвимость ОО, которая могла бы быть использована нарушителем с более высоким потенциалом нападения, чем ожидается в предопределенной среде;

з) тестирование проникновения - тестирование, выполняемое, чтобы сделать заключение о пригодности к использованию в предопределенной среде ОО идентифицированных потенциальных уязвимостей ОО.

11.6.2 Подвид деятельности AVA_VLA.1

11.6.2.1 Цель

Цель данного подвида деятельности - сделать заключение, имеет ли ОО, находящийся в своей предопределенной среде, явные уязвимости, пригодные для использования.

11.6.2.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

а) ЗБ;

б) функциональная спецификация;

в) проект верхнего уровня;

г) руководство пользователя;

д) руководство администратора;

е) процедуры безопасной инсталляции, генерации и запуска;

ж) материалы анализа уязвимостей;

з) ОО, пригодный для тестирования.

Дополнительным исходным материалом для данного подвида деятельности является:

а) текущая информация касательно явных уязвимостей (например, от органа по подтверждению соответствия).

11.6.2.3 Действия оценщика

Этот подвид деятельности включает два элемента действий оценщика из часта 3 ОК:

а)AVA_VLA.1.1E;

б)AVA_VLA.1.2E.

11.6.2.3.1 Действие AVA_VLA.1.1E

AVA_VLA.1.1C

AVA_VLA.1-1 Оценщик ***должен исследовать*** материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, вся ли относящаяся к делу информация рассмотрена при поиске явных уязвимостей.

Предполагается, что анализ уязвимостей, выполненный разработчиком, охватывает поиск разработчиком явных уязвимостей, по меньшей мере, во всех поставляемых для оценки материалах и общедоступных источниках информации. Оценщику следует использовать поставляемые для оценки материалы не для выполнения независимого анализа уязвимостей (что не требуется AVA_VLA.1), а как основу для оценки поиска разработчиком явных уязвимостей.

Информация в общедоступных источниках является очень динамичной. Поэтому возможно, что о новых уязвимостях будет сообщено в общедоступных источниках в период между временем, когда разработчик выполняет анализ уязвимостей, и временем завершения оценки. Моментом превращение мониторинга информации в общедоступных источниках является выпуск органом по подтверждению соответствия результатов оценки; поэтому за указаниями следует обращаться к органу по подтверждению соответствия.

AVA_VLA.1-2 Оценщик ***должен исследовать*** материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, описана ли каждая явная уязвимость и дано ли обоснование того, почему она является непригодной для использования в предопределенной среде ОО.

Предполагается, что разработчик выполнил поиск явных уязвимостей, основываясь на знании ОО и информации из общедоступных источников. Требование задано только по идентификации явных уязвимостей, при этом подробный анализ не предполагается.

Разработчик фильтрует эту информацию на основе вышеизложенного определения и показывает, что явные уязвимости являются непригодными для использования в предопределенной среде.

Оценщику необходимо обратить внимание на три аспекта анализа, выполненного разработчиком:

а) были ли при анализе разработчиком рассмотрены все поставляемые для оценки материалы;

б) приняты ли соответствующие меры для предотвращения использования явных уязвимостей в предопределенной среде;

в) остались ли некоторые явные уязвимости неидентифицированными.

Оценщику не следует беспокоиться, являются ли идентифицированные уязвимости явными или не являются, если это не используется разработчиком в качестве основы для заключения о непригодности уязвимостей для использования. В этом случае оценщик

проверяет правильность утверждении, делая заключение о противодействии нарушителю с низким потенциалом нападения по отношению к идентифицированной уязвимости.

Понятие *явные уязвимости* не связано с понятием *потенциал нападения*. Последний определяется оценщиком в ходе независимого анализа уязвимостей. Так как эти действия не выполняются для AVA_VLA.1, то обычно поиск и фильтрация информации на основе потенциала нападения оценщиком не осуществляются. Однако оценщик может еще обнаружить потенциальные уязвимости в ходе оценки, а заключение, как их следует учитывать, делается путем ссылки на определение явных уязвимостей и понятие низкого потенциала нападения.

Заключение, остались ли некоторые явные уязвимости неидентифицированными, ограничивается оценкой правильности анализа, выполненного разработчиком, сравнением с информацией об уязвимостях из общедоступных источников, а также сравнением с любыми последующими уязвимостями, идентифицированными оценщиком в ходе выполнения других действий по оценке.

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

а) функции или меры безопасности в (ИТ или не-ИТ) среде предотвращают использование уязвимости в предопределенной среде. Например, ограничивая физический доступ к ОО только уполномоченными пользователями, можно фактически сделать уязвимость ОО к вмешательству непригодной для использования;

б) уязвимость является пригодной для использования, но только нарушителями, обладающими умеренным или высоким потенциалом нападения. Например, уязвимость распределенного ОО к нападениям, связанным с перехватом сеанса, требует потенциала нападения выше, чем требуется для использования явной уязвимости. Однако такие уязвимости приводятся в ТОО в качестве остаточных уязвимостей;

в) в ЗБ либо не утверждается о противостоянии определенной угрозе, либо не утверждается о следовании определенной политике безопасности организации, которая может быть нарушена. Например, для межсетевого экрана, в ЗБ которого не заявлена политика доступности и который уязвим к TCP SYN-атакам (нападение на общепринятый протокол Интернета, которое лишает хосты способности к обслуживанию запросов на соединение), не следует делать отрицательного заключения по данному действию оценщица только на основе одной этой уязвимости.

