ФСТЭК РОССИИ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Типовая методика оценки профилей защиты и заданий по безопасности

Введена в действие приказом
ФСТЭК России
от г. №

2005

Содержание

1 Область применения 4
2 Нормативные ссылки 5
3 Термины и определения 6
4 Сокращения 9
5 Процесс оценки и связанные с ним задачи 10
5.1 Введение 10
5.2 Вердикты оценщика 10
5.3 Задача получения исходных данных для оценки 11
5.3.1 Цели 11
5.3.2 Замечания по применению 11
5.3.3 Подзадача управления свидетельством оценки 11
5.4 Подвиды деятельности по оценке 12
5.5 Задача оформления результатов оценки 12
5.5.1 Цели 12
5.5.2 Управление выходными материалами оценки 12
5.5.3 Подзадача подготовки СП 13
5.5.4 Подзадача подготовки ТОО 13
6 Оценка профиля защиты 14
6.1 Введение 14
6.2 Цели 14
6.3 Организация оценки ПЗ 14
6.4 Вид деятельности «Оценка ПЗ» 15
6.4.1 Оценка раздела «Описание ОО» (APE_DES.1) 15
6.4.2 Оценка раздела «Среда безопасности ОО» (APE_ENV.1) 16
6.4.3 Оценка раздела «Введение ПЗ» (APE_INT.1) 19
6.4.4 Оценка целей безопасности (APE_OBJ.1) 21
6.4.5 Оценка раздела «Требования безопасности ИТ» (APE_REQ.1) 26
6.4.6 Оценка требований безопасности ИТ, сформулированных в явном виде (APE_SRE.1) 39
7 Оценка задания по безопасности 42
7.1 Введение 42
7.2 Цели 42
7.3 Организация оценки ЗБ 42
7.4 Вид деятельности «Оценка ЗБ» 44
7.4.1 Оценка раздела «Описание ОО» (ASE_DES.1) 44
7.4.2 Оценка раздела «Среда безопасности ОО» (ASE_ENV.1) 46
7.4.3 Оценка раздела «Введение ЗБ» (ASE_INT.1) 49
7.4.4 Оценка целей безопасности (ASE_OBJ.1) 51
7.4.5 Оценка раздела «Утверждение о соответствии ПЗ» (ASE_PPC.1) 56
7.4.6 Оценка раздела «Требования безопасности ИТ» (ASE_REQ.1) 57

7.4.7 Оценка требований безопасности ИТ, сформулированных в явном виде (ASE_SRE.1) 71
7.4.8 Оценка краткой спецификации ОО (ASE_TSS.1) 73
Приложение А Содержание технического отчета при оценке ПЗ 79

1 Область применения

1 Типовая методика оценки профилей защиты и заданий по безопасности (Методика) предназначена для субъектов системы сертификации средств защиты информации по требованиям безопасности информации – заявителей, испытательных центров (лабораторий) и органов по сертификации, для проверки соответствии ПЗ/ЗБ, представляемых на оценку, требованиям РД Гостехкомиссии России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Общие критерии).

2 Заявители могут использовать Методику в качестве источника информации о тех действиях и шагах, которые будут предприняты испытательным центром (лабораторией) при оценке ПЗ/ЗБ.

3 Испытательные центры (лаборатории) должны использовать Методику в качестве руководства по проведению оценки ПЗ/ЗБ.

4 Органы по сертификации должны использовать Методику в процессе выполнения независимой экспертизы результатов оценки ПЗ/ЗБ, выполненной испытательными центрами (лабораториями).

5 Результаты независимой экспертизы материалов оценки ПЗ используются органами по сертификации при принятии решения о выдаче или отказе в выдаче сертификата соответствия ПЗ требованиям РД «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий».

6 Результаты независимой экспертизы материалов оценки ЗБ совместно с результатами независимой экспертизы материалов оценки соответствующего изделия ИТ используются органами по сертификации при принятии решения о выдаче или отказе в выдаче сертификата соответствия изделия ИТ заданию по безопасности.

7 Настоящий документ разработан на основе Общей методология оценки безопасности информационных технологий версия 1.0 (CEM-99/045).

2 Нормативные ссылки

8 В настоящей Методике использованы ссылки на следующие нормативные документы.

ГОСТ Р ИСО/МЭК 15408—2002 Информационная технология. – Методы и средства обеспечения безопасности. – Критерии оценки безопасности информационных технологий. – Части 1, 2, 3.

Руководящий документ – Безопасность информационных технологий – Критерии оценки безопасности информационных технологий – Часть 1: Введение и общая модель, Гостехкомиссия России, 2002.

Руководящий документ – Безопасность информационных технологий – Критерии оценки безопасности информационных технологий – Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002.

Руководящий документ – Безопасность информационных технологий – Критерии оценки безопасности информационных технологий – Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002.

Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation Methodology, Version 1.0, August 1999.

3 Термины и определения

9 В настоящем документе применены следующие термины из Методологии оценки по Общим критериям с соответствующими определениями. Термины, используемые во всем тексте ОК, и их определения можно найти в Глоссарии части 1 ОК.

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

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

12 ***Задание по безопасности (Security Target):*** Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО.

13 ***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.

14 ***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.

15 ***Методология (Methodology):*** Система принципов, процедур и процессов, применяемых для оценки безопасности ИТ.

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

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

18 ***Поставка для оценки (Evaluation Deliverable):*** Любой ресурс, который оценщик или орган по сертификации требует от заявителя или разработчика

для выполнения одного или нескольких видов деятельности по проведению оценки или по надзору за оценкой.

19 ***Привести в отчете (сообщении) (Report):*** Включить результаты оценки и вспомогательные материалы в технический отчет об оценке (Evaluation Technical Report) или сообщение о проблеме (Observation Report).

20 ***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.

21 ***Профиль защиты (Protection Profile):*** Независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя.

22 ***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).

23 ***Свидетельство оценки (Evaluation Evidence):*** Фактическая поставка для оценки (Evaluation Deliverable).

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

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

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

27 Термин *"Вид деятельности" ("activity")* используется для описания применения класса доверия из части 3 ОК.

28 Термин *"Подвид деятельности" ("sub-activity")* используется для описания применения компонента доверия из части 3 ОК.

29 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.

30 Термин "Шаг оценивания" ("work unit") описывает далее неразделимый фрагмент работы по оценке. Каждое действие включает один или несколько шагов оценивания, которые объединены в пределах действия Методики

согласно содержанию ОК и представлению элемента содержания свидетельств или действий разработчика. Шаги оценивания представлены в Методике в том же порядке, что и элементы ОК, из которых они следуют. Шаги оценивания указаны с левой стороны условным обозначением типа APE_DES.1-2. В этом обозначении последовательность символов APE_DES.1 указывает на компонент ОК (т.е. на подвид деятельности), а завершающая цифра (2) указывает, что это второй шаг оценивания в подвиде деятельности APE_DES.1.

4 Сокращения

ЗБ	задание по безопасности
ИТ	информационные технологии
ОК	Общие критерии
ОМО	Общая методология оценки
ОО	объект оценки
ОУД	оценочный уровень доверия к безопасности
ПБО	политика безопасности объекта оценки
ПЗ	профиль защиты
РД	руководящий документ
СП	сообщение о проблеме
СФБ	стойкость функции безопасности
ФБО	функции безопасности объекта оценки
ТОО	технический отчет об оценке

5 Процесс оценки и связанные с ним задачи

5.1 Введение

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

32 Каждая оценка, как ПЗ, так и ОО (в том числе ЗБ), 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.

33 В этом разделе описаны задача получения исходных данных для оценки и задача оформления результатов оценки, которые связаны с управлением свидетельствами оценки и созданием отчетов и сообщений. Каждая задача объединяет подзадачи, применяемые для всех оценок по ОК (как ПЗ, так и ОО) и являющиеся для них нормативными.

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

35 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.

5.2 Вердикты оценщика

36 Оценщик выносит вердикт относительно выполнения требований ОК. Наименьшая структурная единица ОК, по которой выносится вердикт – элемент действий оценщика. Вердикт по выполняемому элементу действий оценщика из ОК выносится как результат выполнения соответствующего действия из Методики и составляющих его шагов оценивания. В итоге, результат оценки формируется в соответствии с подразделом 5.2 части 1 ОК.

37 В ОМО различаются три взаимоисключающих вида вердикта:

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

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

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

38 Общий вердикт *положительный* тогда и только тогда, когда все составляющие вердикта *положительны*.

5.3 Задача получения исходных данных для оценки

5.3.1 Цели

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

5.3.2 Замечания по применению

40 Ответственность за представление всех требуемых свидетельств оценки возлагается на заявителя.

41 При оценке ПЗ и ЗБ исходными данными в виде свидетельств оценки являются соответственно профиль защиты и задание по безопасности.

42 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.

5.3.3 Подзадача управления свидетельством оценки

5.3.3.1 Контроль конфигурации

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

44 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.

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

5.3.3.2 Дальнейшее использование

46 Система оценки может предусматривать продолжение распоряжения свидетельством оценки после завершения оценки. Это может достигаться посредством одного или нескольких следующих действий:

а) возврата;
б) архивирования;
в) уничтожения.

5.3.3.3 Конфиденциальность

47 Во время проведения оценки оценщик может получить доступ к конфиденциальной информации заявителя и разработчика. Система оценки может предъявить к оценщику требования по поддержке конфиденциальности свидетельств оценки. Заявитель и оценщик могут совместно согласовать и дополнительные требования, не противоречащие системе.

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

5.4 Подвиды деятельности по оценке

49 Подвиды деятельности по оценке варьируются в зависимости от того, оценивается ПЗ или ЗБ (ОО). Они отражены соответственно в разделах 6 и 7 настоящей Методики.

5.5 Задача оформления результатов оценки

5.5.1 Цели

50 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.

51 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 сертификации.

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

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

5.5.2 Управление выходными материалами оценки

53 Оценщик представляет органу по сертификации 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.

5.5.3 Подзадача подготовки СП

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

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

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

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

а) идентификатор оцениваемого ПЗ или ЗБ;

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.

58 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 сертификации и заявителю).

5.5.4 Подзадача подготовки ТОО

5.5.4.1 Цели

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

60 ТОО помогает органу по сертификации подтвердить проведение оценки согласно требуемому стандарту, но, как ожидается, документированные результаты могут не содержать всю необходимую информацию, так что может понадобиться дополнительная информация, требуемая системой оценки.

61 В приложении А приведено минимально необходимое содержание информации, включаемой в ТОО при оценке ПЗ.

6 Оценка профиля защиты

6.1 Введение

62 Этот раздел описывает оценку ПЗ. Требования и методика оценки ПЗ идентичны для каждой оценки ПЗ, независимо от ОУД (или другой совокупности критериев доверия), заявленного в ПЗ.

63 Методика оценки в этом разделе базируется на требованиях к ПЗ, определенных в части 1 ОК, в особенности в Приложении Б, и классе APE из части 3 ОК.

6.2 Цели

64 В ПЗ идентифицируются требования безопасности ИТ, которые направлены на реализацию установленной политики безопасности организации и противостояние сформулированным угрозам с учетом сделанных предположений.

65 Цель оценки ПЗ – сделать заключение, является ли ПЗ:

а) полным: требования безопасности противостоят каждой угрозе и реализуют каждую политику безопасности организации;
б) достаточным: требования безопасности ИТ являются приемлемыми для угроз и политик безопасности организации;
в) логичным: ПЗ должен быть внутренне непротиворечивым.

6.3 Организация оценки ПЗ

66 Деятельность по проведению полной оценки ПЗ охватывает следующее:

а) задачу получения исходных данных для оценки;
б) вид деятельности по оценке ПЗ, включающий следующие подвиды деятельности:
1) оценку раздела ПЗ «Описание ОО» (п. 6.4.1);
2) оценку раздела ПЗ «Среда безопасности ОО» (п. 6.4.2);
3) оценку раздела ПЗ «Введение ПЗ» (п. 6.4.3);
4) оценку раздела ПЗ «Цели безопасности» (п. 6.4.4);
5) оценку раздела ПЗ «Требования безопасности ИТ» (п. 6.4.5);
7) оценку сформулированных в явном виде требований безопасности ИТ (п. 6.4.6);
в) задачу оформления результатов оценки.

67 Подвиды деятельности по оценке определяются требованиями доверия класса APE, содержащимися в части 3 ОК.

68 В настоящем разделе описываются подвиды деятельности, включенные в оценку ПЗ. Хотя подвиды деятельности могут быть строго не упорядочены,

некоторые зависимости между подвидами деятельности должны быть учтены оценщиком.

69 Подвид деятельности по оценке сформулированных в явном виде требований безопасности ИТ выполняется только тогда, когда в состав требований безопасности ИТ включены требования безопасности, взятые не из частей 2 или 3 ОК.

70 Результаты оценки ПЗ оформляются в виде технического отчета по оценке, содержание которого приведено в приложении А.

6.4 Вид деятельности «Оценка ПЗ»

6.4.1 Оценка раздела «Описание ОО» (APE_DES.1)

6.4.1.1 Цели

71 Цель данного подвида деятельности – сделать заключение, содержит ли «Описание ОО» соответствующую для понимания назначения ОО и его функциональных возможностей информацию, а также сделать заключение, является ли описание ОО полным и непротиворечивым.

6.4.1.2 Исходные данные

72 Свидетельством оценки для этого подвида деятельности является ПЗ.

6.4.1.3 Действия оценщика

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

а) APE_DES.1.1E;
б) APE_DES.1.2E;
в) APE_DES.1.3E.

6.4.1.3.1 Действие APE_DES.1.1E

APE_DES.1.1C

APE_DES.1-1 Оценщик ***должен исследовать*** «Описание ОО», чтобы сделать заключение, описан ли в нем тип продукта или системы для ОО.

74 Оценщик делает заключение, достаточно ли «Описание ОО» для того, чтобы дать читателю общее понимание предполагаемого использования продукта или системы, и обеспечивает ли, таким образом, контекст оценки. Примерами некоторых типов продуктов и систем являются: межсетевой экран, смарт-карта, крипто-модем, web-сервер, интрасеть.

75 Существуют ситуации, когда является очевидным, что у ОО ожидается наличие некоторых функциональных возможностей, определяемых типом продукта или системы. Если эти функциональные возможности отсутствуют, то оценщик делает заключение, адекватно ли это отсутствие рассматривается в разделе «Описание ОО». Примером этого является ОО типа «межсетевой

экран», в «Описании ОО» которого изложено, что он не может быть подключен к сетям.

APE_DES.1-2 Оценщик ***должен исследовать*** «Описание ОО», чтобы сделать заключение, описаны ли в нем в общих чертах ИТ-характеристики ОО.

76 Оценщик делает заключение, рассмотрены ли в разделе «Описание ОО» ИТ-характеристики, и в особенности характеристики безопасности, предоставляемые ОО, на таком уровне детализации, который достаточен для общего понимания читателем этих характеристик.

6.4.1.3.2 Действие APE_DES.1.2E

APE_DES.1-3 Оценщик ***должен исследовать*** ПЗ, чтобы сделать заключение, является ли «Описание ОО» логически упорядоченным.

77 Изложение раздела «Описание ОО» является логически упорядоченным, если его текст и структура понятны целевой аудитории (то есть разработчикам, оценщикам и потребителям).

APE_DES.1-4 Оценщик ***должен исследовать*** ПЗ, чтобы сделать заключение, является ли «Описание ОО» внутренне непротиворечивым.

78 Оценщику следует помнить, что этот раздел ПЗ предназначен только для того, чтобы определить общее назначение ОО.

6.4.1.3.3 Действие APE_DES.1.3E

APE_DES.1-5 Оценщик ***должен исследовать*** ПЗ, чтобы сделать заключение, согласовано ли «Описание ОО» с другими частям ПЗ.

79 Оценщик делает заключение, в частности, что в разделе «Описание ОО» не описываются угрозы, характеристики безопасности или конфигурации ОО, которые не рассматриваются в каком-либо другом месте ПЗ.

6.4.2 Оценка раздела «Среда безопасности ОО» (APE_ENV.1)

6.4.2.1 Цели

80 Цель данного подвида деятельности – сделать заключение, обеспечивает ли изложение раздела «Среда безопасности ОО» в ПЗ четкое и непротиворечивое определение проблемы безопасности, решение которой возлагается на ОО и его среду.

6.4.2.2 Исходные данные

81 Свидетельством оценки для этого подвида деятельности является ПЗ.

6.4.2.3 Действия оценщика

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

а) APE_ENV.1.1E;
б) APE_ENV.1.2E.

6.4.2.3.1 Действие APE_ENV.1.1E

APE_ENV.1.1C

APE_ENV.1-1 Оценщик ***должен исследовать*** изложение раздела ПЗ «Среда безопасности ОО», чтобы сделать заключение, идентифицируются и разъясняются ли в нем какие-либо предположения.

83 Предположения могут быть разделены на предположения относительно предполагаемого использования ОО и предположения относительно среды использования ОО.

84 Оценщик делает заключение, учитывают ли предположения относительно предполагаемого использования ОО такие аспекты как предполагаемое применение ОО, потенциальная ценность активов, требующих защиты со стороны ОО, и возможные ограничения использования ОО.

85 Оценщик делает заключение, достаточно ли подробно разъяснено каждое предположение относительно предполагаемого использования ОО для того, чтобы предоставить возможность потребителям решить, соответствует ли предполагаемое использование ими ОО сделанным предположениям. Если предположения не являются понятными, то это может, в конечном счете, привести к тому, что потребители будут использовать ОО в среде, для которой он не предназначен.

86 Оценщик делает заключение, охватывают ли предположения относительно среды использования ОО аспекты физической среды, персонала и внешних связей:

а) Физические аспекты включают какие-либо предположения, которые необходимо сделать относительно физического расположения ОО или подключенных периферийных устройств для того, чтобы ОО функционировал безопасным образом. Несколько примеров:

1) предполагается, что консоли администраторов находятся в некоторой зоне, доступ в которую ограничен только персоналом, являющимся администраторами;

2) предполагается, что все средства хранения файлов для ОО находятся на той рабочей станции, на которой функционирует ОО.

б) Аспекты, имеющие отношение к персоналу, включают какие-либо предположения, которые необходимо сделать относительно пользователей и администраторов ОО или других лиц внутри среды ОО для того, чтобы ОО функционировал безопасным образом. Несколько примеров:

1) предполагается, что пользователи имеют конкретные навыки или специальные знания;

2) предполагается, что пользователи имеют определенную минимально необходимую форму допуска;

3) предполагается, что администраторы обновляют антивирусную базу данных ежемесячно.

в) Аспекты внешних связей включают предположения, которые необходимо сделать относительно связей между ОО и другими внешними по отношению к ОО системами или продуктами ИТ (аппаратными, программными и программно-аппаратными средствами или их комбинацией) для того, чтобы ОО функционировал безопасным образом. Несколько примеров:

1) предполагается, что для хранения файлов регистрации, генерируемых ОО, доступным является, по крайней мере, 100Мб внешнего дискового пространства;

2) предполагается, что ОО является единственным приложением, не относящимся к операционной системе, выполняемым на отдельной рабочей станции;

3) предполагается, что дисковод ОО для накопителей на ГМД отключен;

4) предполагается, что ОО не будет подключаться к недоверенной сети.

87 Оценщик делает заключение, достаточно ли подробно разъяснено каждое предположение относительно среды использования ОО для того, чтобы предоставить возможность потребителям решить, соответствует ли их предполагаемая среда сделанным предположениям о среде ОО. Если предположения не являются понятными, то это может, в конечном счете, привести к тому, что ОО будет использоваться в среде, в которой он не будет функционировать безопасным образом.

APE_ENV.1.2C

APE_ENV.1-2 Оценщик ***должен исследовать*** изложение раздела «Среда безопасности ОО», чтобы сделать заключение, идентифицируются и разъясняются ли в нем какие-либо угрозы.

88 Если цели безопасности для ОО и его среды получены только на основе предположений и политики безопасности организации, то изложение угроз в ПЗ не потребуется. В этом случае этот шаг оценивания не применяем и поэтому считается удовлетворенным.

89 Оценщик делает заключение, все ли идентифицированные угрозы ясно разъясняются в терминах идентифицированного источника угрозы, нападения и актива, являющегося объектом нападения.

90 Оценщик также делает заключение, характеризуются ли источники угроз (нарушители) через их компетентность, ресурсы и мотивацию, а нападения – через методы нападения, какие-либо используемые уязвимости и возможность нападения.

APE_ENV.1.3C

APE_ENV.1-3 Оценщик ***должен исследовать*** изложение раздела «Среда безопасности ОО», чтобы сделать заключение, идентифицируются и

разъясняются ли в нем какие-либо политики безопасности организации.

91 Если цели безопасности для ОО и его среды получены только на основе предположений и угроз, то нет необходимости в том, чтобы политика безопасности организации была представлена в ПЗ. В этом случае данный шаг оценивания не применяем и поэтому считается удовлетворенным.

92 Оценщик делает заключение, выполнено ли изложение политики безопасности организации в виде правил, практических приемов или руководств, установленных организацией, контролирующей среду, в которой предстоит использовать ОО, которым должны следовать ОО или его среда. Примером политики безопасности организации является требование генерации и шифрования паролей в соответствии со стандартом.

93 Оценщик делает заключение, достаточно ли подробно разъяснена и/или интерпретирована каждая политика безопасности организации для того, чтобы сделать ее ясной для понимания; ясное представление формулировок политик является необходимым для того, чтобы дать возможность проследить цели безопасности по отношению к ним.

6.4.2.3.2 Действие APE_ENV.1.2E

APE_ENV.1-4 Оценщик ***должен исследовать*** изложение раздела «Среда безопасности ОО», чтобы сделать заключение, является ли оно логически упорядоченным.

94 Изложение раздела «Среда безопасности ОО» является логически упорядоченным, если его текст и структура понятны целевой аудитории (то есть оценщикам и потребителям).

APE_ENV.1-5 Оценщик ***должен исследовать*** изложение раздела «Среда безопасности ОО», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

95 Примерами внутренне противоречивого изложения раздела «Среда безопасности ОО» являются:

96 изложение раздела «Среда безопасности ОО», которое содержит угрозу, метод нападения для которой – вне возможностей реализации источником угрозы;

97 изложение раздела «Среда безопасности ОО», которое содержит правило политики безопасности организации "ОО не должен подключаться к Интернет" и угрозу, источником которой является злоумышленник из Интернет.

6.4.3 Оценка раздела «Введение ПЗ» (APE_INT.1)

6.4.3.1 Цели

98 Цель данного подвида деятельности – сделать заключение, является ли раздел «Введение ПЗ» полным и согласованным со всеми другими частями ПЗ, и правильно ли в нем идентифицируется ПЗ.

6.4.3.2 Исходные данные

99 Свидетельством оценки для этого подвида деятельности является ПЗ.

6.4.3.3 Действия оценщика

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

а) APE_INT.1.1E;
б) APE_INT.1.2E;
в) APE_INT.1.3E.

6.4.3.3.1 Действие APE_INT.1.1E

APE_INT.1.1C

APE_INT.1-1 Оценщик ***должен проверить***, представлена ли в разделе «Введение ПЗ» идентификационная информация, необходимая для идентификации, каталогизации, регистрации и перекрестной ссылки на ПЗ.

101 Оценщик делает заключение, включает ли идентификационная информация ПЗ:

а) информацию, необходимую для контроля и уникальной идентификации ПЗ (например, наименование ПЗ, номер версии, дату публикации, авторов, организацию-спонсора);
б) указание версии ОК, использованной при разработке ПЗ;
в) регистрационную информацию, если перед оценкой ПЗ был зарегистрирован;
г) перекрестные ссылки, если ПЗ сопоставляется с другим (другими) ПЗ;
д) дополнительную информацию, в соответствии с требованиями системы сертификации.

APE_INT.1.2C

APE_INT.1-2 Оценщик ***должен проверить***, представлена ли в разделе «Введение ПЗ» «Аннотация ПЗ» в повествовательной форме.

102 «Аннотация ПЗ» предназначена, чтобы предоставить краткое резюме содержания ПЗ (более детальное описание предоставляется в разделе «Описание ОО»), которое является достаточно подробным, чтобы дать возможность потенциальному пользователю ПЗ сделать заключение, представляет ли для него интерес данный ПЗ.

6.4.3.3.2 Действие APE_INT.1.2E

APE_INT.1-3 Оценщик ***должен исследовать*** «Введение ПЗ», чтобы сделать заключение, является ли оно логически упорядоченным.

103 «Введение ПЗ» является логически упорядоченным, если его текст и структура изложения понятны целевой аудитории (то есть разработчикам, оценщикам и потребителям).

APE_INT.1-4 Оценщик ***должен исследовать*** «Введение ПЗ», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

104 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.

105 В данном случае анализ внутренней непротиворечивости опирается на краткий обзор ПЗ, представляющий собой резюме содержания ПЗ.

6.4.3.3.3 Действие APE_INT.1.3E

APE_INT.1-5 Оценщик ***должен исследовать*** ПЗ, чтобы сделать заключение, согласовано ли «Введение ПЗ» с другими частями ПЗ.

106 Оценщик делает заключение, предоставляет ли «Аннотация ПЗ» точную общую характеристику ОО. В частности оценщик делает заключение, согласована ли «Аннотация ПЗ» с разделом «Описание ОО», и не излагается и не предполагается ли в нем наличие характеристик безопасности, которые выходят за рамки оценки.

107 Оценщик также делает заключение, согласовано ли «Утверждение о соответствии ОК» с другими частями ПЗ.

6.4.4 Оценка целей безопасности (APE_OBJ.1)

6.4.4.1 Цели

108 Цель данного подвида деятельности – сделать заключение, полностью ли и согласовано ли описаны цели безопасности, а также сделать заключение, направлены ли цели безопасности на противостояние идентифицированным угрозам, на достижение идентифицированной политики безопасности организации, и согласованы ли они с изложенными предположениями.

6.4.4.2 Исходные данные

109 Свидетельством оценки для этого подвида деятельности является ПЗ.

6.4.4.3 Действия оценщика

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

а) APE_OBJ.1.1E;
б) APE_OBJ.1.2E.

6.4.4.3.1 Действие APE_OBJ.1.1E

APE_OBJ.1.1C

APE_OBJ.1-1 Оценщик ***должен проверить***, определены ли в изложении целей безопасности цели безопасности для ОО и его среды.

111 Оценщик делает заключение, ясно ли определено для каждой цели безопасности, относится она к ОО, к среде или к тому и другому.

APE_OBJ.1.2C

APE_OBJ.1-2 Оценщик ***должен исследовать*** «Обоснование целей безопасности», чтобы сделать заключение, все ли цели безопасности для ОО прослеживаются к аспектам идентифицированных угроз, которым необходимо противостоять, и/или к аспектам политики безопасности организации, которой должен следовать ОО.

112 Оценщик делает заключение, прослеживается ли каждая цель безопасности для ОО, по крайней мере, к одной угрозе или правилу политики безопасности организации.

113 Неудача при попытке такого прослеживания свидетельствует о том, что, либо обоснование целей безопасности является неполным, либо изложение угроз/политики безопасности организации является неполным, либо цель безопасности для ОО является бесполезной.

APE_OBJ.1.3C

APE_OBJ.1-3 Оценщик ***должен исследовать*** «Обоснование целей безопасности», чтобы сделать заключение, прослежены ли цели безопасности для среды к идентифицированным угрозам, которым должна противостоять среда ОО, и/или к аспектам политики безопасности организации, которым должна удовлетворять среда ОО, и/или к предположениям, которым должна удовлетворять среда ОО.

114 Оценщик делает заключение, прослеживается ли каждая цель безопасности для среды, по крайней мере, к одному предположению, угрозе или правилу политики безопасности организации.

115 Неудача при попытке такого прослеживания свидетельствует о том, что, либо обоснование целей безопасности является неполным, либо изложение предположений/угроз/политики безопасности организации является неполным, либо цель безопасности для среды является бесполезной.

APE_OBJ.1.4C

APE_OBJ.1-4 Оценщик ***должен исследовать*** «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждой угрозы приемлемое строгое обоснование того, что цели безопасности пригодны для противостояния данной угрозе.

116 Если ни одна цель безопасности не прослежена к конкретной угрозе, то результат данного шага оценивания – «неудовлетворительно».

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

118 Оценщик также делает заключение, действительно ли каждая цель безопасности, которая прослежена к угрозе, будучи достигнутой, вносит вклад в устранение, снижение или компенсацию последствий реализации данной угрозы.

119 Примеры устранения угрозы:

- устранение для источника угрозы (нарушителя) возможности использовать какой-либо метод нападения;
- устранение мотивации источника угрозы (нарушителя) путем применения сдерживающих факторов;
- устранение источника угрозы (например, отключение от сети машин, часто приводящих к фатальному сбою этой сети).

120 Примеры снижения угрозы:

- ограничение для источника угрозы возможности использования методов нападения;
- ограничение возможностей источников угрозы;
- снижение вероятности успешного результата инициированного нападения;
- повышенные требования к компетентности и ресурсам источника угрозы.

121 Примеры компенсации последствий реализации угрозы:

- частое создание резервных копий активов;
- наличие резервных копий ОО;
- частая смена ключей, используемых в течение сеанса связи, чтобы последствия компрометации одного ключа были относительно незначительными.

122 Обратите внимание, что прослеживание целей безопасности к угрозам в обосновании целей безопасности может быть частью строгого обоснования, но само по себе оно не является строгим обоснованием. Даже в том случае, когда цель безопасности является просто заявлением, отражающим намерение предотвратить реализацию конкретной угрозы, то все равно требуется строгое обоснование, хотя в этом случае оно может быть минимальным.

APE_OBJ.1.5C

APE_OBJ.1-5 Оценщик ***должен исследовать*** «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждого аспекта политики безопасности организации приемлемое строгое обоснование того, что цели безопасности пригодны для покрытия данного аспекта политики безопасности организации.

123 Если ни одна цель безопасности не прослежена к политике безопасности организации, то результат данного шага оценивания – «неудовлетворительно».

124 Оценщик делает заключение, демонстрирует ли строгое обоснование для политики безопасности организации то, что, если все цели безопасности, прослеженные к политике безопасности организации, достигнуты, то политика безопасности организации реализована.

125 Оценщик также делает заключение, действительно ли каждая цель безопасности, которая прослежена к политике безопасности организации, будучи достигнутой, вносит вклад в реализацию политики безопасности организации.

126 Обратите внимание, что прослеживание целей безопасности к политике безопасности организации в обосновании целей безопасности может быть частью строгого обоснования, но само по себе оно не является строгим обоснованием. Даже в том случае, когда цель безопасности является просто заявлением, отражающим намерение реализовать конкретную политику безопасности, то все равно требуется строгое обоснование, хотя в этом случае оно может быть минимальным.

APE_OBJ.1-6 Оценщик ***должен исследовать*** «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждого предположения приемлемое строгое обоснование того, что цели безопасности для среды пригодны для покрытия данного предположения.

127 Если ни одна цель безопасности для среды не прослежена к изложенному предположению, то результат данного шага оценивания – «неудовлетворительно».

128 Предположение является или предположением относительно предполагаемого использования ОО, или предположением относительно среды использования ОО.

129 Оценщик делает заключение, демонстрирует ли строгое обоснование для предположения относительно предполагаемого использования ОО то, что, если все цели безопасности для среды, прослеженные к данному предположению, достигнуты, то предполагаемое использование ОО поддерживается.

130 Оценщик также делает заключение, действительно ли каждая цель безопасности для среды, прослеживаемая к некоторому предположению относительно предполагаемого использования ОО, будучи достигнутой, вносит вклад в поддержку предполагаемого использования.

131 Оценщик делает заключение, демонстрирует ли строгое обоснование для предположения относительно среды использования ОО то, что, если все цели безопасности для среды, прослеженные к данному предположению, достигнуты, то среда согласуется с данным предположением.

132 Оценщик также делает заключение, действительно ли каждая цель безопасности для среды, которая прослежена к предположению относительно среды использования ОО, будучи достигнутой, вносит вклад в достижение согласованности среды с предположением.

133 Обратите внимание, что прослеживание целей безопасности для среды к предположениям относительно среды использования ОО в подразделе «Обоснование целей безопасности» может быть частью строгого обоснования, но само по себе оно не является строгим обоснованием. Даже в том случае, когда цель безопасности представляет собой просто перефразированное предположение, то все равно требуется строгое обоснование, хотя в этом случае оно может быть минимальным.

6.4.4.3.2 Действие APE_OBJ.1.2E

APE_OBJ.1-7 Оценщик ***должен исследовать*** изложение раздела «Цели безопасности», чтобы сделать заключение, является ли оно логически упорядоченным.

134 Изложение раздела «Цели безопасности» является логически упорядоченным, если его текст и структура понятны целевой аудитории (то есть оценщикам и потребителям).

APE_OBJ.1-8 Оценщик ***должен исследовать*** изложение раздела «Цели безопасности», чтобы сделать заключение, является ли оно полным.

135 Изложение раздела «Цели безопасности» является полным, если цели безопасности достаточны для противостояния всем идентифицированным угрозам и покрывают все идентифицированные политики безопасности организации и предположения. Данный шаг оценивания может выполняться совместно с шагами оценивания APE_OBJ.1-4, APE_OBJ.1-5 и APE_OBJ.1-6.

APE_OBJ.1-9 Оценщик ***должен исследовать*** изложение раздела «Цели безопасности», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

136 Изложение раздела «Цели безопасности» является внутренне непротиворечивым, если цели безопасности не противоречат друг другу. Примером противоречия могут служить следующие две цели безопасности:

"Идентификатор пользователя не подлежит раскрытию" и "Идентификатор пользователя должен быть доступен другим пользователям".

6.4.5 Оценка раздела «Требования безопасности ИТ» (APE_REQ.1)

6.4.5.1 Цели

137 Цель данного подвида деятельности – сделать заключение, является ли описание требований безопасности ОО (как функциональных требований безопасности ОО, так и требований доверия к безопасности ОО) и требований безопасности для среды ИТ полным и непротиворечивым, и обеспечивают ли данные требования безопасности адекватную основу для разработки ОО, который бы достигал своих целей безопасности.

6.4.5.2 Исходные данные

138 Свидетельством оценки для этого подвида деятельности является ПЗ.

6.4.5.3 Действия оценщика

139 Действия оценщика включают два элемента из части 3 ОК:

а) APE_REQ.1.1E;

б) APE_REQ.1.2E.

6.4.5.3.1 Действие APE_REQ.1.1E

APE_REQ.1.1C

APE_REQ.1-1 Оценщик ***должен проверить*** изложение функциональных требований безопасности ОО, чтобы сделать заключение, идентифицированы ли в нем функциональные требования безопасности ОО, составленные из компонентов функциональных требований из части 2 ОК.

140 Оценщик делает заключение, что все компоненты функциональных требований безопасности ОО, взятые из части 2 ОК, идентифицированы либо путем ссылки на отдельные компоненты из части 2, либо путем воспроизведения их в ПЗ.

APE_REQ.1-2 Оценщик ***должен проверить***, что каждая ссылка на компонент функциональных требований безопасности ОО является правильной.

141 Для каждой ссылки на компонент функционального требования безопасности ОО из части 2 ОК оценщик делает заключение, существует ли упомянутый компонент в части 2 ОК.

APE_REQ.1-3 Оценщик ***должен проверить***, что каждый компонент функциональных требований безопасности ОО, взятый из части 2 ОК и воспроизведенный в ПЗ, воспроизведен правильно.

142 Оценщик делает заключение, правильно ли воспроизведены требования в подразделе ПЗ «Функциональные требования безопасности ОО»; при этом исследование разрешенных операций не проводится. Исследование правильности операций над компонентами осуществляется при выполнении шага оценивания APE_REQ.1-11.

APE_REQ.1.2C

APE_REQ.1-4 Оценщик ***должен проверить*** изложение подраздела ПЗ «Требования доверия к безопасности ОО», чтобы сделать заключение, идентифицированы ли в нем требования доверия к безопасности ОО, составленные из компонентов требований доверия из части 3 ОК.

143 Оценщик делает заключение, все ли компоненты требований доверия к безопасности ОО, взятые из части 3 ОК, идентифицированы либо путем ссылки на некоторый ОУД, либо на отдельные компоненты из части 3, либо путем их воспроизведения в ПЗ.

APE_REQ.1-5 Оценщик ***должен проверить***, что каждая ссылка на компоненты требований доверия к безопасности ОО является правильной.

144 Для каждой ссылки на компонент требований доверия к безопасности ОО из части 3 ОК оценщик делает заключение, существует ли упомянутый компонент в части 3 ОК.

APE_REQ.1-6 Оценщик ***должен проверить***, что каждый компонент требований доверия к безопасности ОО, взятый из части 3 ОК и воспроизведенный в ПЗ, воспроизведен правильно.

145 Оценщик делает заключение, правильно ли воспроизведены требования в подразделе ПЗ «Требования доверия к безопасности ОО»; при этом исследование выполнения разрешенных операций не проводится. Исследование правильности операций над компонентами осуществляется при выполнении шага оценивания APE_REQ.1-11.

APE_REQ.1.3C

APE_REQ.1-7 Оценщик ***должен исследовать*** изложение подраздела «Требования доверия к безопасности ОО», чтобы сделать заключение, включает ли оно ОУД, определенный в части 3 ОК, либо в нем соответствующим образом строго обосновывается, что оно не включает ОУД.