Руководство по определению потенциала нападения, необходимого для использования уязвимости см. в 11.3.2.

AVA_VLA.1-3 Оценщик ***должен исследовать*** материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, согласуются ли они с ЗБ и руководствами.

Анализ уязвимостей разработчиком может быть направлен на некоторую уязвимость с предложением конкретных конфигурации или настроек функции ОО. Если такие ограничения применения считаются действенными и согласованными с ЗБ, то предполагается, что все такие конфигурации/настройки адекватно списаны в руководствах, чтобы их мог применить потребитель

11.6.2.3.2 Действие AVA_VLA.1.2E

AVA_VLA.1-4 Оценщик ***должен придумать*** тесты проникновения, основываясь на материалах анализа уязвимостей, выполненного разработчиком.

Оценщик готовит к тестированию проникновения:

а) то, что необходимо, чтобы попытаться опровергнуть анализ разработчика в случаях, когда обоснование разработчиком непригодности уязвимости для использования является, по мнению оценщика сомнительным;

б) то, что необходимо, чтобы сделать заключение о восприимчивости ОО,

находящегося в своей предопределенной среде, к явкой уязвимости, не рассмотренной разработчиком. Оценщику необходимо иметь доступ к текущей информации (например, от органа по подтверждению соответствия) о явных уязвимостях из общедоступных источников, которые могли быть не рассмотрены разработчиком; оценщик также мог идентифицировать потенциальные уязвимости в результате выполнения других действии по оценке.

Не предполагается тестирования оценщиком на предмет наличия уязвимостей (в том числе известных из общедоступных источников), помимо тех, которые являются явными. Однако в некоторых случаях необходимо будет выполнить тест прежде, чем пригодность к использованию может быть определена. Когда в результате исследований в ходе оценки оценщик обнаруживает некоторую уязвимость, помимо явных, она приводится в ТОО как остаточная уязвимость.

Поняв предполагаемую явную уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. В частности оценщик рассматривает:

а) интерфейсы функций безопасности, которые будут использоваться для инициирования выполнения ФБО и наблюдения их реакции;

б) начальные условия, которые будут необходимы для выполнения теста (т.е., какие-либо конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

в) специальное оборудование для тестирования, которое потребуется либо для инициирования функции безопасности, либо для наблюдения за функцией безопасности (хотя маловероятно, что специальное оборудование потребовалось бы для использования явной уязвимости).

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной явной уязвимости.

AVA_VLA.1-5 Оценщик ***должен разработать*** тестовую документацию для тестов проникновения, основанных на материалах анализа уязвимостей, выполненного разработчиком, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов. Тестовая документация должна включать:

а) идентификацию тестируемой явной уязвимости ОО;

б) инструкции по подключению и установке всего требуемого тестового оборудования, как требуется для проведения конкретного теста проникновения;

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

г) инструкции по инициированию ФБО;

д) инструкции по наблюдению режима выполнения ФБО;

е) описание всех ожидаемых результатов и необходимого анализа, который выполняется по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

ж) инструкции по завершению тестирования и установке необходимого пост-тестового состояния ОО.

Цель определения данного уровня детализации в тестовой документации – дать возможность другому оценщику повторить тесты и получить эквивалентный результат.

AVA_VLA.1-6 Оценщик ***должен провести*** тестирование проникновения, основываясь на материалах анализа уязвимостей, выполненного разработчиком.

Оценщик использует документацию для тестов проникновения, разработанную на шаге оценивания AVA_VLA.1-4, как основу для выполнения тестов проникновения по отношению к ОО, но это не препятствует оценщику выполнить дополнительные

специальные тесты проникновения. Если потребуется, оценщик может придумать специальные тесты в результате изучения информации в процессе тестирования проникновения, которые, если выполнялись оценщиком, заносятся в документацию для тестов проникновения. Такие тесты могут потребоваться, чтобы разобраться с непредвиденными результатами или наблюдениями или исследовать потенциальные уязвимости, существование которых предположил оценщик во время предварительно запланированного тестирования.

AVA_VLA 1-7 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), общий результат должен быть идентичным. Любые различия следует строго обосновать.

AVA_VLA.1-8 Оценщик ***должен исследовать*** результаты всего тестирования проникновения и выводы по всему анализу уязвимостей, чтобы сделать заключение, что ОО (в своей предопределенной среде) не имеет пригодных для использования явных уязвимостей.

Если результаты показывают, что ОО имеет явные уязвимости, пригодные для использования в его предопределенной среде, то это приводит к отрицательному вердикту по данному действию оценщика.

AVA_VLA.1-9 Оценщик ***должен привести*** в ТОО информацию об усилиях оценщика по тестированию проникновения, вкратце 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 этой информации состоит в том, чтобы дать краткий содержательный 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 предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органа по подтверждению соответствия 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, которую обычно можно найти в соответствующем разделе ТОО, включает:

а) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые подвергались тестированию проникновения;

б) функции безопасности, которые подвергались тестированию проникновения. Краткий перечень функций безопасности, на которых было сосредоточено тестирование проникновения;

в) вердикт по данному подвиду деятельности. Общее решение по результатам тестирования проникновения.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует представить в ТОО.

AVA_VLA.1-10 Оценщик ***должен привести*** в ТОО информацию обо всех пригодных для использования уязвимостях и остаточных уязвимостях, детализируя для каждой:

а) ее источник (например, стала известна при выполнении действий МО, известна оценщику, прочитана в публикации);

б) связанную с ней функцию (функции) безопасности, не достигнутую цель (цели), нарушенную политику (политики) безопасности организации, реализованную угрозу (угрозы);

в) описание;

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

д) идентификацию частника оценки (например, разработчик, оценщик), который ее идентифицировал.

11.6.3 Подвид деятельности AVA_VLA.2

11.6.3.1 Цель

Цель данного подвида деятельности - сделать заключение, имеет ли ОО, находящийся в своей предопределенной среде, уязвимости, пригодные для использования нарушителями, обладающими низким потенциалом нападения.

11.6.3.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

а) ЗБ;

б) функциональная спецификация;

в) проект верхнего уровня;

г) проект нижнего уровня;

д) подмножество представления реализации;

е) модель политики безопасности ОО;

ж) руководство пользователя;

з) руководство администратора;

и) процедуры безопасной инсталляции, генерации и запуска;

к) материалы анализа уязвимостей;

л) ОО, пригодный для тестирования.

Дополнительным исходным материалом для данного подвида деятельности является:

а) текущая информация о явных уязвимостях (например, от органа по подтверждению соответствия).

11.6.3.3 Действия оценщика

Этот подвид деятельности включает пять элементов действии оценщика из части 3 ОК:

а) AVA_VLA.2.1E;

б) AVA_VLA.2.2E;

в) AVA_VLA.2.3E;

г) AYA_VLA.2.4E;

д) AVA_VLA.2.5E.

11.6.3.3.1 Действие AVA_VLA.2.1E

AVA_VLA.2.1C, AVA_VLA.2.2C

AVA_VLA.2-1 Оценщик ***должен исследовать*** материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, вся ли относящаяся к делу информация, рассмотрена при поиске уязвимостей.

Предполагается, что анализ уязвимостей, выполненный разработчиком, охватывает поиск разработчиком уязвимостей, по меньшей мере, во всех поставляемых для оценки материалах и общедоступных источниках информации.

Информация в общедоступных источниках является высоко динамичной. Поэтому возможным является, что о новых уязвимостях будет сообщено в общедоступных источниках в период между временем, когда разработчик выполняет анализ уязвимостей, и временем завершения оценки. Моментом прекращения мониторинга информации в общедоступных источниках является выпуск органом по подтверждению соответствия результатов оценки; поэтому за указаниями следует обращаться к органу по подтверждению соответствия.

AVA_VLA.2-2 Оценщик ***должен исследовать*** материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, описана ли каждая идентифицированная уязвимость, и дано ли обоснование того, почему она является непригодной для использования в предопределенной среде ОО.

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

а) функции или меры безопасности в (ИТ или не-ИТ) среде предотвращают использование уязвимости в предопределенной среде. Например, ограничивал физический доступ к ОО только уполномоченными пользователями, можно фактически сделать уязвимость ОО к вмешательству непригодной для использования;

б) уязвимость является пригодной для использования, но только нарушителями, обладающими умеренным или высоким потенциалом нападения. Например, уязвимость распределенного ОО к нападениям, связанным с перехватом сеанса, требует потенциала нападения выше, чем низкий. Однако такие уязвимости приводятся в ТОО в качестве остаточных уязвимостей;

в) в ЗБ либо не утверждается о противостоянии соответствующей угрозе, либо не утверждается о следовании политике безопасности организации, которая может быть нарушена. Например, для межсетевого экрана, в ЗБ которого не заявлена политика доступности и который уязвим к TCP SYN-атакам (нападение на общепринятый протокол Интернета, которое лишает хосты способности к обслуживанию запросов на соединение), не следует делать отрицательного заключения по данному действию оценщица только на основе одной этой уязвимости.

Руководство по определению потенциала нападения, необходимого для использование уязвимости, приведено в 11.3.2.

AVA_VLA.2-3 Оценщик ***должен исследовать*** материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, согласуются ли они с ЗБ и руководствами.

Анализ уязвимостей разработчиком может быть направлен на некоторую уязвимость с предложением конкретных конфигурации или настроек функций ОО. Если такие ограничения применения считаются действенными и согласованными с ЗБ, то предполагается, что все такие конфигурации/настройки адекватно описаны в руководствах, чтобы их мог применить потребитель.

11.6.3.3.2 Действие AVA_VLA.2.2E

AVA_VLA.2-4 Оценщик ***должен придумать*** тесты проникновения, основываясь на материалах анализа уязвимостей, выполненного разработчиком.

Оценщик готовит к тестированию проникновения:

а) то, что необходимо, чтобы попытаться опровергнуть анализ разработчика в случаях, когда обоснование разработчиком непригодности уязвимости для использования является, по мнению оценщика, сомнительным;

б) то, что необходимо, чтобы сделать заключение о восприимчивости ОО, находящегося в своей предопределенной среде, к уязвимости, не рассмотренной разработчиком. Оценщику необходимо иметь доступ к текущей информации (например, от органа по подтверждению соответствия) о явных уязвимостях из общедоступных

источников касаемо явных уязвимостей, которые могли быть не рассмотрены разработчиком, оценщик также мог идентифицировать потенциальные уязвимости в результате выполнения других действий по оценке.

Не предполагается тестирования оценщиком на предмет наличия уязвимостей (в том числе известных из общедоступных источников), помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение. Однако в некоторых случаях необходимо будет выполнить тест прежде, чем требуемый потенциал нападения может быть определен. Когда в результате исследовании в ходе оценки оценщик обнаруживает уязвимость, которая является пригодной для использования только нарушителем с большим, чем низкий, потенциалом нападение, она приводится в ТОО как остаточная уязвимость.