146 Если никакой из ОУД не включен, то оценщик делает заключение, указана ли в строгом обосновании причина невключения ОУД в подраздел «Требования доверия к безопасности ОО». Это строгое обоснование может указывать либо на причину невозможности, нежелательности или нецелесообразности включения ОУД в ПЗ, либо на причину невозможности, нежелательности или нецелесообразности включения конкретных компонентов семейств, составляющих ОУД1 (ACM_CAP, ADO_IGS, ADV_FSP, ADV_RCR, AGD_ADM, AGD_USR и ATE_IND).

APE_REQ.1.4C

APE_REQ.1-8 Оценщик ***должен исследовать*** «Обоснование требований безопасности», чтобы сделать заключение, достаточно ли строго в нем обосновывается то, что изложение требований доверия к безопасности ОО является приемлемым.

147 Если требования доверия содержат какой-либо ОУД, то в строгом обосновании допустимо рассматривать выбор конкретного ОУД в целом, а не каждого отдельного компонента данного ОУД. Если подраздел «Требования доверия к безопасности ОО» содержит компоненты, усиливающие выбранный ОУД, оценщик делает заключение, дано ли строгое обоснование каждого такого усиления. Если подраздел «Требования доверия к безопасности ОО» содержит требования доверия, сформулированные в явном виде, оценщик делает заключение, дано ли строгое обоснование использования каждого сформулированного в явном виде требования доверия.

148 Оценщик делает заключение, дано ли в подразделе «Обоснование требований безопасности» достаточно строгое обоснование, что требования доверия достаточны для изложенной среды безопасности и целей безопасности. Например, если требуется защита от хорошо осведомленных нарушителей, то было бы неприемлемым специфицировать компонент AVA_VLA.1, который является несвойственным для обнаружения недостатков безопасности, кроме очевидных.

149 Строгое обоснование может также включать основания, подобные следующим:

а) специфические требования, установленные конкретной системой оценки, правительством или другими организациями;

б) требования доверия, которые содержались в зависимостях функциональных требований безопасности ОО;

в) требования доверия систем и/или продуктов, предназначенных для совместного использования с ОО;

г) требования потребителей.

150 Краткий обзор назначения и целей для каждого ОУД приведен в подразделе 6.2 части 3 ОК.

151 Оценщику следует помнить, что заключение о том, являются ли требования доверия приемлемыми, может быть субъективным, а значит, анализ достаточности строгого обоснования не следует проводить чрезмерно тщательно.

152 Если подраздел «Требования доверия к безопасности ОО» не содержит какой-либо ОУД, то данный шаг оценивания может быть выполнен совместно с шагом оценивания APE_REQ.1-7.

APE_REQ.1.5C

APE_REQ.1-9 Оценщик ***должен проверить***, что в ПЗ, при необходимости, идентифицированы требования безопасности для среды ИТ.

153 Если ПЗ не содержит требований безопасности для среды ИТ, то данный шаг оценивания не применяем и поэтому считается удовлетворенным.

154 Оценщик делает заключение, все ли зависимости ОО от других ИТ в рамках его среды, направленные на обеспечение каких-либо функциональных возможностей безопасности с тем, чтобы достичь целей безопасности для ОО, четко идентифицированы в ПЗ как требования безопасности для среды ИТ.

155 Пример требований безопасности для среды ИТ – межсетевой экран полагается на базовую операционную систему в части обеспечения аутентификации администраторов и долговременного хранения данных аудита. В этом случае требования безопасности для среды ИТ обычно содержат компоненты из классов FAU и FIA.

156 Отметим, что «Требования безопасности для среды ИТ» могут содержать как функциональные требования, так и требования доверия.

157 Пример зависимости от среды ИТ: программный крипто-модуль, который периодически проверяет свой код и, в случае обнаружения несанкционированной модификации, самоотключается. Чтобы дать возможность восстановления, предусмотрено требование FPT_RCV.2 (автоматическое восстановление). Поскольку крипто-модуль не может самостоятельно восстановить свой код после самоотключения, то требование по восстановлению становится требованием к среде ИТ. Одной из зависимостей компонента FPT_RCV.2 является компонент AGD_ADM.1 (руководство администратора). Следовательно, это требование доверия становится требованием доверия для среды ИТ.

158 Оценщику следует помнить, что ссылка требований безопасности для среды ИТ на ФБО относится к функциям безопасности среды, а не к функциям безопасности ОО.

APE_REQ.1.6C

APE_REQ.1-10 Оценщик ***должен проверить***, что все завершенные операции над требованиями безопасности ИТ идентифицированы.

159 Допустимо, чтобы ПЗ содержал элементы с незавершенными операциями. То есть, ПЗ может содержать формулировки функциональных требований безопасности, которые включают незавершенные операции «назначение» или «выбор». Данные операции должны быть впоследствии завершены в ЗБ, отображающем этот ПЗ. Это дает разработчику ЗБ большую гибкость при разработке ОО и соответствующего ЗБ, в котором утверждается о соответствии конкретному ПЗ.

160 Разрешенными операциями для функциональных компонентов из части 2 ОК являются «назначение», «итерация», «выбор» и «уточнение». Операции

«назначение» и «выбор» разрешены только в специально обозначенных местах компонента. Операции «итерация» и «уточнение» разрешены для всех функциональных компонентов.

161 Разрешенными операциями для компонентов доверия из части 3 ОК являются операции «итерация» и «уточнение».

162 Оценщик делает заключение, все ли операции идентифицированы в каждом компоненте, где они используются. Необходимо, чтобы завершенные и незавершенные операции были идентифицированы таким образом, чтобы они могли быть различимы, и было ясно, завершена ли конкретная операция или нет. Идентификация может быть осуществлена либо путем введения типографских различий, либо путем использования явной идентификации в сопроводительном тексте, либо любым другим способом.

APE_REQ.1-11 Оценщик ***должен исследовать*** изложение раздела ПЗ «Требования безопасности ИТ», чтобы сделать заключение, корректно ли выполнены операции.

163 Оценщику следует помнить, что операции над требованиями безопасности необязательно должны быть выполнены и завершены в ПЗ.

164 Оценщик сравнивает каждую формулировку требований в ПЗ с элементом, из которого она получена, чтобы сделать заключение:

а) для операции «назначение» – выбраны ли значения параметров или переменных в соответствии с указанным типом, требуемым операцией «назначение»;

б) для операции «выбор» – принадлежит ли выбранный пункт или пункты множеству пунктов, указанных во фрагменте «выбор» данного элемента. Оценщик также делает заключение, приемлемо ли число выбранных пунктов для данного требования. Для некоторых требований требуется выбор только одного пункта (например, FAU_GEN.1.1.b), в других случаях приемлем выбор нескольких пунктов (например, вторая операция в FDP_ITT.1.1).

в) для операции «уточнение» – уточнен ли компонент таким образом, что ОО, удовлетворяющий уточненному требованию, также удовлетворяет и не уточненному требованию. Если уточненное требование выходит за эти рамки, то оно считается расширенным требованием.

Пример: ADV_SPM.1.2C – Модель ПБО должна содержать описание правил и характеристик всех политик безопасности организации, которые могут быть смоделированы.

Уточнение: Модель ПБО должна охватывать только управление доступом.

Если политика управления доступом является единственной политикой ПБО, то такое уточнение является правомерным. Если в ПБО также имеются политики идентификации и аутентификации, а уточнение означает сформулировать, что моделировать следует только контроль доступа, то это уточнение не является правомерным.

Особым случаем уточнения является редакционное уточнение, когда в требование вносятся небольшие изменения, а именно переформулирование предложения в соответствии с особенностями грамматики. Не допускается, чтобы такое изменение каким-либо образом изменяло смысл требования.

Пример редакционного уточнения – FAU_ARP.1 с единственным действием. Вместо записи: «ФБО должны предпринять *информировать оператора* при обнаружении возможного нарушения безопасности» допускается, чтобы разработчик ПЗ написал: «ФБО должны *информировать оператора* при обнаружении возможного нарушения безопасности».

Оценщику следует помнить, что редакционные уточнения должны быть четко идентифицированы (см. шаг оценивания APE_REQ.1-10).

г) для операции «итерация» – отличается ли каждая итерация компонента от каждой другой итерации этого компонента (по крайней мере, один элемент одной итерации компонента должен отличаться от соответствующего элемента другой итерации компонента), или что компонент применяется к разным частям ОО.

APE_REQ.1.7C

APE_REQ.1-12 Оценщик ***должен исследовать*** изложение раздела ПЗ «Требования безопасности ИТ», чтобы сделать заключение, идентифицированы ли все незавершенные операции над требованиями безопасности ИТ, включенными в ПЗ.

165 Оценщик делает заключение, все ли операции идентифицированы в каждом компоненте, где такая операция используется. Необходимо, чтобы завершенные и незавершенные операции были идентифицированы таким образом, чтобы они могли быть различимы, и было ясно, завершена ли операция или нет. Идентификация может быть осуществлена либо путем введения типографских различий, либо путем явной идентификации в сопроводительном тексте, либо любым другим способом.

APE_REQ.1.8C

APE_REQ.1-13 Оценщик ***должен исследовать*** изложение раздела ПЗ «Требования безопасности ИТ», чтобы сделать заключение, удовлетворены ли зависимости, требуемые компонентами, используемыми при изложении раздела ПЗ «Требования безопасности ИТ».

166 Зависимости могут быть удовлетворены включением соответствующего компонента (или компонента, иерархичного по отношению к последнему) в

подраздел ПЗ «Требования безопасности для ОО» или в подраздел «Требования безопасности для среды ИТ».

167 Хотя ОК способствуют проведению анализа зависимостей путем их включения в описание компонентов требований, сам по себе этот факт не является строгим обоснованием того, что никакие другие зависимости не существуют. Приведем пример существования таких зависимостей: элемент, в который включена ссылка «все объекты» или «все субъекты», может иметь зависимость по отношению к уточнению в другом элементе или наборе элементов, в котором перечисляются данные объекты или субъекты.

168 Предполагается, что зависимости требований безопасности для среды ИТ излагаются и удовлетворяются в ПЗ.

169 Оценщику следует помнить, что в ОК не требуется, чтобы все зависимости были удовлетворены: см. следующий шаг оценивания.

APE_REQ.1.9C

APE_REQ.1-14 Оценщик ***должен исследовать*** «Обоснование требований безопасности», чтобы сделать заключение, содержится ли в нем приемлемое строгое обоснование для каждого случая, когда зависимости требований безопасности не удовлетворены.

170 Оценщик с учетом идентифицированных целей безопасности делает заключение, объясняется ли в строгом обосновании, почему удовлетворение зависимости не требуется.

171 Оценщик подтверждает, что никакое неудовлетворение зависимости не препятствует тому, чтобы набор требований безопасности адекватно учитывал цели безопасности. Такой анализ проводится в соответствии с APE_REQ.1.13C.

172 Пример приемлемого строгого обоснования. Для программного ОО имеется цель безопасности следующего содержания – "случаи неуспешной аутентификации должны быть зарегистрированы с указанием идентификационной информации о пользователе, времени и дате", и для удовлетворения данной цели безопасности используется функциональное требование на основе компонента FAU_GEN.1 (генерация данных аудита). Компонент FAU_GEN.1 содержит зависимость от компонента FPT_STM.1 (надежные метки времени). Так как ОО не имеет встроенных часов, то FPT_STM.1 определяется разработчиком ПЗ как требование безопасности для среды ИТ. Разработчик ПЗ указывает на то, что данное требование не подлежит удовлетворению, приводя следующее строгое обоснование: "в данной конкретной среде существуют возможности проведения атак на механизм меток времени; таким образом, среда может не обеспечить надежные метки времени. Но имеющиеся источники угроз неспособны к проведению атак на механизмы меток времени, а другие атаки со стороны

этих источников угроз могут быть подвергнуты анализу с регистрацией времени и даты осуществления".

APE_REQ.1.10C

APE_REQ.1-15 Оценщик ***должен проверить***, включено ли в ПЗ заявление минимального уровня стойкости функции безопасности для функциональных требований безопасности ОО, и определен ли этот уровень СФБ как базовый, средний или высокий.

173 Если требования доверия к безопасности ОО не включают компонент AVA_SOF.1, то данный шаг оценивания не применяем и поэтому считается удовлетворенным.

174 Стойкость криптографических алгоритмов находится вне области действия ОК. Стойкость функции безопасности применяется только к вероятностным и перестановочным механизмам, которые являются некриптографическими. Следовательно, когда в ПЗ содержится утверждение о минимальном уровне СФБ, оно не применимо к каким бы то ни было криптографическим механизмам, с точки зрения оценки по ОК. Когда такие криптографические механизмы включены в ОО, то оценщик делает заключение, включено ли в ПЗ четкое изложение того, что оценка стойкости криптографических алгоритмов не является частью оценки по ОК.

175 ОО может состоять из нескольких отдельных доменов, тогда автор ПЗ может посчитать более приемлемым иметь минимальный уровень стойкости функций безопасности для каждого домена, а не иметь один общий минимальный уровень стойкости функций безопасности для всего ОО. В этом случае допускается разделить функциональные требования безопасности ОО на отдельные поднаборы и иметь различные минимальные уровни стойкости функций безопасности, ассоциированные с каждым поднабором.

176 Примером этого является распределенная терминальная система, включающая терминалы пользователей, расположенные в общедоступных местах, и терминалы администраторов, расположенные в физически защищенном месте. С требованиями по аутентификации для терминалов пользователей связана средняя СФБ, в то время как с требованиями по аутентификации для терминалов администраторов связана базовая СФБ. Вместо заявления о базовой СФБ как о минимальном уровне СФБ для ОО, что могло бы утвердить потенциальных потребителей ОО во мнении, что провести успешную атаку на механизмы аутентификации на терминалах пользователя относительно несложно, автор ПЗ разделяет ОО на два домена: домен пользователей и домен администраторов; разделяет функциональные требования безопасности ОО на два поднабора, соответствующие выделенным доменам ОО; назначает в качестве минимального уровня СФБ

базовую СФБ для поднабора требований, соответствующих домену администраторов, и среднюю СФБ для поднабора требований, соответствующих домену пользователей.

APE_REQ.1.11C

APE_REQ.1-16 Оценщик ***должен проверить***, что в ПЗ идентифицированы все конкретные функциональные требования безопасности ОО, для которых целесообразна заявленная в явном виде стойкость функции безопасности вместе с конкретной метрикой.

177 Если подраздел «Требования доверия к безопасности ОО» не содержит компонент AVA_SOF.1, то данный шаг оценивания не применяем и поэтому считается удовлетворенным.

178 Заявленной в явном виде стойкостью функции безопасности может быть «базовая СФБ», «средняя СФБ», «высокая СФБ» или заданная специфическая метрика. Когда используется специфическая метрика, оценщик делает заключение, является ли она приемлемой для конкретного типа функциональных требований, и имеется ли возможность оценки утверждений о СФБ, выраженных в данной метрике.

179 Дальнейшие указания по приемлемости и допустимости метрик стойкости функций безопасности могут быть представлены конкретной системой оценки.

APE_REQ.1.12C

APE_REQ.1-17 Оценщик ***должен исследовать*** «Обоснование требований безопасности», чтобы сделать заключение, демонстрирует ли оно согласованность минимального уровня стойкости функций, а также каждой заявленной в явном виде стойкости функции с целями безопасности для ОО.

180 Если в подраздел «Требования доверия к безопасности ОО» не включен компонент AVA_SOF.1, то данный шаг оценивания не применяем и поэтому считается удовлетворенным.

181 Оценщик делает заключение, учтены ли в подразделе ПЗ «Обоснование требований безопасности» детали, имеющие отношение к предполагаемой компетентности, ресурсам и мотивации нарушителей, описанные в разделе «Среда безопасности ОО». Например, утверждение о базовой СФБ неприемлемо, если требуется, чтобы ОО обеспечил защиту от нарушителей, обладающих высоким потенциалом нападения.

182 Оценщик также делает заключение, учтены ли в подразделе ПЗ «Обоснование требований безопасности» все специфические, связанные со стойкостью функций безопасности, характеристики целей безопасности. Оценщик может использовать прослеживание от требований к целям безопасности, чтобы сделать заключение, что требования, прослеженные к

целям безопасности со специфическими, связанными со стойкостью функций безопасности, характеристиками, при необходимости, включают соответствующее утверждение о стойкости связанных с этими требованиями функций безопасности.

APE_REQ.1.13C

APE_REQ.1-18 Оценщик ***должен исследовать*** «Обоснование требований безопасности», чтобы сделать заключение, прослежены ли требования безопасности ОО к целям безопасности для ОО.

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

184 Отсутствие такого прослеживания означает, что-либо подраздел «Обоснование требований безопасности» является неполным, либо раздел «Цели безопасности» является неполным, либо функциональное требование безопасности ОО является бесполезным.

185 Является также допустимым, но необязательным, прослеживание отдельных или всех требований доверия к безопасности ОО к целям безопасности для ОО.

186 Пример прослеживания требования доверия к безопасности ОО к цели безопасности для ОО – ПЗ, содержащий угрозу: "Пользователь непреднамеренно раскрывает информацию, используя изделие, которое он принимает за ОО" и цель безопасности для ОО для противостояния данной угрозе: "ОО должен быть четко помечен соответствующим номером версии". Изложенная цель безопасности для ОО может быть достигнута путем выполнения требований компонента ACM_CAP.1, и поэтому разработчик ПЗ прослеживает данный компонент к рассматриваемой цели безопасности для ОО.

APE_REQ.1-19 Оценщик ***должен исследовать*** подраздел ПЗ «Обоснование требований безопасности», чтобы сделать заключение, прослежены ли требования безопасности для среды ИТ к целям безопасности для среды.

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

188 Отсутствие такого прослеживания означает, что-либо подраздел «Обоснование требований безопасности» является неполным, либо подраздел «Цели безопасности для среды» является неполным, либо функциональное требование безопасности для среды ИТ является бесполезным.

189 Является также допустимым, но необязательным, для некоторых или всех требований доверия к безопасности для среды ИТ прослеживание к целям безопасности для среды.

APE_REQ.1-20 Оценщик ***должен исследо***вать «Обоснование требований безопасности», чтобы сделать заключение, содержится ли в нем для каждой цели безопасности для ОО приемлемое строгое обоснование того, что требования безопасности ОО пригодны для удовлетворения данной цели безопасности.

190 Если никакие требования безопасности ОО не прослежены к конкретной цели безопасности для ОО, то данный шаг оценивания считается неуспешным.

191 Оценщик делает заключение, демонстрирует ли строгое обоснование для цели безопасности для ОО, что, если все требования безопасности ОО, прослеженные к данной цели, удовлетворены, то цель безопасности для ОО достигнута.

192 Оценщик также делает заключение, действительно ли каждое требование безопасности ОО, прослеженное к цели безопасности для ОО, будучи удовлетворенным, вносит вклад в достижение данной цели безопасности.