Поняв предполагаемую уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. В частности оценщик рассматривает:

а) интерфейсы функций безопасности, которые будут использоваться для инициирования выполнения ФБО и наблюдения их реакции;

б) начальные условия, которые будут необходимы для выполнения теста (т.е., какие-либо конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

в) специальное оборудование для тестирования, которое потребуется либо для инициирования функции безопасности, либо для наблюдения за функцией безопасности.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной уязвимости.

AVA_VLA.2-5 Оценщик ***должен разработать*** тестовую документацию для тестов проникновения, основанных на материалах анализа уязвимостей, выполненного разработчиком, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов. Тестовая документация должна включать:

а) идентификацию тестируемой уязвимости ОО;

б) инструкции по подключению и установке всего требуемого тестового оборудования, как требуется для проведения конкретного теста проникновения;

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

г) инструкции по инициированию ФБО;

д) инструкции по наблюдению режима выполнения ФБО;

е) описание всех ожидаемых результатов и необходимого анализа, который выполняется по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

ж) инструкции по завершению тестирования и установке необходимого пост-тестового состояния ОО.

Цель установления данного уровня детализации в тестовой документации – дать возможность другому оценщику повторить тесты и получить эквивалентный результат.

AVA_VLA.2-6 Оценщик ***должен провести*** тестирование проникновения, основываясь на материалах анализа уязвимостей, выполненного разработчиком.

Оценщик использует документацию для тестов проникновения, разработанную на шаге оценивания AVA_VLA.2-4, как основу для выполнения тестов проникновения по отношению к ОО, но это не препятствует оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может придумать специальные тесты в результате изучения информации в процессе тестирование проникновения, которые, если выполнялись оценщиком, заносятся в документацию для тестов проникновение. Такие тесты могут потребоваться, чтобы разобраться с

непредвиденными результатами или наблюдениями или исследовать потенциальные уязвимости, существование которых предположил оценщик во время предварительно запланированного тестирования.

AVA_VLA.2-7 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), общий результат должен быть идентичным. Любые различия следует строго обосновать.

AVA_VLA.2-8 Оценщик ***должен привести*** в ТОО информацию об усилиях оценщика по тестированию проникновения, вкратце 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 этой информации состоит в том, чтобы дать краткий содержательный 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 предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органа по подтверждению соответствия 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, которую обычно можно найти в соответствующем разделе ТОО, включает:

а) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые подвергались тестированию проникновения;

б) функции безопасности, которые подвергались тестированию проникновения. Краткий перечень функции безопасности, на которых было сосредоточено тестирование проникновения;

в) вердикт по данному подвиду деятельности. Общее решение по результатам тестирования проникновения.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует представить в ТОО.

11.6.3.3.3 Действие AVA_VLA.2.3E

AVA_VLA.2-9 Оценщик ***должен исследовать*** все исходные данные для данного подвида деятельности, чтобы сделать заключение о возможных уязвимостях безопасности, не учтенных ранее при анализе уязвимостей разработчиком.

Следует использовать методологию гипотез о недостатках, посредством которой анализируются спецификации и документация ОО, а после этого делаются предположения об уязвимостях в ОО. Затем перечень предполагаемых уязвимостей упорядочивается по приоритетам на основе оцененной вероятности существования 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 используется для руководства тестированием проникновения в ОО.

Руководство по определению потенциала нападения, необходимого для

использование уязвимости, приведено в 11.3.2.

Уязвимости, предполагаемые как пригодные для использования только нарушителями, обладающими умеренным или высоким потенциалом нападения, не приводят к отрицательному заключению по этому действию оценщика. Когда материалы анализа подтверждают данную гипотезу, то соответствующие уязвимости в дальнейшем не рассматриваются в качестве исходных данных для тестирования проникновения. Однако такие уязвимости приводятся в ТОО в качестве остаточных уязвимостей.

Уязвимости, предположительно пригодные для использования нарушителем, обладающим низким потенциалом нападения, которые не приводят к нарушению целей безопасности, указанных в ЗБ, не приводят к отрицательному вердикту по этому действию оценщика. Когда материалы анализа подтверждают данную гипотезу, то нет необходимости рассматривать соответствующие уязвимости в дальнейшем в качестве исходных данных для тестирования проникновения.

Уязвимости, предполагаемые как потенциально пригодные для использования нарушителем, обладающим низким потенциалом нападения, и приводящие к нарушению целей безопасности, следует отнести к самым высоко-приоритетным потенциальным уязвимостям, содержащимся в перечне, используемом для руководства тестированием проникновения в ОО.

Исходя из конкретных угроз, присутствующих в предопределенной среде, оценщику при независимом анализе уязвимостей следует рассмотреть характерные уязвимости под каждой из следующих рубрик:

а) уязвимости, характерные для конкретного типа оцениваемого ОО, которые могут быть указаны органом по подтверждению соответствия;

б) обход;

в) вмешательство;

г) прямые нападения;

д) неправильное применение.

Пункты б) – д) далее объясняются более детально.

Обход

Обход включает любой способ, посредством которого нарушитель мог бы избежать осуществления мер безопасности путем:

а) использования возможностей интерфейсов ОО или утилит, которые могут взаимодействовать с ОО;

б) наследования привилегий или других возможностей, которые следовало бы наоборот запретить;

в) (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:

а) Нападения, основанные на использовании возможностей интерфейсов или утилит, обычно используют в своих целях отсутствие требуемых мер безопасности для этих интерфейсов. Например, получение доступа к функциональные 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.

б) 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 функции безопасности вызывается на одном из интерфейсов ОО (например, проверка управление доступом), то оценщику следует рассмотреть, возможен ли обход функции безопасности путем выполнения соответствующего вызова в более поздней точке последовательности или пропуска ее целиком;

в) 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 использованием анализаторов сетевого трафика (дополнительным компонентом здесь является анализатор сетевого трафика);

г) 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 предопределялась. 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);

д) Использование подробностей реализации, представленных в менее абстрактных представлениях, опять включает использование скрытых каналов, через которые нарушитель использует в своих целях дополнительные функции, ресурсы или атрибуты, представленные в ОО, как последствия процесса усовершенствования (например, использование переменной типа «блокировка» как скрытого канала). Дополнительные функциональные возможности также могут обеспечиваться тестовыми фрагментами кода, содержащимися в программных модулях ОО;

е) 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 высоко чувствительных 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;

ж) Нападения, основанные на наследовании привилегий, в основном базируются на незаконном приобретении привилегий или возможностей некоторого привилегированного компонента ОС, 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 к свойств, на которые полагаются компоненты белее низкого уровня.

з) 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 автоматически выполняются при редактировании данного файла или получении доступа к нему, наследуя, таким образом, привилегии, которые имеет владелец файла);

и) 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 систем, то может оказаться возможным поручить такой доступ сразу после выполнения входной последовательности, исследуя, пока пароль аутентифицируется, результаты ввода различных управляющих или *escape*-последовательностей;

к) Нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня, включает нападения, основанные на выходе из-под действия ограничении 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;

л) 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 пользователи могут получить. 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, высокий системный) и кто имеет доступ к этому каталогу.

Вмешательство

Вмешательство включает любое нападение, основанное на попытке нарушителя повлиять на режим выполнения функции безопасности или механизма (т.е., искажение или блокировка), например, путем:

а) доступа к данным, на конфиденциальность или целостность которых полагается функция или механизм безопасности;

б) вынуждения ОО функционировать в необычных или непредусмотренных условиях;

в) отключения или задержки обеспечения безопасности.

В ходе независимого анализа уязвимостей оценщику следует рассмотреть (когда это уместно) каждый из следующих аспектов:

а) Нападение 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.

б) Чтение, запись или модификация внутренних данных прямо или косвенно охватывают следующие типы нападении, 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.

в) Может оказаться возможным обмануть доверенный процесс для модификации защищенного файла, к которому в обычном состоянии доступ не был бы получен;

г) Оценщику следует также рассмотреть следующие "опасные характеристики":

1) исходный текст 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.

д) 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);

е) 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;

ж) 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.

з) 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.

и) 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, то может ли это дать преимущества нарушителю;

к) Корректный режим выполнения функций безопасности может зависеть от предположений, которые нарушаются при 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.

л) 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.

м) 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.

н) Необходимо исследовать результаты завершения процессов, критических для безопасности (например, демона 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);

о) 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;

п) Использование взаимного влияния компонентов, которое невидимо на более высоком уровне абстракции, может обеспечить способ задержки критического по времени доверенного процесса.

Прямые нападения

Прямое нападение включает идентификацию любых тестов проникновения, необходимых для подтверждения или опровержения заявленной минимальной стойкости функций безопасности. При идентификации тестов проникновения под этим заголовком оценщику следует также осознать возможность существования уязвимостей вследствие наличия механизмов безопасности, восприимчивых к прямым нападениям.

Неправильное применение

Неправильное применение включает идентификацию любых тестов проникновения, необходимых для подтверждения или опровержения материалов анализа неправильного применения. Вопросы, подлежащие рассмотрению, включают:

а) режим функционирования ОО при активации запуска, завершения работы или восстановления после ошибок;

б) режим функционирования ОО в экстремальных условиях (иногда называемых перегрузкой или асимптотическим режимом), в частности, когда это могло бы привести к деактивации или отключению некоторой функции или механизма, направленных на обеспечение безопасности;

в) любая потенциальная возможность неумышленной ошибки в конфигурации или небезопасного использования, являющегося результатом нападений, упоминавшихся выше под рубрикой «Вмешательство».

11.6.3.3.4 Действие AVA_VLA.2.4E

AVA_VLA.2-10 Оценщик ***должен придумать*** тесты проникновения, основанные на независимом анализе уязвимостей.

Оценщик готовится к тестированию проникновения, основываясь на упорядоченном по приоритетам перечне уязвимостей, предположения о существовании которых были сделаны при выполнении действия оценщика AVA_VLA.2.3E.

Не предполагается тестирования оценщиком уязвимостей, помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение. Однако в результате исследований в ходе оценки оценщик может обнаружить уязвимость, которая является пригодной для использования только нарушителем с большим, чем низкий, потенциалом нападение. Такие уязвимости приводятся в ТОО как остаточные уязвимости.

Поняв предполагаемую уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. В частности оценщик рассматривает:

а) интерфейсы функций безопасности, которые будут использоваться для инициирования выполнения ФБО и наблюдения их реакции;

б) начальные условия, которые будут необходимы для выполнения теста (т.е., какие-либо конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

в) специальное оборудование для тестирования, которое потребуется либо для инициирования функции безопасности либо для наблюдения за функцией безопасности.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной уязвимости.