193 Обратите внимание, что прослеживание от требований безопасности ОО к целям безопасности для ОО, представленное в подразделе «Обоснование требований безопасности», может быть частью строгого обоснования, но само по себе оно не является строгим обоснованием.

APE_REQ.1-21 Оценщик ***должен исследовать*** подраздел ПЗ «Обоснование требований безопасности», чтобы сделать заключение, содержит ли он для каждой цели безопасности для среды ИТ приемлемое строгое обоснование, что требования безопасности для среды ИТ пригодны для удовлетворения данной цели безопасности для среды ИТ.

194 Если никакие требования безопасности для среды ИТ не прослежены к конкретной цели безопасности для среды ИТ, то данный шаг оценивания считается неуспешным.

195 Оценщик делает заключение, демонстрирует ли строгое обоснование для цели безопасности для среды, что, если все требования безопасности для среды ИТ, прослеженные к данной цели безопасности для среды ИТ, удовлетворены, то цель безопасности для среды ИТ достигнута.

196 Оценщик также делает заключение, действительно ли каждое требование безопасности для среды ИТ, прослеженное к цели безопасности для среды ИТ, будучи удовлетворенным, вносит вклад в достижение данной цели безопасности.

197 Обратите внимание, что прослеживание требований безопасности для среды ИТ к целям безопасности для среды ИТ, представленное в подразделе

«Обоснование требований безопасности» может быть частью строгого обоснования, но само по себе оно не является строгим обоснованием.

APE_REQ.1.14C

APE_REQ.1-22 Оценщик ***должен исследовать*** подраздел ПЗ «Обоснование требований безопасности», чтобы сделать заключение, демонстрирует ли он внутреннюю непротиворечивость совокупности требований безопасности ИТ.

198 Оценщик делает заключение, что во всех случаях, когда различные требования безопасности ИТ имеют отношение к одним и тем же типам событий, операций, данных, тестов, подлежащих выполнению, и т.д., и данные требования могут вступать в противоречие друг с другом, дано приемлемое строгое обоснование отсутствия таких противоречий.

199 Например, если ПЗ содержит требования, связанные как с индивидуальной подотчетностью пользователей, так и с их анонимностью, необходимо, чтобы было показано, что данные требования не противоречат друг другу. Это может включать показ того, что ни одно из подлежащих аудиту событий, для которых требуется индивидуальная подотчетность пользователей, не имеет отношения к действиям, для которых требуется анонимность пользователей.

APE_REQ.1-23 Оценщик ***должен исследовать*** подраздел ПЗ «Обоснование требований безопасности», чтобы сделать заключение, демонстрирует ли он, что совокупность требований безопасности ИТ образует взаимно поддерживающее целое.

200 Данный шаг оценивания основывается на заключениях, сделанных в ходе выполнения шагов оценивания APE_REQ.1-18 и APE_REQ.1-19, связанных с исследованием прослеживания от требований безопасности ИТ к целям безопасности, и шагов оценивания APE_REQ.1-20 и APE_REQ.1-21, связанных с исследованием пригодности требований безопасности ИТ для удовлетворения целей безопасности. Данный шаг оценивания требует от оценщика рассмотреть возможность фактического недостижения какой-либо цели безопасности из-за недостаточной поддержки со стороны других требований безопасности ИТ.

201 Данный шаг оценивания также основывается на анализе зависимостей, выполняемом на предыдущих шагах оценивания, так как, если функциональное требование A имеет зависимость от функционального требования B, то B поддерживает A по определению.

202 Оценщик делает заключение, демонстрирует ли подраздел ПЗ «Обоснование требований безопасности» поддержку функциональными требованиями друг друга, где необходимо, даже когда указано, что зависимости между этими требованиями нет. Предполагается, что такая демонстрация охватывает те функциональные требования безопасности, которые направлены на:

а) предотвращение обхода механизмов, реализующих другие функциональные требования безопасности, такие, например, как FPT_RVM.1;

б) предотвращение вмешательства в работу механизмов, реализующих другие функциональные требования безопасности, такие, например, как FPT_SEP;

в) предотвращение деактивации механизмов, реализующих другие функциональные требования безопасности, такие, например, как FMT_MOF.1;

г) обеспечение возможности обнаружения нападений (атак), направленных на нарушение работы механизмов, реализующих другие функциональные требования безопасности, такие, например, как компоненты класса FAU.

203 В своем анализе оценщик учитывает результаты выполненных операций, чтобы сделать заключение, затрагивают ли они взаимную поддержку требованиями друг друга.

6.4.5.3.2 Действие APE_REQ.1.2E

APE_REQ.1-24 Оценщик ***должен исследовать*** изложение раздела ПЗ «Требования безопасности ИТ», чтобы сделать заключение, является ли оно логически упорядоченным.

204 Изложение требований безопасности ИТ является логически упорядоченным, если его содержание и структура изложения понятны целевой аудитории (то есть, оценщикам и потребителям).

APE_REQ.1-25 Оценщик ***должен исследовать*** изложение раздела ПЗ «Требования безопасности ИТ», чтобы сделать заключение, является ли оно полным.

205 При выполнении данного шага оценивания используются результаты шагов оценивания, выполняемых в соответствии с требованиями APE_REQ.1.1E и APE_SRE.1.1E, и в особенности – результаты исследования оценщиком подраздела «Обоснование требований безопасности».

206 Изложение раздела «Требования безопасности ИТ» является полным, если оценщик считает требования безопасности достаточными для обеспечения удовлетворения всех целей безопасности для ОО.

APE_REQ.1-26 Оценщик ***должен исследовать*** изложение раздела ПЗ «Требования безопасности ИТ», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

207 При выполнении данного шага оценивания используются результаты шагов оценивания, выполняемых в соответствии с требованиями APE_REQ.1.1E и APE_SRE.1.1E, и в особенности – результаты исследования оценщиком подраздела «Обоснование требований безопасности».

208 Изложение раздела «Требования безопасности ИТ» является внутренне непротиворечивым, если оценщик делает заключение, что ни одно требование безопасности не противоречит любому другому требованию

безопасности таким образом, что цель безопасности не будет полностью удовлетворена.

6.4.6 Оценка требований безопасности ИТ, сформулированных в явном виде (APE_SRE.1)

6.4.6.1 Цели

209 Цель данного подвида деятельности – сделать заключение, являются ли функциональные требования и/или требования доверия к безопасности, сформулированные без ссылки на ОК, приемлемыми и адекватными.

6.4.6.2 Замечания по применению

210 Этот раздел применим только в случае, если в ПЗ содержатся требования безопасности, сформулированные в явном виде без ссылки на часть 2 или 3 ОК. В противном случае все шаги оценивания, описанные в данном разделе, не применяемы и поэтому считаются удовлетворенными.

211 Требования семейства APE_SRE не заменяют требования семейства APE_REQ, а являются дополнительными к ним. Это означает, что требования безопасности, сформулированные в явном виде без ссылки на часть 2 или 3 ОК, должны быть оценены на соответствие критериям семейства APE_SRE, а также в сочетании со всеми остальными требованиями безопасности – на соответствие критериям семейства APE_REQ.

6.4.6.3 Исходные данные

212 Свидетельством оценки для этого подвида деятельности является ПЗ.

6.4.6.4 Действия оценщика

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

а) APE_SRE.1.1E;
б) APE_SRE.1.2E.

6.4.6.4.1 Действие APE_SRE.1.1E

APE_SRE.1.1C

APE_SRE.1-1 Оценщик ***должен проверить***, что в изложении раздела ПЗ «Требования безопасности ИТ» идентифицированы все требования безопасности ОО, которые сформулированы в явном виде без ссылки на ОК.

214 Требуется, чтобы все функциональные требования безопасности ОО, которые не специфицированы на основе функциональных компонентов из части 2 ОК, были четко идентифицированы как таковые. Аналогично также требуется, чтобы все требования доверия к безопасности ОО, которые не специфицированы на основе компонентов доверия из части 3 ОК, были четко идентифицированы как таковые.

APE_SRE.1.2C

APE_SRE.1-2 Оценщик ***должен проверить***, что в изложении раздела ПЗ «Требования безопасности ИТ» идентифицированы все требования безопасности для среды ИТ, которые сформулированы в явном виде без ссылки на ОК.

215 Требуется, чтобы все функциональные требования безопасности для среды ИТ, которые не специфицированы на основе функциональных компонентов из части 2 ОК, были четко идентифицированы как таковые. Аналогично также требуется, чтобы все требования доверия к среде ИТ, которые не специфицированы на основе компонентов доверия из части 3 ОК, были четко идентифицированы как таковые.

APE_SRE.1.3C

APE_SRE.1-3 Оценщик ***должен исследовать*** «Обоснование требований безопасности», чтобы сделать заключение, содержится ли в нем приемлемое строгое обоснование, почему каждое из сформулированных в явном виде требований безопасности пришлось сформулировать в явном виде.

216 Оценщик для каждого сформулированного в явном виде требования безопасности ИТ делает заключение, объясняется ли в строгом обосновании, почему существующие функциональные компоненты или компоненты доверия (из частей 2 и 3 ОК соответственно) не могли быть использованы для выражения требований безопасности, сформулированных в явном виде. При вынесении заключения оценщик принимает во внимание возможность выполнения операций (то есть, назначение, итерация, выбор и уточнение) над этими существующими компонентами.

APE_SRE.1.4C

APE_SRE.1-4 Оценщик ***должен исследовать*** каждое сформулированное в явном виде требование безопасности ИТ, чтобы сделать заключение, использованы ли для этого требования в качестве модели для представления компоненты, семейства и классы требований из ОК.

217 Оценщик делает заключение, представлены ли сформулированные в явном виде требования безопасности ИТ в том же стиле и на сопоставимом уровне детализации, что и компоненты из частей 2 или 3 ОК. Оценщик также делает заключение, подразделяются ли функциональные требования на отдельные функциональные элементы, и определяют ли требования доверия элементы действий разработчика, содержания и представление свидетельств, а также действий оценщика.

APE_SRE.1.5C

APE_SRE.1-5 Оценщик ***должен исследовать*** каждое сформулированное в явном виде требование безопасности ИТ, чтобы сделать заключение, измеримо ли оно и формулирует ли объективные требования оценки,

такие, что соответствие или несоответствие им ОО может быть определено и продемонстрировано систематическим методом.

218 Оценщик делает заключение, изложены ли функциональные требования таким образом, что они тестируемы и прослеживаемы к соответствующим представлениям ФБО. Оценщик также делает заключение, что требования доверия не приводят к потребности вынесения о них субъективного суждения со стороны оценщика.

APE_SRE.1.6C

APE_SRE.1-6 Оценщик ***должен исследовать*** каждое сформулированное в явном виде требование безопасности ИТ, чтобы сделать заключение, выражено ли оно четко и однозначно.

APE_SRE.1.7C

APE_SRE.1-7 Оценщик ***должен исследовать*** «Обоснование требований безопасности», чтобы сделать заключение, демонстрирует ли оно, что требования доверия применимы и приемлемы для поддержки любых сформулированных в явном виде функциональных требований безопасности ОО.

219 Оценщик делает заключение, приведет ли применение специфицированных требований доверия к получению значимого результата оценки для каждого сформулированного в явном виде функционального требования безопасности или следует специфицировать какие-либо другие требования доверия. Например, сформулированное в явном виде функциональное требование может предполагать потребность в конкретном документальном свидетельстве (таком, например, как модель ПБО), конкретной глубине тестирования или конкретном анализе (таком, как анализ стойкости функций безопасности ОО или анализ скрытых каналов).

6.4.6.4.2 Действие APE_SRE.1.2E

APE_SRE.1-8 Оценщик ***должен исследовать*** изложение раздела ПЗ «Требования безопасности ИТ», чтобы сделать заключение, все ли зависимости сформулированных в явном виде требований безопасности ИТ были идентифицированы.

220 Оценщик подтверждает, что никакие подлежащие удовлетворению зависимости не были пропущены разработчиком ПЗ.

221 Примеры возможных зависимостей: компоненты класса FAU, если в сформулированном в явном виде функциональном требовании упоминается аудит; компоненты семейства ADV_IMP, если в сформулированном в явном виде требовании доверия упоминается исходный текст или представление реализации ОО.

7 Оценка задания по безопасности

7.1 Введение

222 Этот раздел описывает оценку ЗБ. Оценка ЗБ начинается до начала каких-либо других действий по оценке ОО, так как ЗБ является основой и определяет условия выполнения данных действий. Окончательный вердикт по результатам оценки ЗБ не может быть вынесен до завершения оценки ОО, так как по результатам выполнения действий по оценке ОО в ЗБ могут быть внесены изменения.

223 Требования и методика оценки ЗБ идентичны для каждой оценки ЗБ, независимо от ОУД (или другой совокупности критериев доверия), заявленного в ЗБ.

224 Методика оценки в этом разделе базируется на требованиях к ЗБ, определенных в части 1 ОК, в особенности в Приложении В, и классе ASE из части 3 ОК.

7.2 Цели

225 В ЗБ идентифицируются функции безопасности и, возможно, механизмы безопасности, которые направлены на реализацию установленной политики безопасности организации и противостояние сформулированным угрозам с учетом сделанных предположений. Также предполагается, что в ЗБ определяются меры, которые обеспечивают доверие к тому, что продукт или система надлежащим образом противостоят угрозам и реализуют политику безопасности организации.

226 Цель оценки ЗБ – сделать заключение, является ли ЗБ:

а) полным: функции безопасности противостоят каждой угрозе и реализуют каждую политику безопасности организации;

б) достаточным: функции безопасности являются приемлемыми для угроз и политик безопасности организации, а меры доверия обеспечивают достаточное доверие к тому, что функции безопасности реализованы надлежащим образом;

в) логичным: ЗБ должно быть внутренне непротиворечиво;

г) точным отображением: если в ЗБ утверждается о соответствии одному или нескольким ПЗ, то ЗБ должно быть полным и точным отображением каждого упоминаемого ПЗ. В этом случае многие из результатов оценки ПЗ могут повторно использоваться при оценке ЗБ.

7.3 Организация оценки ЗБ

227 Деятельность по проведению полной оценки ЗБ охватывает следующее:

а) задачу получения исходных данных для оценки;

б) вид деятельности по оценке ЗБ, включающий следующие подвиды деятельности:

1) оценку раздела ЗБ «Описание ОО» (п. 7.4.1);

2) оценку раздела ЗБ «Среда безопасности ОО» (п. 7.4.2);

3) оценку раздела ЗБ «Введение ЗБ» (п. 7.4.3);

4) оценку раздела ЗБ «Цели безопасности» (п. 7.4.4);

5) оценку раздела ЗБ «Утверждения о соответствии ПЗ» (п. 7.4.5);

6) оценку раздела ЗБ «Требования безопасности ИТ» (п. 7.4.6);

7) оценку сформулированных в явном виде требований безопасности ИТ (п. 7.4.7);

8) оценку раздела ЗБ «Краткая спецификация ОО» (п. 7.4.8).

в) задачу оформления результатов оценки.

228 Подвиды деятельности по оценке определяются требованиями доверия класса ASE, содержащимися в части 3 ОК.

229 В настоящей главе описываются подвиды деятельности, включенные в оценку ЗБ. Хотя подвиды деятельности могут быть строго не упорядочены, некоторые зависимости между подвидами деятельности должны быть учтены оценщиком.

230 Необходимость выполнения подвидов деятельности по оценке утверждений о соответствии ПЗ и по оценке сформулированных в явном виде требований безопасности ИТ существует не всегда: подвид деятельности по оценке утверждений о соответствии ПЗ выполняется только тогда, когда имеет место утверждение о соответствии ПЗ, а подвид деятельности по оценке сформулированных в явном виде требований безопасности ИТ выполняется только тогда, когда в изложение требований безопасности ИТ включены требования безопасности, взятые не из частей 2 или 3 ОК.

231 Некоторая информация, подлежащая включению в ЗБ, может быть представлена соответствующей ссылкой. Например, если в ЗБ утверждается о соответствии некоторому ПЗ, то такая информация из ПЗ, как описание среды и угроз, может рассматриваться как часть ЗБ, и предполагается, что она соответствует критериям для ЗБ.

232 Если в ЗБ утверждается о соответствии оцененному ПЗ, и ЗБ в значительной степени основано на содержании этого ПЗ, то допускается повторное использование результатов оценки ПЗ при выполнении многих из перечисленных выше подвидов деятельности. В частности, повторное использование может оказаться возможным при оценке изложения среды безопасности, целей безопасности и требований безопасности ИТ. В ЗБ допускается утверждение о соответствии нескольким ПЗ.

7.4 Вид деятельности «Оценка ЗБ»

7.4.1 Оценка раздела «Описание ОО» (ASE_DES.1)

7.4.1.1 Цели

233 Цель данного подвида деятельности – сделать заключение, содержит ли «Описание ОО» соответствующую для понимания назначения ОО и его функциональных возможностей информацию, а также сделать заключение, является ли описание ОО полным и непротиворечивым.

7.4.1.2 Исходные данные

234 Свидетельством оценки для этого подвида деятельности является ЗБ.

7.4.1.3 Замечания по применению

235 Между ОО и продуктом, который может приобрести потребитель, могут существовать некоторые отличия. ОО представляет собой сущность, которая оценивается в соответствии с ЗБ. Хотя в некоторых случаях ОО может представлять собой единый продукт, в общем случае это не так. ОО может быть продуктом, частью продукта, набором продуктов, уникальной технологией, которая никогда не реализовывалась в виде продукта, или комбинацией всего перечисленного в конкретной конфигурации или в нескольких конфигурациях. Эта конкретная конфигурация или совокупность конфигураций называется *оцениваемой конфигурацией*. ЗБ четко описывает соотношение между ОО и любыми связанными с ним продуктами.

7.4.1.4 Действия оценщика

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

а) ASE_DES.1.1E;
б) ASE_DES.1.2E;
в) ASE_DES.1.3E.

7.4.1.4.1 Действие ASE_DES.1.1E

ASE_DES.1.1C

ASE_DES.1-1 Оценщик ***должен исследовать*** «Описание ОО», чтобы сделать заключение, описан ли в нем тип продукта или системы для ОО.

237 Оценщик делает заключение, достаточно ли «Описание ОО» для того, чтобы дать читателю общее понимание предполагаемого использования продукта или системы, и обеспечивает ли, таким образом, контекст оценки. Примерами некоторых типов продуктов и систем являются: межсетевой экран, смарт-карта, крипто-модем, web-сервер, интрасеть.

238 Существуют ситуации, когда является очевидным, что у ОО ожидается наличие некоторых функциональных возможностей, определяемых типом продукта или системы. Если эти функциональные возможности отсутствуют,

то оценщик делает заключение, адекватно ли это отсутствие рассматривается в разделе «Описание ОО». Примером этого является ОО типа «межсетевой экран», в «Описании ОО» которого изложено, что он не может быть подключен к сетям.