AVA_VLA.2-11 Оценщик ***должен разработать*** тестовую документацию для тестов проникновения, основанных на независимом анализе уязвимостей, детализация которой достаточна, чтобы обеспечить повторяемость тестов. Тестовая документация должна включать:

а) идентификацию явкой уязвимости, на предмет которой тестируется ОО;

б) инструкции по подключению и установке всего требуемого тестового оборудования, как требуется для проведения конкретного теста проникновения;

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

г) инструкции по инициированию ФБО;

д) инструкции по наблюдению режима выполнения ФБО;

е) описание всех ожидаемых результатов и необходимого анализа, который выполняется по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

ж) инструкции по завершению тестирования и установке необходимого пост-тестового состояния ОО.

Цель установления данного уровня детализации в тестовой документации – дать возможность другому оценщику повторить тесты и получить эквивалентный результат.

AVA_VLA.2-12 Оценщик ***должен провести*** тестирование проникновения, основываясь на независимом анализе уязвимостей.

Оценщик использует документацию для тестов проникновения, полученную на шаге оценивания AVA_VLA.2-10, как основу для выполнения тестов проникновения по отношению к ОО, но это не мешает оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может придумать новые тесты в результате изучения информации в процессе тестирования проникновения, которые если выполнялись оценщиков, необходимо зафиксировать в документации для тестов проникновения. Такие тесты могут потребоваться, чтобы разобраться с результатами или наблюдениями, отличными от ожидаемых, или исследовать потенциальные уязвимости, о существовании которых сделал предположение оценщик во время предварительно запланированного тестирования.

Если тестирование проникновения показывает, что предполагавшаяся уязвимость не существует, то оценщику следует сделать заключение, был ли корректным или не был корректным собственный анализ оценщика, или не являются ли предоставленные для оценки материалы некорректными или неполными.

AVA_VLA.2-13 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), общий результат должен быть идентичным. Любые различия следует строго обосновать.

AVA_VLA.2-14 Оценщик ***должен принести*** в ТОО информацию об усилиях оценщика по тестированию проникновения, вкратце 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 этой информации состоит в том, чтобы дать содержательный краткий обзор усилий оценщика по тестированию проникновения. Это не значит, что информация в ТОО относительно тестирования проникновения является точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органа по подтверждению соответствия 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, которую обычно можно найти в соответствующем разделе ТОО, включает:

а) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые подвергались тестированию проникновения;

б) функции безопасности, которые подвергались тестированию проникновения. Краткий перечень функций безопасности, на которых было сосредоточено тестирование проникновения;

в) вердикт по данному подвиду деятельности. Общий вывод по результатам тестирования проникновения.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования проникновения выполненного оценщиком в процессе оценки, которую следует представить в ТОО.

11.6.3.3.5 Действие AVA_VLA.2.5E

AVA_VLA.2-15 Оценщик ***должен исследовать*** результаты всего тестирования проникновения и выводы по всему анализу уязвимости, чтобы сделать заключение, является ли ОО, находящийся в своей предопределенной среде, стойким к нарушителю, обладающему низким потенциалом нападения.

Если результаты показывают, что ОО, находящийся в своей предопределенной среде, имеет уязвимости, пригодные для использования нарушителем, обладающим меньшим, чем умеренный, потенциалом нападения, то по данному действию оценщиком делается отрицательное заключение.

AVA_VLA.2-16 Оценщик ***должен привести*** в ТОО информацию обо всех пригодных для использования уязвимостях и остаточных уязвимостях, детализируя для каждой:

а) ее источник (например, стала известна при выполнении действий ОМО, известна оценщицу, прочитана в публикации);

б) связанную с ней функцию (функции) безопасности, не достигнутую цель (цели), нарушенную политику (политики) безопасности организации, реализованную угрозу (угрозы);

в) описание;

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

д) идентификацию участника оценки (например, разработчик, оценщик), который ее идентифицировал.

12 Общие указания по оценке

12.1 Цели

Цель данного раздела 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.

12.2 Выборка

Данный подраздел содержит общие указания по осуществлению выборке. Конкретная и подробная информация дана в тех шагах оценивания, соответствующих определенным элементам действии оценщика, где выборку необходимо выполнить.

Выборка - определенная процедура, выполняемая оценщиком, посредством которой некоторое подмножество требуемой совокупности свидетельств оценки исследуется и

полагается 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:

а) На подмножестве не обнаружено никаких ошибок, что дает оценщику определенную уверенность в том, что совокупность в целом корректна;

б) 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.

В ОК определены следующие элементы действии оценщика, для которых заведомо применима выборка:

а) ADV_RCR.3.2E: "Оценщик должен сделать независимое заключение о правильности доказательств соответствия, избирательно верифицируя формальный анализ";

6) ATE_IND.*.2E: "Оценщик должен протестировать подмножество ФБО как необходимо, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями";

в) ATE_IND.2.3E: "Оценщик должен выполнить выборку тестов из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком";

г) AVA_CCA.*.3E: "Оценщик должен выборочно подтвердить правильность результатов анализа скрытых каналов, применяя тестирование";

д) AVA_MSU.2.2E и AVA_MSU.3.2E: "Оценщик должен повторить все процедуры конфигурирования и установки и выборочно другие процедуры для подтверждения, что ОО можно безопасно конфигурировать и использовать, применяя только представленные руководства".

е) AMA_SIA.1.2E: "Оценщик должен выборочно проверить, что при анализе влияния на безопасность изменения задокументированы на приемлемом уровне детализации вместе с соответствующим строгим обоснованием поддержки доверил в текущей версии ОО".