ASE_DES.1-2 Оценщик ***должен исследовать*** «Описание ОО», чтобы сделать заключение, описаны ли в нем в общих чертах физическая область применения и границы ОО.

239 Оценщик делает заключение, рассматриваются ли в разделе «Описание ОО» аппаратные, программно-аппаратные и программные компоненты и/или модули, которые составляют ОО, на том уровне детализации, который достаточен для общего понимания читателем этих компонентов и/или модулей.

240 Если ОО не тождественен продукту, то оценщик делает заключение, описано ли надлежащим образом в «Описании ОО» физическое соотношение между ОО и продуктом.

ASE_DES.1-3 Оценщик ***должен исследовать*** «Описание ОО», чтобы сделать заключение, описаны ли в нем в общих чертах логическая область применения и границы ОО.

241 Оценщик делает заключение, рассмотрены ли в разделе «Описание ОО» ИТ-характеристики, и в особенности характеристики безопасности, предоставляемые ОО, на таком уровне детализации, который достаточен для общего понимания читателем этих характеристик.

242 Если ОО не тождественен продукту, то оценщик делает заключение, описано ли надлежащим образом в «Описании ОО» логическое соотношение между ОО и продуктом.

7.4.1.4.2 Действие ASE_DES.1.2E

ASE_DES.1-4 Оценщик ***должен исследовать*** ЗБ, чтобы сделать заключение, является ли «Описание ОО» логически упорядоченным.

243 Изложение раздела «Описание ОО» является логически упорядоченным, если его текст и структура понятны целевой аудитории (то есть оценщикам и потребителям).

ASE_DES.1-5 Оценщик ***должен исследовать*** ЗБ, чтобы сделать заключение, является ли «Описание ОО» внутренне непротиворечивым.

244 Оценщику следует помнить, что этот раздел ЗБ предназначен только для того, чтобы определить общее назначение ОО.

7.4.1.4.3 Действие ASE_DES.1.3E

ASE_DES.1-6 Оценщик ***должен исследовать*** ЗБ, чтобы сделать заключение, согласовано ли «Описание ОО» с другими частям ЗБ.

245 Оценщик делает заключение, в частности, что в разделе «Описание ОО» не описываются угрозы, характеристики безопасности или конфигурации ОО, которые не рассматриваются в каком-либо другом месте ЗБ.

7.4.2 Оценка раздела «Среда безопасности ОО» (ASE_ENV.1)

7.4.2.1 Цели

246 Цель данного подвида деятельности – сделать заключение, обеспечивает ли изложение раздела «Среда безопасности ОО» в ЗБ четкое и непротиворечивое определение проблемы безопасности, решение которой возлагается на ОО и его среду.

7.4.2.2 Исходные данные

247 Свидетельством оценки для этого подвида деятельности является ЗБ.

7.4.2.3 Действия оценщика

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

а) ASE_ENV.1.1E;
б) ASE_ENV.1.2E.

7.4.2.3.1 Действие ASE_ENV.1.1E

ASE_ENV.1.1C

ASE_ENV.1-1 Оценщик ***должен исследовать*** изложение раздела ЗБ «Среда безопасности ОО», чтобы сделать заключение, идентифицируются и разъясняются ли в нем какие-либо предположения.

249 Предположения могут быть разделены на предположения относительно предполагаемого использования ОО и предположения относительно среды использования ОО.

250 Оценщик делает заключение, учитывают ли предположения относительно предполагаемого использования ОО такие аспекты как предполагаемое применение ОО, потенциальная ценность активов, требующих защиты со стороны ОО, и возможные ограничения использования ОО.

251 Оценщик делает заключение, достаточно ли подробно разъяснено каждое предположение относительно предполагаемого использования ОО для того, чтобы предоставить возможность потребителям решить, соответствует ли предполагаемое использование ими ОО сделанным предположениям. Если предположения не являются понятными, то это может, в конечном счете, привести к тому, что потребители будут использовать ОО в среде, для которой он не предназначен.

252 Оценщик делает заключение, охватывают ли предположения относительно среды использования ОО аспекты физической среды, персонала и внешних связей:

а) Физические аспекты включают какие-либо предположения, которые необходимо сделать относительно физического расположения ОО или подключенных периферийных устройств для того, чтобы ОО функционировал безопасным образом. Несколько примеров:

- предполагается, что консоли администраторов находятся в некоторой зоне, доступ в которую ограничен только персоналом, являющимся администраторами;
- предполагается, что хранение всех файлов для ОО осуществляется на той рабочей станции, на которой функционирует ОО.

б) Аспекты, имеющие отношение к персоналу, включают какие-либо предположения, которые необходимо сделать относительно пользователей и администраторов ОО или других лиц (включая потенциальные источники угроз) внутри среды ОО для того, чтобы ОО функционировал безопасным образом. Несколько примеров:

- предполагается, что пользователи имеют конкретные навыки или специальные знания;
- предполагается, что пользователи имеют определенный минимальный допуск;
- предполагается, что администраторы обновляют антивирусную базу данных ежемесячно.

в) Аспекты внешних связей включают предположения, которые необходимо сделать относительно связей между ОО и другими внешними по отношению к ОО системами или продуктами ИТ (аппаратными, программными и программно-аппаратными средствами или их комбинацией) для того, чтобы ОО функционировал безопасным образом. Несколько примеров:

- предполагается, что для хранения файлов регистрации, генерируемых ОО, доступным является, по крайней мере, 100Мб внешнего дискового пространства;
- предполагается, что ОО является единственным приложением, не относящимся к операционной системе, выполняемым на отдельной рабочей станции;
- предполагается, что дисковод ОО для накопителей на ГМД отключен;
- предполагается, что ОО не будет подключаться к недоверенной сети.

253 Оценщик делает заключение, достаточно ли подробно разъяснено каждое предположение относительно среды использования ОО для того, чтобы предоставить возможность потребителям решить, соответствует ли их предполагаемая среда сделанным предположениям о среде ОО. Если предположения не являются понятными, то это может, в конечном счете,

привести к тому, что ОО будет использоваться в среде, в которой он не будет функционировать безопасным образом.

ASE_ENV.1.2C

ASE_ENV.1-2 Оценщик ***должен исследовать*** изложение раздела «Среда безопасности ОО», чтобы сделать заключение, идентифицируются и разъясняются ли в нем какие-либо угрозы.

254 Если цели безопасности для ОО и его среды получены только на основе предположений и политики безопасности организации, то изложение угроз в ЗБ не потребуется. В этом случае этот шаг оценивания не применяем и поэтому считается удовлетворенным.

255 Оценщик делает заключение, все ли идентифицированные угрозы ясно разъясняются в терминах идентифицированного источника угрозы, нападения и актива, являющегося объектом нападения.

256 Оценщик также делает заключение, характеризуются ли источники угроз (нарушители) через их компетентность, ресурсы и мотивацию, а нападения – через методы нападения, какие-либо используемые уязвимости и возможность нападения.

ASE_ENV.1.3C

ASE_ENV.1-3 Оценщик ***должен исследовать*** изложение раздела «Среда безопасности ОО», чтобы сделать заключение, идентифицируются и разъясняются ли в нем какие-либо политики безопасности организации.

257 Если цели безопасности для ОО и его среды получены только на основе предположений и угроз, то нет необходимости в том, чтобы политика безопасности организации была представлена в ЗБ. В этом случае данный шаг оценивания не применяем и поэтому считается удовлетворенным.

258 Оценщик делает заключение, выполнено ли изложение политики безопасности организации в виде правил, практических приемов или руководств, установленных организацией, контролирующей среду, в которой предстоит использовать ОО, которым должны следовать ОО или его среда. Примером политики безопасности организации является требование генерации и шифрования паролей в соответствии со стандартом.

259 Оценщик делает заключение, достаточно ли подробно разъяснена и/или интерпретирована каждая политика безопасности организации для того, чтобы сделать ее ясной для понимания; ясное представление формулировок политик является необходимым для того, чтобы дать возможность проследить цели безопасности по отношению к ним.

7.4.2.3.2 Действие ASE_ENV.1.2E

ASE_ENV.1-4 Оценщик ***должен исследовать*** изложение раздела «Среда безопасности ОО», чтобы сделать заключение, является ли оно логически упорядоченным.

260 Изложение раздела «Среда безопасности ОО» является логически упорядоченным, если его текст и структура целевой аудитории (то есть оценщикам и потребителям).

ASE_ENV.1-5 Оценщик ***должен исследовать*** изложение раздела «Среда безопасности ОО», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

261 Примерами внутренне противоречивого изложения раздела «Среда безопасности ОО» являются:

– изложение раздела «Среда безопасности ОО», которое содержит угрозу, метод нападения для которой – вне возможностей реализации источником угрозы;

– изложение раздела «Среда безопасности ОО», которое содержит правило политики безопасности организации "ОО не должен подключаться к Интернет" и угрозу, источником которой является злоумышленник из Интернет.

7.4.3 Оценка раздела «Введение ЗБ» (ASE_INT.1)

7.4.3.1 Цели

262 Цель данного подвида деятельности – сделать заключение, является ли раздел «Введение ЗБ» полным и согласованным со всеми другими частями ЗБ, и правильно ли в нем идентифицируется ЗБ.

7.4.3.2 Исходные данные

263 Свидетельством оценки для этого подвида деятельности является ЗБ.

7.4.3.3 Действия оценщика

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

а) ASE_INT.1.1E;
б) ASE_INT.1.2E;
в) ASE_INT.1.3E.

7.4.3.3.1 Действие ASE_INT.1.1E

ASE_INT.1.1C

ASE_INT.1-1 Оценщик ***должен проверить***, представлена ли в разделе «Введение ЗБ» идентификационная информация, необходимая для контроля и идентификации ЗБ и ОО, на который данное ЗБ ссылается.

265 Оценщик делает заключение, включает ли идентификационная информация ЗБ:

а) информацию, необходимую для контроля и уникальной идентификации ЗБ (например, наименование ЗБ, номер версии, дату публикации, авторов);

б) информацию, необходимую для контроля и уникальной идентификации ОО, на который данное ЗБ ссылается (например, идентификационную информацию ОО, номер версии ОО);

в) указание версии ОК, использованной при разработке ЗБ;

г) дополнительную информацию, в соответствии с требованиями системы сертификации.

ASE_INT.1.2C

ASE_INT.1-2 Оценщик ***должен проверить***, представлена ли в разделе «Введение ЗБ» «Аннотация ЗБ» в повествовательной форме.

266 «Аннотация ЗБ» предназначена, чтобы предоставить краткое резюме содержания ЗБ (более детальное описание предоставляется в разделе «Описание ОО»), которое является достаточно подробным, чтобы дать возможность потенциальному потребителю сделать заключение, представляет ли для него интерес данный ОО (а значит и все остальные части ЗБ).

ASE_INT.1.3C

ASE_INT.1-3 Оценщик ***должен проверить***, содержит ли «Введение ЗБ» подраздел «Утверждение о соответствии ОК», в котором излагается утверждение о соответствии ОО Общим критериям.

267 Оценщик делает заключение, соответствует ли «Утверждение о соответствии ОК» подразделу 5.4 части 1 ОК.

268 Оценщик делает заключение, что «Утверждение о соответствии ОК» содержит утверждение либо о соответствии части 2, либо части 2, расширенной другими компонентами требований.

269 Оценщик делает заключение, что «Утверждение о соответствии ОК» содержит утверждение о соответствии либо к части 3, либо к части 3, усиленной и/или расширенной другими компонентами требований доверия.

270 Если утверждается о соответствии части 3, то оценщик делает заключение, сформулировано ли в подразделе «Утверждение о соответствии ОК», какой ОУД или другой пакет доверия заявлен.

271 Если утверждается об усилении части 3, то оценщик делает заключение, сформулировано ли в подразделе «Утверждение о соответствии ОК», какой ОУД или другой пакет доверия заявлен, а также какое усиление данного ОУД или пакета доверия заявлено.

272 Если утверждается о расширении части 3 и требования доверия представлены в виде ОУД, дополненного требованиями доверия не из части 3, то оценщик делает заключение, сформулировано ли в подразделе «Утверждение о соответствии ОК», какой ОУД заявлен.

273 Если утверждается о расширении части 3 и требования доверия представлены в виде пакета требований доверия, дополненного требованиями доверия не из части 3, то оценщик делает заключение, сформулировано ли в подразделе «Утверждение о соответствии ОК», какие требования доверия, взятые из части 3 ОК, заявлены.

274 Если утверждается о соответствии ПЗ, то оценщик делает заключение, сформулировано ли в подразделе «Утверждение о соответствии ОК», по отношению к какому профилю защиты или профилям защиты сделано утверждение о соответствии.

275 Оценщику следует помнить, что если делается утверждение о соответствии ПЗ, то применяются критерии ASE_PPC.1, и что если утверждается о расширении части 3 или части 2 ОК, то применяются критерии ASE_SRE.1.

7.4.3.3.2 Действие ASE_INT.1.2E

ASE_INT.1-4 Оценщик ***должен исследовать*** «Введение ЗБ», чтобы сделать заключение, является ли оно логически упорядоченным.

276 «Введение ЗБ» является логически упорядоченным, если его текст и структура изложения понятны целевой аудитории (то есть оценщикам и потребителям).

ASE_INT.1-5 Оценщик ***должен исследовать*** «Введение ЗБ», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

277 Анализ внутренней непротиворечивости, естественно, опирается на краткий обзор ЗБ, представляющий собой резюме содержания ЗБ.

7.4.3.3.3 Действие ASE_INT.1.3E

ASE_INT.1-6 Оценщик ***должен исследовать*** ЗБ, чтобы сделать заключение, согласовано ли «Введение ЗБ» с другими частями ЗБ.

278 Оценщик делает заключение, предоставляет ли «Аннотация ЗБ» точную общую характеристику ОО. В частности оценщик делает заключение, согласована ли «Аннотация ЗБ» с разделом «Описание ОО», и не излагается и не предполагается ли в нем наличие характеристик безопасности, которые выходят за рамки оценки.

279 Оценщик также делает заключение, согласовано ли «Утверждение о соответствии ОК» с другими частями ЗБ.

7.4.4 Оценка целей безопасности (ASE_OBJ.1)

7.4.4.1 Цели

280 Цель данного подвида деятельности – сделать заключение, полностью ли и согласовано ли описаны цели безопасности, а также сделать заключение, направлены ли цели безопасности на противостояние идентифицированным угрозам, на достижение идентифицированной политики безопасности организации, и согласованы ли они с изложенными предположениями.

7.4.4.2 Исходные данные

281 Свидетельством оценки для этого подвида деятельности является ЗБ.

7.4.4.3 Действия оценщика

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

а) ASE_OBJ.1.1E;
б) ASE_OBJ.1.2E.

7.4.4.3.1 Действие ASE_OBJ.1.1E

ASE_OBJ.1.1C

ASE_OBJ.1-1 Оценщик ***должен проверить***, определены ли в изложении целей безопасности цели безопасности для ОО и его среды.

283 Оценщик делает заключение, ясно ли определено для каждой цели безопасности, относится она к ОО, к среде или к тому и другому.

ASE_OBJ.1.2C

ASE_OBJ.1-2 Оценщик ***должен исследовать*** «Обоснование целей безопасности», чтобы сделать заключение, все ли цели безопасности для ОО прослеживаются к аспектам идентифицированных угроз, которым необходимо противостоять, и/или к аспектам политики безопасности организации, которой должен следовать ОО.

284 Оценщик делает заключение, прослеживается ли каждая цель безопасности для ОО, по крайней мере, к одной угрозе или правилу политики безопасности организации.

285 Неудача при попытке такого прослеживания свидетельствует о том, что, либо обоснование целей безопасности является неполным, либо изложение угроз/политики безопасности организации является неполным, либо цель безопасности для ОО является бесполезной.

ASE_OBJ.1.3C

ASE_OBJ.1-3 Оценщик ***должен исследовать*** «Обоснование целей безопасности», чтобы сделать заключение, прослежены ли цели безопасности для среды к идентифицированным угрозам, которым должна противостоять среда ОО, и/или к аспектам политики безопасности организации, которым должна удовлетворять среда ОО, и/или к предположениям, которым должна удовлетворять среда ОО.

286 Оценщик делает заключение, прослеживается ли каждая цель безопасности для среды, по крайней мере, к одному предположению, угрозе или правилу политики безопасности организации.

287 Неудача при попытке такого прослеживания свидетельствует о том, что, либо обоснование целей безопасности является неполным, либо изложение предположений/угроз/политики безопасности организации является неполным, либо цель безопасности для среды является бесполезной.

ASE_OBJ.1.4C

ASE_OBJ.1-4 Оценщик ***должен исследовать*** «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждой угрозы приемлемое строгое обоснование того, что цели безопасности пригодны для противостояния данной угрозе.

288 Если ни одна цель безопасности не прослежена к конкретной угрозе, то результат данного шага оценивания – «неудовлетворительно».

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

290 Оценщик также делает заключение, действительно ли каждая цель безопасности, которая прослежена к угрозе, будучи достигнутой, вносит вклад в устранение, снижение или компенсацию последствий реализации данной угрозы.

291 Примеры устранения угрозы:

- устранение для источника угрозы (нарушителя) возможности использовать какой-либо метод нападения;
- устранение мотивации источника угрозы (нарушителя) путем применения сдерживающих факторов;
- устранение источника угрозы (например, отключение от сети машин, часто приводящих к фатальному сбою этой сети).

292 Примеры снижения угрозы:

- ограничение для источника угрозы возможности использования методов нападения;
- ограничение возможностей источников угрозы;
- снижение вероятности успешного результата инициированного нападения;
- повышенные требования к компетентности и ресурсам источника угрозы.

293 Примеры компенсации последствий реализации угрозы:

– частое создание резервных копий активов;

– наличие резервных копий ОО;

– частая смена ключей, используемых в течение сеанса связи, чтобы последствия компрометации одного ключа были относительно незначительными.

294 Обратите внимание, что прослеживание целей безопасности к угрозам в обосновании целей безопасности может быть частью строгого обоснования, но само по себе оно не является строгим обоснованием. Даже в том случае, когда цель безопасности является просто изложением, отражающим намерение предотвратить реализацию конкретной угрозы, то все равно требуется строгое обоснование, хотя в этом случае оно может быть минимальным.

ASE_OBJ.1.5C

ASE_OBJ.1-5 Оценщик ***должен исследовать*** «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждого аспекта политики безопасности организации приемлемое строгое обоснование того, что цели безопасности пригодны для покрытия данного аспекта политики безопасности организации.

295 Если ни одна цель безопасности не прослежена к политике безопасности организации, то результат данного шага оценивания – «неудовлетворительно».

296 Оценщик делает заключение, демонстрирует ли строгое обоснование для политики безопасности организации то, что, если все цели безопасности, прослеженные к политике безопасности организации, достигнуты, то политика безопасности организации реализована.

297 Оценщик также делает заключение, действительно ли каждая цель безопасности, которая прослежена к политике безопасности организации, будучи достигнутой, вносит вклад в реализацию политики безопасности организации.

298 Обратите внимание, что прослеживание целей безопасности к политике безопасности организации в обосновании целей безопасности может быть частью строгого обоснования, но само по себе оно не является строгим обоснованием. Даже в том случае, когда цель безопасности является просто изложением, отражающим намерение реализовать конкретную политику безопасности, то все равно требуется строгое обоснование, хотя в этом случае оно может быть минимальным.

ASE_OBJ.1-6 Оценщик ***должен исследовать*** «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждого предположения приемлемое строгое обоснование того, что цели

безопасности для среды пригодны для покрытия данного предположения.

299 Если ни одна цель безопасности для среды не прослежена к изложенному предположению, то результат данного шага оценивания – «неудовлетворительно».

300 Предположение является или предположением относительно предполагаемого использования ОО, или предположением относительно среды использования ОО.

301 Оценщик делает заключение, демонстрирует ли строгое обоснование для предположения относительно предполагаемого использования ОО то, что, если все цели безопасности для среды, прослеженные к данному предположению, достигнуты, то предполагаемое использование ОО поддерживается.

302 Оценщик также делает заключение, действительно ли каждая цель безопасности для среды, прослеживаемая к некоторому предположению относительно предполагаемого использования ОО, будучи достигнутой, вносит вклад в поддержку предполагаемого использования.

303 Оценщик делает заключение, демонстрирует ли строгое обоснование для предположения относительно среды использования ОО то, что, если все цели безопасности для среды, прослеженные к данному предположению, достигнуты, то среда согласуется с данным предположением.

304 Оценщик также делает заключение, действительно ли каждая цель безопасности для среды, которая прослежена к предположению относительно среды использования ОО, будучи достигнутой, вносит вклад в достижение согласованности среды с предположением.

305 Обратите внимание, что прослеживание целей безопасности для среды к предположениям относительно среды использования ОО в подразделе «Обоснование целей безопасности» может быть частью строгого обоснования, но само по себе оно не является строгим обоснованием. Даже в том случае, когда цель безопасности представляет собой просто перефразированное предположение, то все равно требуется строгое обоснование, хотя в этом случае оно может быть минимальным.

7.4.4.3.2 Действие ASE_OBJ.1.2E

ASE_OBJ.1-7 Оценщик ***должен исследовать*** изложение раздела «Цели безопасности», чтобы сделать заключение, является ли оно логически упорядоченным.

306 Изложение раздела «Цели безопасности» является логически упорядоченным, если его текст и структура понятны целевой аудитории (то есть оценщикам и потребителям).

ASE_OBJ.1-8 Оценщик ***должен исследовать*** изложение раздела «Цели безопасности», чтобы сделать заключение, является ли оно полным.

307 Изложение раздела «Цели безопасности» является полным, если цели безопасности достаточны для противостояния всем идентифицированным угрозам и покрывают все идентифицированные политики безопасности организации и предположения. Данный шаг оценивания может выполняться совместно с шагами оценивания ASE_OBJ.1-4, ASE_OBJ.1-5 и ASE_OBJ.1-6.

ASE_OBJ.1-9 Оценщик ***должен исследовать*** изложение раздела «Цели безопасности», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

308 Изложение раздела «Цели безопасности» является внутренне непротиворечивым, если цели безопасности не противоречат друг другу. Примером противоречия могут служить следующие две цели безопасности: "Идентификатор пользователя не подлежит раскрытию" и "Идентификатор пользователя должен быть доступен другим пользователям".

7.4.5 Оценка раздела «Утверждение о соответствии ПЗ» (ASE_PPC.1)

309 Данный подраздел применим только, если в ЗБ утверждается о соответствии одному или нескольким ПЗ. Если в ЗБ не утверждается о соответствии одному или нескольким ПЗ, то все шаги оценивания из этого подраздела не применяемы и поэтому считаются удовлетворенными.

7.4.5.1 Цели

310 Цель данного подвида деятельности – сделать заключение, является ли ЗБ корректным отображением любого ПЗ, соответствие которому заявлено в ЗБ.

7.4.5.2 Исходные данные

311 Свидетельствами оценки для этого подвида деятельности являются:

а) ЗБ;

б) профиль (профили) защиты, о соответствии которому (которым) заявлено в ЗБ.

7.4.5.3 Действия оценщика

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

а) ASE_PPC.1.1E;

б) ASE_PPC.1.2E.

7.4.5.3.1 Действие ASE_PPC.1.1E

ASE_PPC.1.1C

ASE_PPC.1-1 Оценщик ***должен проверить***, что в каждом утверждении о соответствии ПЗ в ЗБ идентифицирован ПЗ, о соответствии которому делается утверждение.

313 Оценщик делает заключение, идентифицирован ли однозначно каждый ПЗ, о соответствии которому в ЗБ делается утверждение (например, путем указания наименования и номера версии или использования идентификационной информации, включенной в раздел «Введение» данного ПЗ). Оценщику следует помнить, что утверждения о частичном соответствии ПЗ не допускаются ОК.

ASE_PPC.1.2C

ASE_PPC.1-2 Оценщик ***должен проверить***, что в каждом утверждении о соответствии ПЗ идентифицированы формулировки требований безопасности ИТ, в которых завершены разрешенные операции ПЗ или иначе выполнено дальнейшее уточнение требований ПЗ.

314 В ЗБ нет необходимости повторять формулировки требований безопасности, содержащиеся в ПЗ и не модифицируемые в данном ЗБ. Если, однако, функциональные требования безопасности ПЗ содержат незавершенные операции, или разработчик ЗБ применил операцию «уточнение» к какому-либо требованию безопасности ПЗ, то эти требования в ЗБ должны быть ясно определены.

ASE_PPC.1.3C

ASE_PPC.1-3 Оценщик ***должен проверить***, что для каждого утверждения о соответствии ПЗ идентифицированы те цели безопасности и требования безопасности ИТ, которые являются дополнительными по отношению к целям безопасности и требованиям безопасности ИТ, содержащимся в ПЗ.

315 Оценщик делает заключение, ясно ли определены все цели безопасности и требования безопасности, которые включены в ЗБ, но не были включены в ПЗ.

7.4.5.3.2 Действие ASE_PPC.1.2E

ASE_PPC.1-4 Для каждого утверждения о соответствии ПЗ оценщик ***должен исследовать*** ЗБ, чтобы сделать заключение, все ли операции, выполненные по отношению к требованиям безопасности ИТ из ПЗ, не выходят за рамки, установленные ПЗ.

316 Данный шаг оценивания охватывает не только незавершенные операции «назначение» и «выбор» в ПЗ, но также и любое применение операции «уточнение» по отношению к требованиям безопасности, взятым из ПЗ.

7.4.6 Оценка раздела «Требования безопасности ИТ» (ASE_REQ.1)

7.4.6.1 Цели

317 Цель данного подвида деятельности – сделать заключение, является ли описание требований безопасности ОО (как функциональных требований безопасности ОО, так и требований доверия к безопасности ОО) и требований безопасности для среды ИТ полным и непротиворечивым, и

обеспечивают ли данные требования безопасности адекватную основу для разработки ОО, который бы достигал своих целей безопасности.

7.4.6.2 Исходные данные

318 Свидетельством оценки для этого подвида деятельности является ЗБ.

7.4.6.3 Действия оценщика

319 Действия оценщика включают два элемента из части 3 ОК:

а) ASE_REQ.1.1E;

б) ASE_REQ.1.2E.

7.4.6.3.1 Действие ASE_REQ.1.1E

ASE_REQ.1.1C

ASE_REQ.1-1 Оценщик ***должен проверить*** изложение функциональных требований безопасности ОО, чтобы сделать заключение, идентифицированы ли в нем функциональные требования безопасности ОО, составленные из компонентов функциональных требований из части 2 ОК.

320 Оценщик делает заключение, что все компоненты функциональных требований безопасности ОО, взятые из части 2 ОК, идентифицированы либо путем ссылки на отдельные компоненты из части 2, либо путем ссылки на отдельные компоненты из ПЗ, о соответствии которому утверждается в ЗБ, либо путем воспроизведения их в ЗБ.

ASE_REQ.1-2 Оценщик ***должен проверить***, что каждая ссылка на компонент функциональных требований безопасности ОО является правильной.

321 Для каждой ссылки на компонент функционального требования безопасности ОО из части 2 ОК оценщик делает заключение, существует ли упомянутый компонент в части 2 ОК.

322 Для каждой ссылки на компонент функционального требования безопасности ОО из ПЗ оценщик делает заключение, существует ли упомянутый компонент в данном ПЗ.

ASE_REQ.1-3 Оценщик ***должен проверить***, что каждый компонент функциональных требований безопасности ОО, взятый из части 2 ОК и воспроизведенный в ЗБ, воспроизведен правильно.

323 Оценщик делает заключение, правильно ли воспроизведены требования в подразделе ЗБ «Функциональные требования безопасности ОО»; при этом исследование разрешенных операций не проводится. Исследование правильности операций над компонентами осуществляется при выполнении шагов оценивания ASE_REQ.1-11 и ASE_REQ.1-12.

ASE_REQ.1.2C

ASE_REQ.1-4 Оценщик ***должен проверить*** изложение подраздела ЗБ «Требования доверия к безопасности ОО», чтобы сделать заключение,

идентифицированы ли в нем требования доверия к безопасности ОО, составленные из компонентов требований доверия из части 3 ОК.

324 Оценщик делает заключение, все ли компоненты требований доверия к безопасности ОО, взятые из части 3 ОК, идентифицированы либо путем ссылки на некоторый ОУД, либо на отдельные компоненты из части 3, либо путем ссылки на ПЗ, соответствие которому заявлено в ЗБ, либо путем их воспроизведения в ЗБ.

ASE_REQ.1-5 Оценщик ***должен проверить***, что каждая ссылка на компоненты требований доверия к безопасности ОО является правильной.

325 Для каждой ссылки на компонент требований доверия к безопасности ОО из части 3 ОК оценщик делает заключение, существует ли упомянутый компонент в части 3 ОК.

326 Для каждой ссылки на компонент требований доверия к безопасности ОО из ПЗ оценщик делает заключение, существует ли упомянутый компонент в данном ПЗ.

ASE_REQ.1-6 Оценщик ***должен проверить***, что каждый компонент требований доверия к безопасности ОО, взятый из части 3 ОК и воспроизведенный в ЗБ, воспроизведен правильно.

327 Оценщик делает заключение, правильно ли воспроизведены требования в подразделе ЗБ «Требования доверия к безопасности ОО»; при этом исследование выполнения разрешенных операций не проводится. Исследование правильности операций над компонентами осуществляется при выполнении шагов оценивания ASE_REQ.1-11 и ASE_REQ.1-12.

ASE_REQ.1.3C

ASE_REQ.1-7 Оценщик ***должен исследовать*** изложение подраздела «Требования доверия к безопасности ОО», чтобы сделать заключение, включает ли оно ОУД, определенный в части 3 ОК, либо в нем соответствующим образом строго обосновывается, что оно не включает ОУД.

328 Если никакой из ОУД не включен, то оценщик делает заключение, указана ли в строгом обосновании причина невключения ОУД в подраздел «Требования доверия к безопасности ОО». Это строгое обоснование может указывать либо на причину невозможности, нежелательности или нецелесообразности включения ОУД в ЗБ, либо на причину невозможности, нежелательности или нецелесообразности включения конкретных компонентов семейств, составляющих ОУД1 (ACM_CAP, ADO_IGS, ADV_FSP, ADV_RCR, AGD_ADM, AGD_USR и ATE_IND).

ASE_REQ.1.4C

ASE_REQ.1-8 Оценщик ***должен исследовать*** «Обоснование требований безопасности», чтобы сделать заключение, достаточно ли строго в нем

обосновывается то, что изложение требований доверия к безопасности ОО является приемлемым.

329 Если требования доверия содержат какой-либо ОУД, то в строгом обосновании допустимо рассматривать выбор конкретного ОУД в целом, а не каждого отдельного компонента данного ОУД. Если подраздел «Требования доверия к безопасности ОО» содержит компоненты, усиливающие выбранный ОУД, оценщик делает заключение, дано ли строгое обоснование каждого такого усиления. Если подраздел «Требования доверия к безопасности ОО» содержит требования доверия, сформулированные в явном виде, оценщик делает заключение, дано ли строгое обоснование использования каждого сформулированного в явном виде требования доверия.

330 Оценщик делает заключение, дано ли в подразделе «Обоснование требований безопасности» достаточно строгое обоснование, что требования доверия достаточны для изложенной среды безопасности и целей безопасности. Например, если требуется защита от хорошо осведомленных нарушителей, то было бы неприемлемым специфицировать компонент AVA_VLA.1, который является несвойственным для обнаружения недостатков безопасности, кроме очевидных.

331 Строгое обоснование может также включать основания, подобные следующим:

а) требования доверия, включенные в ПЗ, соответствие которым заявлено в ЗБ;

б) специфические требования, установленные конкретной системой оценки, правительством или другими организациями;

в) требования доверия, которые содержались в зависимостях функциональных требований безопасности ОО;

г) требования доверия систем и/или продуктов, предназначенных для совместного использования с ОО;

д) требования потребителей.

332 Краткий обзор назначения и целей для каждого ОУД приведен в подразделе 6.2 части 3 ОК.

333 Оценщику следует помнить, что заключение о том, являются ли требования доверия приемлемыми, может быть субъективным, а значит, анализ достаточности строгого обоснования не следует проводить чрезмерно тщательно.

334 Если подраздел «Требования доверия к безопасности ОО» не содержит какой-либо ОУД, то данный шаг оценивания может быть выполнен совместно с шагом оценивания ASE_REQ.1-7.

ASE_REQ.1.5C

ASE_REQ.1-9 Оценщик ***должен проверить***, что в ЗБ, при необходимости, идентифицированы требования безопасности для среды ИТ.

335 Если ЗБ не содержит требований безопасности для среды ИТ, то данный шаг оценивания не применяем и поэтому считается удовлетворенным.

336 Оценщик делает заключение, все ли зависимости ОО от других ИТ в рамках его среды, направленные на обеспечение каких-либо функциональных возможностей безопасности с тем, чтобы достичь целей безопасности для ОО, четко идентифицированы в ЗБ как требования безопасности для среды ИТ.

337 Пример требований безопасности для среды ИТ – межсетевой экран полагается на базовую операционную систему в части обеспечения аутентификации администраторов и долговременного хранения данных аудита. В этом случае требования безопасности для среды ИТ обычно содержат компоненты из классов FAU и FIA.

338 Отметим, что «Требования безопасности для среды ИТ» могут содержать как функциональные требования, так и требования доверия.

339 Пример зависимости от среды ИТ: программный крипто-модуль, который периодически проверяет свой код и, в случае обнаружения несанкционированной модификации, самоотключается. Чтобы дать возможность восстановления, предусмотрено требование FPT_RCV.2 (автоматическое восстановление). Поскольку крипто-модуль не может самостоятельно восстановить свой код после самоотключения, то требование по восстановлению становится требованием к среде ИТ. Одной из зависимостей компонента FPT_RCV.2 является компонент AGD_ADM.1 (руководство администратора). Следовательно, это требование доверия становится требованием доверия для среды ИТ.

340 Оценщику следует помнить, что ссылка требований безопасности для среды ИТ на ФБО относится к функциям безопасности среды, а не к функциям безопасности ОО.

ASE_REQ.1.6C

ASE_REQ.1-10 Оценщик ***должен проверить***, что все операции над требованиями безопасности ИТ идентифицированы.

341 Разрешенными операциями для функциональных компонентов из части 2 ОК являются «назначение», «итерация», «выбор» и «уточнение». Операции «назначение» и «выбор» разрешены только в специально обозначенных местах компонента. Операции «итерация» и «уточнение» разрешены для всех функциональных компонентов.

342 Разрешенными операциями для компонентов доверия из части 3 ОК являются операции «итерация» и «уточнение».

343 Оценщик делает заключение, все ли операции идентифицированы в каждом компоненте, где они используются. Идентификация может быть осуществлена либо путем введения типографских различий, либо путем использования явной идентификации в сопроводительном тексте, либо любым другим способом.

ASE_REQ.1-11 Оценщик ***должен исследовать*** изложение раздела ЗБ «Требования безопасности ИТ», чтобы сделать заключение, все ли операции «назначение» и «выбор» выполнены.

344 Оценщик делает заключение, что все операции «назначение» и «выбор» во всех компонентах либо были полностью выполнены (в компонентах не остается незавершенных операций), либо их неполное выполнение соответствующим образом строго обосновано.

345 Пример неполного выполнения операции – спецификация диапазона значений при выполнении операции «назначение» в компоненте FTA_MCS.1 "Базовое ограничение на параллельные сеансы" для определения числа параллельных сеансов, принадлежащих одному пользователю. Приемлемое строгое обоснование для этого случая заключается в том, что конкретное значение будет выбрано из диапазона допустимых значений администратором в процессе инсталляции ОО.

ASE_REQ.1-12 Оценщик ***должен исследовать*** ЗБ, чтобы сделать заключение, все ли операции выполнены корректно.

346 Оценщик сравнивает каждую формулировку требований в ЗБ с элементом из ОК, из которого она получена, чтобы сделать заключение:

а) для операции «назначение» – выбраны ли значения параметров или переменных в соответствии с указанным типом, требуемым операцией «назначение»;

б) для операции «выбор» – принадлежит ли выбранный пункт или пункты множеству пунктов, указанных во фрагменте «выбор» данного элемента. Оценщик также делает заключение, приемлемо ли число выбранных пунктов для данного требования. Для некоторых требований требуется выбор только одного пункта (например, FAU_GEN.1.1.b), в других случаях приемлем выбор нескольких пунктов (например, вторая операция в FDP_ITT.1.1).

в) для операции «уточнение» – уточнен ли компонент таким образом, что ОО, удовлетворяющий уточненному требованию, также удовлетворяет и не уточненному требованию. Если уточненное требование выходит за эти рамки, то оно считается расширенным требованием.

Пример: ADV_SPM.1.2C – Модель ПБО должна содержать описание правил и характеристик всех политик безопасности организации, которые могут быть смоделированы.

Уточнение: Модель ПБО должна охватывать только управление доступом.

Если политика управления доступом является единственной политикой ПБО, то такое уточнение является правомерным. Если в ПБО также имеются политики идентификации и аутентификации, а уточнение означает сформулировать, что моделировать следует только контроль доступа, то это уточнение не является правомерным.