Кроме того, в ADV_IMP.1.1D требуется, чтобы разработчик обеспечил представление реализации только для подмножества ФБО. Выборку подмножества ему следует согласовать с оценщиком. Предоставление разработчиком выборки представления реализации позволяет оценщику, как оценить само предоставленное представление реализации, так и выборочно проверить свидетельство прослеживания требований безопасности в представлениях проекта ОО, чтобы получить уверенность в соответствии между проектом нижнего уровня и представлением реализации.

В дополнение к выборке, предусмотренной в ОК, МО определяет следующие действия, для которых выборка применима:

а) Действие ACM_CAP.*.1E: "Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств".

Здесь выборка применяется для элементов содержания и представления свидетельств ACM_CAP.3.8C и ACM_CAP.3.9C.

6) Действие ATE_FUN.1.1.E: "Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств".

Здесь выборка применяется для элементов содержания и представления свидетельств ATE_FUN_1.3C, ATE_FUN_1.4C, и ATE_FUN.1.5C.

в) Действие ALC_DVS.1.1E: "Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств".

Здесь выборка применяется для элементов содержания и представления свидетельств ALC_DVS.1.2C.

Выборка в случаях, указанных в ОК или специально оговоренных в шагах оценивания ОМО, признается как рентабельный 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 око 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 ОК, который обычно весь требуется проверить или исследовать, и когда не ожидается, что такое действие повысит соответственно степень доверия.

Выборка нуждается в строгом обосновании, принимая во внимание возможное влияние на цепи 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, правильно ли выполнялся процесс. Во многих случаях, когда от оценщика требуется определить, что процесс действительно выполняется, рекомендуется стратегия выборки. Подход здесь отличается от того, который применяется при выборке результатов тестирования разработчиком. 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 приходится анализировать в случаях связанных с правильной реализацией ОО, нежели с необходимостью удостовериться, что процесс выполняется. При выборке рекомендуется всегда придерживаться следующих принципов:

а) Объем выборки следует сопоставить с рентабельностью оценки, он зависит от некоторых характеристик ОО (например, от размеров и сложности ОО, от объема документации), но минимальный объем в 20% следует принять за норму для выборки из материалов, относящихся к реализации ОО. Там, где выборка осуществляется для получения свидетельства выполнения некоторого процесса (например, контроля посетителей или анализа проекта), задание определенного процента не применяется. Оценщику следует выбрать объем информации, достаточный для получения приемлемой уверенности в выполнении процесса и строго обосновать объем выборки;

б) Следует, чтобы выборка 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);

в) 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;

г) 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 спорадические. Если ошибка систематическая, следует устранить ее причину и полностью выполнить новую выборку. При надлежащем объяснении разработчика вопрос о спорадических ошибках может быть решен без необходимости новой выборки, хотя такое объяснение следует подтвердить. Оценщику следует руководствоваться здравым смыслом при определении, увеличить ли объем выборки или использовать другую выборку.

12.3 Анализ непротиворечивости

В данном подразделе представлено общее руководство по анализу непротиворечивости. Конкретная и подробная информация дана в тех шагах оценивания, соответствующих определенным элементам действий оценщика, где анализ непротиворечивости необходимо выполнить.

Анализ непротиворечивости - определенная процедура, выполняемая оценщиком, посредством которой выбранная часть одной из поставок для оценки анализируется автономно (на внутреннюю непротиворечивость) или сравнивается с одной или несколькими другими поставками для оценки.

В ОК различаются несколько типов анализа непротиворечивости.

а) Оценщику необходимо проанализировать внутреннюю непротиворечивость поставки для оценки.

Примеры

- ADV_FSP.1.2C: "Функциональная спецификация должна быть внутренне непротиворечивой".

- ADV_HLD.1.2C: "Проект верхнего уровня должен быть внутренне непротиворечивым".

- ADV_IMP.1.2C: "Представление реализации должно быть внутренне непротиворечивым".

- ADV_LLD.1.2C: "Проект нижнего уровня должен быть внутренне непротиворечивым".

При выполнении анализа внутренней непротиворечивости оценщику необходимо удостовериться, что представленная поставка не содержит неоднозначности. Поставка для оценки не должна содержать противоречащие формулировки в различных своих составляющих. Например, неформальные, полуформальные или формальные представления одного и того же свидетельства следует согласовать между собой.

Оценщику следует учесть, что составляющие поставки для оценки могут быть представлены в нескольких документах (например, процедуры безопасной установки, генерации и запуска могут быть описаны в трех различных документах).

б) Оценщику необходимо проанализировать, согласована ли поставка для оценки с одной или несколькими другими поставками.

Примеры

- ***AGD_ADM.1.7C: ''Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки".***
- ***AGD_USR.1.5C: ''Руководство пользователя должно быть согласовано со всей другой документацией, представленной для оценки".***

При анализе непротиворечивости от оценщика требуется верифицировать согласованность описания функций, параметров безопасности, процедур и событий, относящихся к безопасности, в одном документе с их описанием в других документах, представленных для оценки. Это означает, что оценщику следует учесть возможные противоречия с другими источниками информации. Примерами являются:

– противоречия с другими указаниями по использованию функции безопасности;

– противоречия с ЗБ (например, в части угроз, предположений безопасного использования, не-ИТ-целей безопасности или функций безопасности ИТ);

– применение параметров безопасности, противоречащее их описанию в функциональной спецификации или в проекте нижнего уровня;

– описание событий, относящихся к безопасности, противоречащее информации, содержащейся в проектах верхнего или нижнего уровня;

– несоответствие функций, осуществляющих безопасность, неформальной модели ПБО.