Особым случаем уточнения является редакционное уточнение, когда в требование вносятся небольшие изменения, а именно переформулирование предложения в соответствии с особенностями грамматики. Не допускается, чтобы такое изменение каким-либо образом изменяло смысл требования.

Пример редакционного уточнения – FAU_ARP.1 с единственным действием. Вместо записи: «ФБО должны предпринять *информировать оператора* при обнаружении возможного нарушения безопасности» допускается, чтобы разработчик ЗБ написал: «ФБО должны *информировать оператора* при обнаружении возможного нарушения безопасности».

Оценщику следует помнить, что редакционные уточнения должны быть четко идентифицированы (см. шаг оценивания ASE_REQ.1-10).

г) для операции «итерация» – отличается ли каждая итерация компонента от каждой другой итерации этого компонента (по крайней мере, один элемент одной итерации компонента должен отличаться от соответствующего элемента другой итерации компонента), или что компонент применяется к разным частям ОО.

ASE_REQ.1.7C

ASE_REQ.1-13 Оценщик ***должен исследовать*** изложение раздела ЗБ «Требования безопасности ИТ», чтобы сделать заключение, удовлетворены ли зависимости, требуемые компонентами, используемыми при изложении раздела ЗБ «Требования безопасности ИТ».

347 Зависимости могут быть удовлетворены включением соответствующего компонента (или компонента, иерархичного по отношению к последнему) в подраздел ЗБ «Требования безопасности для ОО» или в подраздел «Требования безопасности для среды ИТ».

348 Хотя ОК способствуют проведению анализа зависимостей путем их включения в описание компонентов требований, сам по себе этот факт не является строгим обоснованием того, что никакие другие зависимости не существуют. Приведем пример существования таких зависимостей: элемент, в который включена ссылка «все объекты» или «все субъекты», может иметь зависимость по отношению к уточнению в другом элементе или наборе элементов, в котором перечисляются данные объекты или субъекты.

349 Предполагается, что зависимости требований безопасности для среды ИТ излагаются и удовлетворяются в ЗБ.

350 Оценщику следует помнить, что в ОК не требуется, чтобы все зависимости были удовлетворены: см. следующий шаг оценивания.

ASE_REQ.1.8C

ASE_REQ.1-14 Оценщик ***должен исследовать*** «Обоснование требований безопасности», чтобы сделать заключение, содержится ли в нем приемлемое строгое обоснование для каждого случая, когда зависимости требований безопасности не удовлетворены.

351 Оценщик с учетом идентифицированных целей безопасности делает заключение, объясняется ли в строгом обосновании, почему удовлетворение зависимости не требуется.

352 Оценщик подтверждает, что никакое неудовлетворение зависимости не препятствует тому, чтобы набор требований безопасности адекватно учитывал цели безопасности. Такой анализ проводится в соответствии с ASE_REQ.1.12C.

353 Пример приемлемого строгого обоснования. Для программного ОО имеется цель безопасности следующего содержания – "случаи неуспешной аутентификации должны быть зарегистрированы с указанием идентификационной информации о пользователе, времени и дате", и для удовлетворения данной цели безопасности используется функциональное требование на основе компонента FAU_GEN.1 (генерация данных аудита). Компонент FAU_GEN.1 содержит зависимость от компонента FPT_STM.1 (надежные метки времени). Так как ОО не имеет встроенных часов, то FPT_STM.1 определяется разработчиком ЗБ как требование безопасности для среды ИТ. Разработчик ЗБ указывает на то, что данное требование не подлежит удовлетворению, приводя следующее строгое обоснование: "в данной конкретной среде существуют возможности проведения атак на механизм меток времени; таким образом, среда может не обеспечить надежные метки времени. Но имеющиеся источники угроз неспособны к проведению атак на механизмы меток времени, а другие атаки со стороны этих источников угроз могут быть подвергнуты анализу с регистрацией времени и даты осуществления".

ASE_REQ.1.9C

ASE_REQ.1-15 Оценщик ***должен проверить***, включено ли в ЗБ заявление минимального уровня стойкости функции безопасности для функциональных требований безопасности ОО, и определен ли этот уровень СФБ как базовый, средний или высокий.

354 Если требования доверия к безопасности ОО не включают компонент AVA_SOF.1, то данный шаг оценивания не применяем и поэтому считается удовлетворенным.

355 Стойкость криптографических алгоритмов находится вне области действия ОК. Стойкость функции безопасности применяется только к вероятностным и перестановочным механизмам, которые являются некриптографическими. Следовательно, когда в ЗБ содержится утверждение о минимальном уровне СФБ, оно не применимо к каким бы то ни было криптографическим механизмам, с точки зрения оценки по ОК. Когда такие криптографические механизмы включены в ОО, то оценщик делает заключение, включено ли в ЗБ четкое изложение того, что оценка стойкости криптографических алгоритмов не является частью оценки по ОК.

356 ОО может состоять из нескольких отдельных доменов, тогда автор ЗБ может посчитать более приемлемым иметь минимальный уровень стойкости функций безопасности для каждого домена, а не иметь один общий минимальный уровень стойкости функций безопасности для всего ОО. В этом случае допускается разделить функциональные требования безопасности ОО на отдельные поднаборы и иметь различные минимальные уровни стойкости функций безопасности, ассоциированные с каждым поднабором.

357 Примером этого является распределенная терминальная система, включающая терминалы пользователей, расположенные в общедоступных местах, и терминалы администраторов, расположенные в физически защищенном месте. С требованиями по аутентификации для терминалов пользователей связана средняя СФБ, в то время как с требованиями по аутентификации для терминалов администраторов связана базовая СФБ. Вместо заявления о базовой СФБ как о минимальном уровне СФБ для ОО, что могло бы утвердить потенциальных потребителей ОО во мнении, что провести успешную атаку на механизмы аутентификации на терминалах пользователя относительно несложно, автор ЗБ разделяет ОО на два домена: домен пользователей и домен администраторов; разделяет функциональные требования безопасности ОО на два поднабора, соответствующие выделенным доменам ОО; назначает в качестве минимального уровня СФБ базовую СФБ для поднабора требований, соответствующих домену администраторов, и среднюю СФБ для поднабора требований, соответствующих домену пользователей.

ASE_REQ.1.10C

ASE_REQ.1-16 Оценщик ***должен проверить***, что в ЗБ идентифицированы все конкретные функциональные требования безопасности ОО, для

которых целесообразна заявленная в явном виде стойкость функции безопасности вместе с конкретной метрикой.

358 Если подраздел «Требования доверия к безопасности ОО» не содержит компонент AVA_SOF.1, то данный шаг оценивания не применяем и поэтому считается удовлетворенным.

359 Заявленной в явном виде стойкостью функции безопасности может быть «базовая СФБ», «средняя СФБ», «высокая СФБ» или заданная специфическая метрика. Когда используется специфическая метрика, оценщик делает заключение, является ли она приемлемой для конкретного типа функциональных требований, и имеется ли возможность оценки утверждений о СФБ, выраженных в данной метрике.

360 Дальнейшие указания по приемлемости и допустимости метрик стойкости функций безопасности могут быть представлены конкретной системой оценки.

ASE_REQ.1.11C

ASE_REQ.1-17 Оценщик ***должен исследовать*** «Обоснование требований безопасности», чтобы сделать заключение, демонстрирует ли оно согласованность минимального уровня стойкости функций, а также каждой заявленной в явном виде стойкости функции с целями безопасности для ОО.

361 Если в подраздел «Требования доверия к безопасности ОО» не включен компонент AVA_SOF.1, то данный шаг оценивания не применяем и поэтому считается удовлетворенным.

362 Оценщик делает заключение, учтены ли в подразделе ЗБ «Обоснование требований безопасности» детали, имеющие отношение к предполагаемой компетентности, ресурсам и мотивации нарушителей, описанные в разделе «Среда безопасности ОО». Например, утверждение о базовой СФБ неприемлемо, если требуется, чтобы ОО обеспечил защиту от нарушителей, обладающих высоким потенциалом нападения.

363 Оценщик также делает заключение, учтены ли в подразделе ЗБ «Обоснование требований безопасности» все специфические, связанные со стойкостью функций безопасности, характеристики целей безопасности. Оценщик может использовать прослеживание от требований к целям безопасности, чтобы сделать заключение, что требования, прослеженные к целям безопасности со специфическими, связанными со стойкостью функций безопасности, характеристиками, при необходимости, включают соответствующее утверждение о стойкости связанных с этими требованиями функций безопасности.

ASE_REQ.1.12C

ASE_REQ.1-18 Оценщик ***должен исследовать*** «Обоснование требований безопасности», чтобы сделать заключение, прослежены ли требования безопасности ОО к целям безопасности для ОО.

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

365 Отсутствие такого прослеживания означает, что-либо подраздел «Обоснование требований безопасности» является неполным, либо раздел «Цели безопасности» является неполным, либо функциональное требование безопасности ОО является бесполезным.

366 Является также допустимым, но необязательным, прослеживание отдельных или всех требований доверия к безопасности ОО к целям безопасности для ОО.

367 Пример прослеживания требования доверия к безопасности ОО к цели безопасности для ОО – ЗБ, содержащее угрозу: "Пользователь непреднамеренно раскрывает информацию, используя изделие, которое он принимает за ОО" и цель безопасности для ОО для противостояния данной угрозе: "ОО должен быть четко помечен соответствующим номером версии". Изложенная цель безопасности для ОО может быть достигнута путем выполнения требований компонента ACM_CAP.1, и поэтому разработчик ЗБ прослеживает данный компонент к рассматриваемой цели безопасности для ОО.

ASE_REQ.1-19 Оценщик ***должен исследовать*** подраздел ЗБ «Обоснование требований безопасности», чтобы сделать заключение, прослежены ли требования безопасности для среды ИТ к целям безопасности для среды.

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

369 Отсутствие такого прослеживания означает, что-либо подраздел «Обоснование требований безопасности» является неполным, либо подраздел «Цели безопасности для среды» является неполным, либо функциональное требование безопасности для среды ИТ является бесполезным.

370 Является также допустимым, но необязательным, для некоторых или всех требований доверия к безопасности для среды ИТ прослеживание к целям безопасности для среды.

ASE_REQ.1-20 Оценщик ***должен исследо***вать «Обоснование требований безопасности», чтобы сделать заключение, содержится ли в нем для

каждой цели безопасности для ОО приемлемое строгое обоснование того, что требования безопасности ОО пригодны для удовлетворения данной цели безопасности.

371 Если никакие требования безопасности ОО не прослежены к конкретной цели безопасности для ОО, то данный шаг оценивания считается неуспешным.

372 Оценщик делает заключение, демонстрирует ли строгое обоснование для цели безопасности для ОО, что, если все требования безопасности ОО, прослеженные к данной цели, удовлетворены, то цель безопасности для ОО достигнута.

373 Оценщик также делает заключение, действительно ли каждое требование безопасности ОО, прослеженное к цели безопасности для ОО, будучи удовлетворенным, вносит вклад в достижение данной цели безопасности.

374 Обратите внимание, что прослеживание от требований безопасности ОО к целям безопасности для ОО, представленное в подразделе «Обоснование требований безопасности», может быть частью строгого обоснования, но само по себе оно не является строгим обоснованием.

ASE_REQ.1-21 Оценщик ***должен исследовать*** подраздел ЗБ «Обоснование требований безопасности», чтобы сделать заключение, содержит ли он для каждой цели безопасности для среды ИТ приемлемое строгое обоснование, что требования безопасности для среды ИТ пригодны для удовлетворения данной цели безопасности для среды ИТ.

375 Если никакие требования безопасности для среды ИТ не прослежены к конкретной цели безопасности для среды ИТ, то данный шаг оценивания считается неуспешным.

376 Оценщик делает заключение, демонстрирует ли строгое обоснование для цели безопасности для среды, что, если все требования безопасности для среды ИТ, прослеженные к данной цели безопасности для среды ИТ, удовлетворены, то цель безопасности для среды ИТ достигнута.

377 Оценщик также делает заключение, действительно ли каждое требование безопасности для среды ИТ, прослеженное к цели безопасности для среды ИТ, будучи удовлетворенным, вносит вклад в достижение данной цели безопасности.

378 Обратите внимание, что прослеживание требований безопасности для среды ИТ к целям безопасности для среды ИТ, представленное в подразделе «Обоснование требований безопасности» может быть частью строгого обоснования, но само по себе оно не является строгим обоснованием.

ASE_REQ.1.13C

ASE_REQ.1-22 Оценщик ***должен исследовать*** подраздел ЗБ «Обоснование требований безопасности», чтобы сделать заключение, демонстрирует ли он внутреннюю непротиворечивость совокупности требований безопасности ИТ.

379 Оценщик делает заключение, что во всех случаях, когда различные требования безопасности ИТ имеют отношение к одним и тем же типам событий, операций, данных, тестов, подлежащих выполнению, и т.д., и данные требования могут вступать в противоречие друг с другом, дано приемлемое строгое обоснование отсутствия таких противоречий.

380 Например, если ЗБ содержит требования, связанные как с индивидуальной подотчетностью пользователей, так и с их анонимностью, необходимо, чтобы было показано, что данные требования не противоречат друг другу. Это может включать показ того, что ни одно из подлежащих аудиту событий, для которых требуется индивидуальная подотчетность пользователей, не имеет отношения к действиям, для которых требуется анонимность пользователей.

ASE_REQ.1-23 Оценщик ***должен исследовать*** подраздел ЗБ «Обоснование требований безопасности», чтобы сделать заключение, демонстрирует ли он, что совокупность требований безопасности ИТ образует взаимно поддерживающее целое.

381 Данный шаг оценивания основывается на заключениях, сделанных в ходе выполнения шагов оценивания ASE_REQ.1-18 и ASE_REQ.1-19, связанных с исследованием прослеживания от требований безопасности ИТ к целям безопасности, и шагов оценивания ASE_REQ.1-20 и ASE_REQ.1-21, связанных с исследованием пригодности требований безопасности ИТ для удовлетворения целей безопасности. Данный шаг оценивания требует от оценщика рассмотреть возможность фактического недостижения какой-либо цели безопасности из-за недостаточной поддержки со стороны других требований безопасности ИТ.

382 Данный шаг оценивания также основывается на анализе зависимостей, выполняемом на предыдущих шагах оценивания, так как, если функциональное требование A имеет зависимость от функционального требования B, то B поддерживает A по определению.

383 Оценщик делает заключение, демонстрирует ли подраздел ЗБ «Обоснование требований безопасности» поддержку функциональными требованиями друг друга, где необходимо, даже когда указано, что зависимости между этими требованиями нет. Предполагается, что такая демонстрация охватывает те функциональные требования безопасности, которые направлены на:

а) предотвращение обхода механизмов, реализующих другие функциональные требования безопасности, такие, например, как FPT_RVM.1;

б) предотвращение вмешательства в работу механизмов, реализующих другие функциональные требования безопасности, такие, например, как FPT_SEP;

в) предотвращение деактивации механизмов, реализующих другие функциональные требования безопасности, такие, например, как FMT_MOF.1;

г) обеспечение возможности обнаружения нападений (атак), направленных на нарушение работы механизмов, реализующих другие функциональные требования безопасности, такие, например, как компоненты класса FAU.

384 В своем анализе оценщик учитывает результаты выполненных операций, чтобы сделать заключение, затрагивают ли они взаимную поддержку требованиями друг друга.

7.4.6.3.2 Действие ASE_REQ.1.2E

ASE_REQ.1-24 Оценщик ***должен исследовать*** изложение раздела ЗБ «Требования безопасности ИТ», чтобы сделать заключение, является ли оно логически упорядоченным.

385 Изложение требований безопасности ИТ является логически упорядоченным, если его содержание и структура изложения понятны целевой аудитории (то есть, оценщикам и потребителям).

ASE_REQ.1-25 Оценщик ***должен исследовать*** изложение раздела ЗБ «Требования безопасности ИТ», чтобы сделать заключение, является ли оно полным.

386 При выполнении данного шага оценивания используются результаты шагов оценивания, выполняемых в соответствии с требованиями ASE_REQ.1.1E и ASE_SRE.1.1E, и в особенности – результаты исследования оценщиком подраздела «Обоснование требований безопасности».

387 Изложение раздела «Требования безопасности ИТ» является полным, если все операции над требованиями завершены, и оценщик делает вывод, что требования безопасности достаточны для удовлетворения всех целей безопасности для ОО.

ASE_REQ.1-26 Оценщик ***должен исследовать*** изложение раздела ЗБ «Требования безопасности ИТ», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

388 При выполнении данного шага оценивания используются результаты шагов оценивания, выполняемых в соответствии с требованиями ASE_REQ.1.1E и ASE_SRE.1.1E, и в особенности – результаты исследования оценщиком подраздела «Обоснование требований безопасности».

389 Изложение раздела «Требования безопасности ИТ» является внутренне непротиворечивым, если оценщик делает заключение, что ни одно требование безопасности не противоречит любому другому требованию безопасности таким образом, что цель безопасности не будет полностью удовлетворена.

7.4.7 Оценка требований безопасности ИТ, сформулированных в явном виде (ASE_SRE.1)

7.4.7.1 Цели

390 Цель данного подвида деятельности – сделать заключение, являются ли функциональные требования и/или требования доверия к безопасности, сформулированные без ссылки на ОК, приемлемыми и адекватными.

7.4.7.2 Замечания по применению

391 Этот раздел применим только в случае, если в ЗБ содержатся требования безопасности, сформулированные в явном виде без ссылки на часть 2 или 3 ОК. В противном случае все шаги оценивания, описанные в данном разделе, не применяемы и поэтому считаются удовлетворенными.

392 Требования семейства ASE_SRE не заменяют требования семейства ASE_REQ, а являются дополнительными к ним. Это означает, что требования безопасности, сформулированные в явном виде без ссылки на часть 2 или 3 ОК, должны быть оценены на соответствие критериям семейства ASE_SRE, а также в сочетании со всеми остальными требованиями безопасности – на соответствие критериям семейства ASE_REQ.

7.4.7.3 Исходные данные

393 Свидетельством оценки для этого подвида деятельности является ЗБ.

7.4.7.4 Действия оценщика

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

а) ASE_SRE.1.1E;

б) ASE_SRE.1.2E.

7.4.7.4.1 Действие ASE_SRE.1.1E

ASE_SRE.1.1C

ASE_SRE.1-1 Оценщик ***должен проверить***, что в изложении раздела ЗБ «Требования безопасности ИТ» идентифицированы все требования безопасности ОО, которые сформулированы в явном виде без ссылки на ОК.

395 Требуется, чтобы все функциональные требования безопасности ОО, которые не специфицированы на основе функциональных компонентов из части 2 ОК, были четко идентифицированы как таковые. Аналогично также требуется, чтобы все требования доверия к безопасности ОО, которые не специфицированы на основе компонентов доверия из части 3 ОК, были четко идентифицированы как таковые.