в) Оценщику необходимо проанализировать и то, что поставка для оценки внутренне непротиворечива, и то, что поставка для оценки согласована с другими поставками.

Пример - AVA_MSU.1.2C: "Руководства должны быть полны, понятны, непротиворечивы и обоснованы".

Здесь требуется, чтобы руководство в целом удовлетворяло требованию непротиворечивости. Учитывая, что руководство может содержаться в одном документе или же в нескольких отдельных документах, требование относится к непротиворечивости всего руководства, как в пределах отдельных документов, так и между ними.

г) Оценщику необходимо проверить результата: анализа, представленные разработчиком и требуемые для демонстрации непротиворечивости.

Примеры

- ***ADV_SPM.1.3C: ''Модель ПБО должна включать в себя обоснование, которое демонстрирует, что она согласована и полна относительно всех политик безопасности организации, которые могут быть смоделированы".***
- ***ADV_SPM.1.4C: "Демонстрация соответствия между моделью ПБО и функциональной спецификацией должка показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели ПБО".***

В указанных случаях свидетельство непротиворечивости представляется разработчиком. Тем не менее, оценщику необходимо уяснить этот анализ и подтвердить его, возможно, даже выполнив, при необходимости, независимый анализ.

Анализ непротиворечивости может быть выполнен посредством исследования поставки (поставок) для оценки. Оценщику следует принять разумный и структурированный подход к анализу непротиворечивости документов и, возможно, объединить его с другими видами деятельности типа отображения или прослеживания, которые выполняются как часть других шагов оценивания. Оценщик может разрешить любые найденные противоречия, обращаясь к формальному описанию при его наличии. Аналогично, для уменьшения неоднозначности в поставках возможно использование полуформальной нотации, пусть и не столь точной, как формальная нотация.

Неоднозначность может возникать явно, например, из-за противоречивых формулировок, или неявно, когда формулировки недостаточно точны. Следует отметить, что пространная формулировка не является, сама по себе, достаточным основанием для принятия отрицательного заключения по критерию непротиворечивости.

Проверка непротиворечивости поставок для оценки может выявить упущения, из-за которых может потребоваться повторное выполнение завершенных ранее шагов оценивания. Например, проверка непротиворечивости целей безопасности может выявить пропуск одного или нескольких требований безопасности. В этом случае оценщику следует проверить соответствие между целями безопасности и ФБО.

12.4 Зависимости

В общем случае выполнение требуемых видов и подвидов деятельности и действии 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.

12.4.1 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 обеспечивает 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.

12.4.2 Зависимости между подвидами деятельности

Оценщику необходимо учитывать зависимости между компонентами, указанные в части 3 ОК. Пример такого вида зависимости - AVA_VLA.1. В этом компоненте заявлены зависимости от ADV_FSP.1, ADV_HLD.1, AGD_ADM.1 и AGD_USR.1.

Обычно положительное заключение по подвиду деятельности можно принять только при успешном завершении всех тех подвидов деятельности, от которых зависит данный подвид деятельности. Например, как правило, положительное заключение по AVA_VLA.1 может быть принято, если только по подвидам деятельности, относящимся к ADV_FSP.1, ADV_HLD.1, AGD_ADM.1 и AGD_USR.1, также принято положительное заключение.

Поэтому при определении 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, положительное заключение по зависимому подвиду деятельности может оказаться невозможным до устранения всех недостатков, относящихся к подвиду деятельности, от которого он зависит.

12.4.3 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 к представления свидетельств.

12.5 Посещение объектов

В данном подразделе представлено общее руководство по посещению объектов. Конкретная и подробная информация дана в шагах оценивания тех подвидов деятельности, где предусмотрены такие посещения:

а) ACM_AUT;

б) ACM_CAP.n (при n>2);

в) ADO_DEL;

г) ALC_DVS.

Посещение объектов разработки - полезный способ определения оценщиком, выполняются ли процедуры способом, не противоречащим своему описанию в документации.

Объекты посещаются для того, чтобы ознакомиться с:

а) использованием системы УК, как описано в плане УК;

б) практическим применением процедур поставки;

в) применением мер безопасности во время разработки.

Во время оценки часто необходимы несколько встреч оценщика с разработчиком, и одни 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, оценщику следует стремиться к получению более глубокого понимания анализируемых процедур на месте разработки, их практического использования и применения в соответствии с приставленными свидетельствами сценки. Такие интервью дополняют, но не заменяют исследование свидетельств оценки.

При подготовке к посещению объекта оценщику следует составить перечень проверок, основанный на представленных свидетельствах оценки. Результата посещения объекта следует зафиксировать в документальной форме.

Посещения объекта не обязательны, если например, место разработки недавно посещалось для другой оценки ОО или ранее было подтверждено следование определенным процедурам согласно стандарту ИСО 9000. Тогда следует рассмотреть иные подходы для получения уверенности, предоставляющие эквивалентный уровень доверия (например, проанализировать свидетельства оценки). Любое решение отменить посещение следует принимать после консультации с органом по подтверждению соответствия.

УДК 681.3 **МКС** 35.040

Ключевые слова: информационная технология, задание по безопасности, объект оценки, критерии оценки безопасности, оценка анализа уязвимостей, уровень стойкости, вмешательство.

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы, Есіл өзенінің жағалауы, № 35 көше, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074