ASE_SRE.1.2C

ASE_SRE.1-2 Оценщик ***должен проверить***, что в изложении раздела ЗБ «Требования безопасности ИТ» идентифицированы все требования безопасности для среды ИТ, которые сформулированы в явном виде без ссылки на ОК.

396 Требуется, чтобы все функциональные требования безопасности для среды ИТ, которые не специфицированы на основе функциональных компонентов из части 2 ОК, были четко идентифицированы как таковые. Аналогично также требуется, чтобы все требования доверия к среде ИТ, которые не специфицированы на основе компонентов доверия из части 3 ОК, были четко идентифицированы как таковые.

ASE_SRE.1.3C

ASE_SRE.1-3 Оценщик ***должен исследовать*** «Обоснование требований безопасности», чтобы сделать заключение, содержится ли в нем приемлемое строгое обоснование, почему каждое из сформулированных в явном виде требований безопасности пришлось сформулировать в явном виде.

397 Оценщик для каждого сформулированного в явном виде требования безопасности ИТ делает заключение, объясняется ли в строгом обосновании, почему существующие функциональные компоненты или компоненты доверия (из частей 2 и 3 ОК соответственно) не могли быть использованы для выражения требований безопасности, сформулированных в явном виде. При вынесении заключения оценщик принимает во внимание возможность выполнения операций (то есть, назначение, итерация, выбор и уточнение) над этими существующими компонентами.

ASE_SRE.1.4C

ASE_SRE.1-4 Оценщик ***должен исследовать*** каждое сформулированное в явном виде требование безопасности ИТ, чтобы сделать заключение, использованы ли для этого требования в качестве модели для представления компоненты, семейства и классы требований из ОК.

398 Оценщик делает заключение, представлены ли сформулированные в явном виде требования безопасности ИТ в том же стиле и на сопоставимом уровне детализации, что и компоненты из частей 2 или 3 ОК. Оценщик также делает заключение, подразделяются ли функциональные требования на отдельные функциональные элементы, и определяют ли требования доверия элементы действий разработчика, содержания и представление свидетельств, а также действий оценщика.

ASE_SRE.1.5C

ASE_SRE.1-5 Оценщик ***должен исследовать*** каждое сформулированное в явном виде требование безопасности ИТ, чтобы сделать заключение, измеримо ли оно и формулирует ли объективные требования оценки,

такие, что соответствие или несоответствие им ОО может быть определено и продемонстрировано систематическим методом.

399 Оценщик делает заключение, изложены ли функциональные требования таким образом, что они тестируемы и прослеживаемы к соответствующим представлениям ФБО. Оценщик также делает заключение, что требования доверия не приводят к потребности вынесения о них субъективного суждения со стороны оценщика.

ASE_SRE.1.6C

ASE_SRE.1-6 Оценщик ***должен исследовать*** каждое сформулированное в явном виде требование безопасности ИТ, чтобы сделать заключение, выражено ли оно четко и однозначно.

ASE_SRE.1.7C

ASE_SRE.1-7 Оценщик ***должен исследовать*** «Обоснование требований безопасности», чтобы сделать заключение, демонстрирует ли оно, что требования доверия применимы и приемлемы для поддержки любых сформулированных в явном виде функциональных требований безопасности ОО.

400 Оценщик делает заключение, приведет ли применение специфицированных требований доверия к получению значимого результата оценки для каждого сформулированного в явном виде функционального требования безопасности или следует специфицировать какие-либо другие требования доверия. Например, сформулированное в явном виде функциональное требование может предполагать потребность в конкретном документальном свидетельстве (таком, например, как модель ПБО), конкретной глубине тестирования или конкретном анализе (таком, как анализ стойкости функций безопасности ОО или анализ скрытых каналов).

7.4.7.4.2 Действие ASE_SRE.1.2E

ASE_SRE.1-8 Оценщик ***должен исследовать*** изложение раздела ЗБ «Требования безопасности ИТ», чтобы сделать заключение, все ли зависимости сформулированных в явном виде требований безопасности ИТ были идентифицированы.

401 Оценщик подтверждает, что никакие подлежащие удовлетворению зависимости не были пропущены разработчиком ЗБ.

402 Примеры возможных зависимостей: компоненты класса FAU, если в сформулированном в явном виде функциональном требовании упоминается аудит; компоненты семейства ADV_IMP, если в сформулированном в явном виде требовании доверия упоминается исходный текст или представление реализации ОО.

7.4.8 Оценка краткой спецификации ОО (ASE_TSS.1)

7.4.8.1 Цели

403 Цель данного подвида деятельности – сделать заключение, представлено ли в разделе ЗБ «Краткая спецификация ОО» четкое и непротиворечивое высокоуровневое определение функций безопасности и мер доверия, и удовлетворяют ли они специфицированным требованиям безопасности ОО.

7.4.8.2 Исходные данные

404 Свидетельством оценки для этого подвида деятельности является ЗБ.

7.4.8.3 Действия оценщика

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

а) ASE_TSS.1.1E;

б) ASE_TSS.1.2E.

7.4.8.3.1 Действие ASE_TSS.1.1E

ASE_TSS.1.1C

ASE_TSS.1-1 Оценщик ***должен проверить***, что раздел ЗБ «Краткая спецификация ОО» содержит описание функций безопасности ИТ и мер доверия ОО.

406 Оценщик делает заключение, представлено ли в разделе ЗБ «Краткая спецификация ОО» высокоуровневое определение функций безопасности, заявленных как предназначенные для удовлетворения функциональных требований, и мер доверия, заявленных как предназначенные для удовлетворения требований доверия к безопасности ОО.

407 Меры доверия могут быть сформулированы в явном виде или определены посредством ссылки на документы, которые удовлетворяют требованиям доверия к безопасности (например, соответствующие планы качества, планы жизненного цикла, планы управления).

ASE_TSS.1.2C

ASE_TSS.1-2 Оценщик ***должен проверить*** раздел ЗБ «Краткая спецификация ОО», чтобы сделать заключение, прослежена ли каждая функция безопасности ИТ, по крайней мере, к одному функциональному требованию безопасности ОО.

408 Отсутствие такого прослеживания означает, что, либо «Краткая спецификация ОО» является неполной, либо изложение функциональных требований безопасности ОО является неполным, либо функция безопасности ИТ является бесполезной.

ASE_TSS.1.3C

ASE_TSS.1-3 Оценщик ***должен исследовать*** каждую функцию безопасности ИТ, чтобы сделать заключение, описана ли она в неформальном стиле на уровне детализации, необходимом для понимания ее назначения.

409 В одних случаях функция безопасности ИТ может быть представлена на уровне детализации не большем, чем уровень детализации соответствующего

функционального требования или требований безопасности ОО. В других случаях разработчик ЗБ может добавить специфические для ОО детали, например, используя специфическую для ОО терминологию вместо общих терминов, таких, например, как «атрибут безопасности».

410 Обратите внимание, что полуформальный или формальный стиль описания функций безопасности ИТ здесь недопустим, если он не сопровождается неформальным описанием тех же функций. Преследуемая цель – это, в первую очередь, обеспечение понимания назначения функции, а не вынесение заключения о таких свойствах функций безопасности, как полнота и корректность.

ASE_TSS.1.4C

ASE_TSS.1-4 Оценщик ***должен исследовать*** раздел ЗБ «Краткая спецификация ОО», чтобы сделать заключение, все ли ссылки на механизмы безопасности, включенные в ЗБ, прослежены к соответствующим функциям безопасности ИТ.

411 Ссылки в ЗБ на механизмы безопасности являются необязательными, но могут (например) оказаться целесообразными в тех случаях, когда имеются требования о реализации конкретных протоколов или алгоритмов (например, установленные алгоритмы генерации паролей или шифрования). Если ЗБ не содержит никаких ссылок на механизмы безопасности, то данный шаг оценивания не применяем и поэтому считается удовлетворенным.

412 Оценщик делает заключение, прослежен ли каждый механизм безопасности, на который ссылается ЗБ, по крайней мере, к одной функции безопасности ИТ.

413 Отсутствие такого прослеживания означает, что, либо краткая спецификация ОО является неполной, либо механизм безопасности является бесполезным.

ASE_TSS.1.5C

ASE_TSS.1-5 Оценщик ***должен исследовать*** «Обоснование краткой спецификации ОО», чтобы сделать заключение, содержится ли в нем для каждого функционального требования безопасности ОО приемлемое строгое обоснование, что функции безопасности ИТ пригодны для удовлетворения данного функционального требования безопасности ОО.

414 Если никакие функции безопасности ИТ не прослежены к конкретному требованию безопасности ОО, то результат данного шага оценивания – «неудовлетворительно».

415 Оценщик делает заключение, демонстрирует ли строгое обоснование для функционального требования безопасности ОО, что, если все функции безопасности ИТ безопасности, которые прослежены к данному требованию, реализованы, то функциональное требование безопасности ОО выполнено.

416 Оценщик также делает заключение, что каждая функция безопасности ИТ, которая прослежена к функциональному требованию безопасности ОО, будучи реализованной, действительно вносит вклад в удовлетворение данного требования.

417 Обратите внимание, что прослеживание функций безопасности ИТ к функциональным требованиям безопасности ОО, представленное в краткой спецификации ОО, может быть частью строгого обоснования, но само по себе оно не является строгим обоснованием.

ASE_TSS.1-6 Оценщик ***должен исследовать*** подраздел ЗБ «Обоснование краткой спецификации ОО», чтобы сделать заключение, согласуются ли утверждения о стойкости для функций безопасности ИТ со стойкостью функций безопасности для функциональных требований безопасности ОО.

418 Для выполнения данного шага оценивания следует использовать результаты шага оценивания ASE_TSS.1-10.

419 Оценщик делает заключение, что для каждой функции безопасности ИТ, по отношению к которой утверждение о стойкости является приемлемым, данное утверждение является адекватным для всех функциональных требований безопасности ОО, к которым прослежена данная функция безопасности.

420 Обычно адекватность означает, что стойкость функции безопасности ИТ равна или выше, чем стойкость функций безопасности для всех функциональных требований безопасности ОО, к которым данная функция прослежена, но возможны и исключения. Примером такого исключения является случай, когда последовательно используются несколько функций с базовой стойкостью для реализации требования о средней стойкости для аутентификации (например, использование биометрии и PIN-кода).

ASE_TSS.1.6C

ASE_TSS.1-7 Оценщик ***должен исследовать*** подраздел ЗБ «Обоснование краткой спецификации ОО», чтобы сделать заключение, демонстрирует ли он, что сочетание специфицированных функций безопасности ИТ совместно работает так, чтобы удовлетворить функциональные требования безопасности ОО.

421 Этот шаг оценивания основан на заключении о взаимной поддержке функциональных требований безопасности для ОО, сделанном на шаге оценивания ASE_REQ.1-23. Оценщик анализирует последствия включения дополнительной информации в описание функций безопасности ИТ и делает заключение, не приводит ли включение данной информации к внесению потенциальных недостатков безопасности, таких, например, как вмешательство в работу или деактивация механизмов, реализующих другие функции безопасности ИТ.

ASE_TSS.1.7C

ASE_TSS.1-8 Оценщик ***должен проверить*** раздел ЗБ «Краткая спецификация ОО», чтобы сделать заключение, прослежена ли каждая мера доверия, по крайней мере, к одному требованию доверия к безопасности ОО.

422 Отсутствие такого прослеживания означает, что, либо краткая спецификация ОО является неполной, либо изложение требований доверия к безопасности ОО является неполным, либо мера доверия является бесполезной.

ASE_TSS.1.8C

ASE_TSS.1-9 Оценщик ***должен исследовать*** «Обоснование краткой спецификации ОО», чтобы сделать заключение, содержится ли в нем для каждого требования доверия к безопасности ОО приемлемое строгое обоснование того, что меры доверия удовлетворяют требования доверия к безопасности ОО.

423 Если ни одна мера доверия не прослежена к конкретному требованию доверия к безопасности ОО, то результат данного шага оценивания – «неудовлетворительно».

424 Оценщик делает заключение, демонстрирует ли строгое обоснование для требования доверия к безопасности ОО, что, если все меры доверия, которые прослежены к данному требованию, реализованы, то данное требование удовлетворено.

425 Оценщик также делает заключение, действительно ли каждая мера доверия, прослеженная к некоторому требованию доверия к безопасности ОО, будучи реализованной, вносит вклад в удовлетворение данного требования.

426 В изложении меры доверия содержится описание того, как разработчик учитывает требования доверия. Цель данного шага оценивания состоит в том, чтобы сделать заключение о том, являются ли специфицированные меры доверия приемлемыми для удовлетворения требований доверия.

427 Обратите внимание, что прослеживание мер доверия к требованиям доверия к безопасности ОО, представленное в разделе «Краткая спецификация ОО», может быть частью строгого обоснования, но само по себе оно не является строгим обоснованием.

ASE_TSS.1.9C

ASE_TSS.1-10 Оценщик ***должен проверить***, идентифицированы ли в разделе ЗБ «Краткая спецификация ОО» все функции безопасности ИТ, которые реализованы вероятностными или перестановочными механизмами.

428 Если требования доверия к безопасности ОО не включают компонент AVA_SOF.1, то данный шаг оценивания не применяем и поэтому считается удовлетворенным.

429 Может возникнуть необходимость возвращения к данному шагу оценивания, если при анализе других свидетельств оценки будут выявлены перестановочные или вероятностные механизмы, которые не были идентифицированы как таковые в ЗБ.

ASE_TSS.1.10C

ASE_TSS.1-11 Оценщик ***должен проверить***, что для каждой функции безопасности ИТ, для которой это приемлемо, в разделе «Краткая спецификация ОО» установлено требование стойкости функции либо по специальной метрике, либо как базовая, средняя или высокая СФБ.

430 Если требования доверия к безопасности ОО не включают компонент AVA_SOF.1, то данный шаг оценивания не применяем и поэтому считается удовлетворенным.

7.4.8.3.2 Действие ASE_TSS.1.2E

ASE_TSS.1-12 Оценщик ***должен исследовать*** раздел ЗБ «Краткая спецификация ОО», чтобы сделать заключение, является ли данный раздел полным.

431 Раздел ЗБ «Краткая спецификация ОО» является полным, если оценщик сделает вывод, что функции безопасности ИТ и меры доверия достаточны для удовлетворения всех специфицированных требований безопасности ОО. Данный шаг оценивания следует выполнять вместе с шагами оценивания ASE_TSS.1-5 и ASE_TSS.1-9.

ASE_TSS.1-13 Оценщик ***должен исследовать*** раздел ЗБ «Краткая спецификация ОО», чтобы сделать заключение, является ли данный раздел логически упорядоченным.

432 Раздел ЗБ «Краткая спецификация ОО» является логически упорядоченным, если его содержание и структура понятны целевой аудитории (то есть, оценщикам и разработчикам).

ASE_TSS.1-14 Оценщик ***должен исследовать*** раздел ЗБ «Краткая спецификация ОО», чтобы сделать заключение, является ли данный раздел внутренне непротиворечивым.

433 Раздел ЗБ «Краткая спецификация ОО» является внутренне непротиворечивой, если оценщик делает заключение об отсутствии таких противоречий между функциями безопасности ИТ или между мерами доверия, при которых какое-то требование безопасности для ОО не будет полностью удовлетворено.

Приложение A Содержание технического отчета при оценке ПЗ

434 В данном приложении приведено минимально необходимое содержание информации, включаемой в ТОО при оценке ПЗ. Содержание ТОО показано на рисунке А.1; этот рисунок может использоваться как образец при построении структурной схема ТОО.

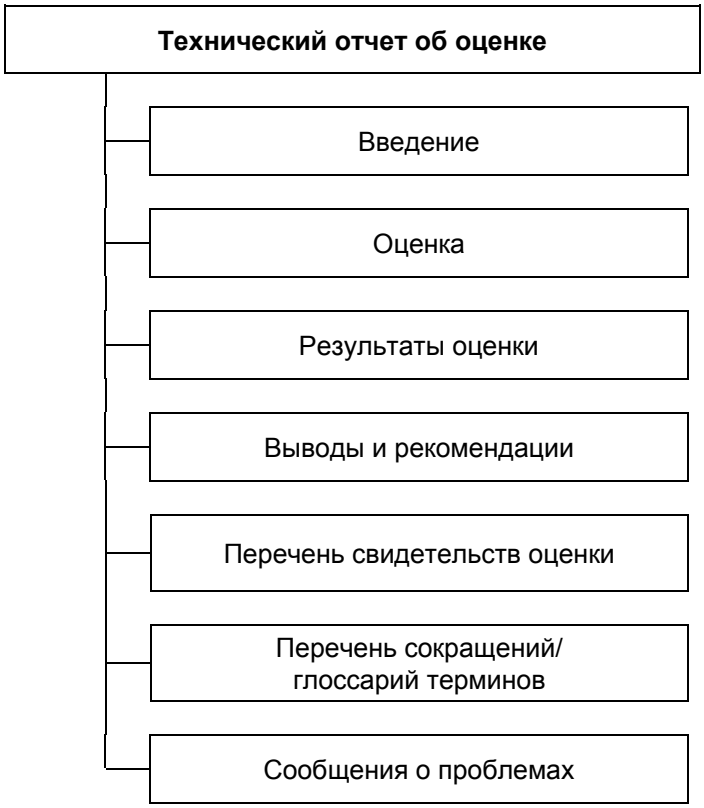

Рисунок А.1 – Содержание ТОО при оценке ПЗ

Введение

435 Оценщик ***должен привести в отчете*** идентификаторы системы сертификации.

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

437 Оценщик ***должен привести в отчете*** идентификаторы контроля конфигурации ТОО.

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

439 Оценщик ***должен привести в отчете*** идентификаторы контроля конфигурации ПЗ.

440 Идентификаторы контроля конфигурации ПЗ (например, название, дата составления и номер версии) требуются, чтобы определить для органа по сертификации, что именно оценивается, и подтвердить правильность вынесенных оценщиком вердиктов.

441 Оценщик ***должен привести в отчете*** идентификатор разработчика.

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

443 Оценщик ***должен привести в отчете*** идентификатор заявителя.

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

445 Оценщик ***должен привести в отчете*** идентификатор оценщика.

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

Оценка

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

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

449 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.

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

Результаты оценки

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

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

Выводы и рекомендации

453 Оценщик ***должен привести в отчете*** выводы по результатам оценки, в частности, общий вердикт в соответствии с подразделом 5.2 части 1 ОК и процедурой вынесения вердикта, описанной в подразделе 5.2 "Вердикты оценщика".

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

Перечень свидетельств оценки

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

- составитель (например, разработчик, заявитель);
- название;
- уникальная ссылка (например, дата составления и номер версии).

Перечень сокращений/глоссарий терминов

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

457 В ТОО нет необходимости повторять определения глоссария, уже приведенные в ОК.

Сообщения о проблемах

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

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